UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA INGENIERÍA EN TELECOMUNICACIONES

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR

PROYECTO DE INVESTIGACIÓN

TEMA:

"ETHICAL HACKING PARA LA IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN FRECUENCIAS INALÁMBRICAS DE PORTONES ELÉCTRICOS MEDIANTE EL USO DE DISPOSITIVO ANALIZADORES DE ESPECTRO"

Trabajo de Grado previo a la obtención del título de Ingeniera en Telecomunicaciones.

Línea de investigación: Desarrollo, aplicación de software y cybersecurity.

AUTOR:

Tandayamo Valencia Smith Francisco

DIRECTOR:

Msc. Fabián Geovanny Cuzme Rodríguez

Ibarra, 2025

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1753015609		
APELLIDOS Y NOMBRES:	Tandayamo Valencia Smith Francisco		
DIRECCIÓN:	Av. Luis Cordero y 23 de Julio		
EMAIL:	francismithv@gmail.com		
TELÉFONO FIJO:	022361351	**TELF. MOVIL**	0992337955

DATOS DE LA OBRA	
TÍTULO:	ETHICAL HACKING PARA LA IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN FRECUENCIAS INALÁMBRICAS DE PORTONES ELÉCTRICOS MEDIANTE EL USO DE DISPOSITIVO ANALIZADORES DE ESPECTRO
AUTOR (ES):	Tandayamo Valencia Smith Francisco
FECHA: AAAAMMDD	2025/01/06
SOLO PARA TRABAJOS DE INTEGRACIÓN CURRICULAR	
CARRERA/PROGRAMA:	X **GRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniera en Telecomunicaciones
DIRECTOR:	**MSC. Fabián Cuzme**

AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Tandayamo Valencia Smith Francisco, con cédula de identidad Nro. 1753015609, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de integración curricular descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

Ibarra, a los 06 días del mes de enero de 2025

EL AUTOR:

.....

Tandayamo Valencia Smith Francisco

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 06 días, del mes de enero de 2025

EL AUTOR:

Tandayamo Valencia Smith Francisco
C.I.175305609

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 06 de enero de 2025

MAGÍSTER CUZME RODRÍGUEZ FABIÁN GEOVANNY, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

MSc. Fabián G. Cuzme Rodríguez
C.I.: 1311527012
DIRECTOR

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular "Ethical Hacking para la identificación de vulnerabilidades de seguridad en frecuencias inalámbricas de portones eléctricos mediante el uso de dispositivo analizadores de espectro" elaborado por Tandayamo Valencia Smith Francisco, previo a la obtención del título del Ingeniero en Telecomunicaciones, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

.....

Ing. Fabián Geovanny Cuzme Rodriguez, MSc.
C.C.: 1311527012

.....

Ing. Luis Edilberto Suárez Zambrano, MSc.
C.C.:1002304291

DEDICATORIA

La presente tesis la dedico a mis amados padres,

Francisco y Norma por todo el esfuerzo que me brindaron durante todos estos años de carrera. Por darme el carácter y valores necesarios para afrontar este camino que está llegando a su fin. A siempre perseguir mis sueños y ver plasmados en mis logros el cariño y sacrificio que mi brindaron día a día.

Tandayamo Valencia Smith Francisco

AGRADECIMIENTO

A mis queridos padres, que siempre estuvieron para apoyarme en esta etapa de mi vida.

A mi hermano y hermanas, gracias a su apoyo moral y tiempo en todo este recorrido para poder lograr mis metas.

A mis padrinos de la infancia que siempre estuvieron pendientes en cada uno de los escalones que tenía que subir años tras año.

A mi director de tesis MsC Fabián Cuzme, por su valiosa enseñanza académica durante el transcurso de la carrera, a todo el tiempo prestado y amplio conocimiento de diversos temas para poder terminar con éxito la presente investigación.

Finalmente agradecer a todas las personas que formaron parte de esta etapa académica, especialmente a mis queridos amigos.

Tandayamo Valencia Smith Francisco

RESUMEN EJECUTIVO

La presente investigación analiza las vulnerabilidades de seguridad inalámbrica en los portones automáticos, evidenciando los riesgos asociados a su uso cotidiano. Se evaluaron las frecuencias utilizadas por estos dispositivos en diversos escenarios, aplicando la metodología de Offensive Security en sus diferentes fases y cumpliendo con los lineamientos establecidos en la norma ISO/IEC/IEEE 29148.
En la fase 1, se identificaron las características esenciales de la comunicación inalámbrica en portones eléctricos. Posteriormente para la Fase 2, se analizaron los riesgos asociados a los mandos inalámbricos, destacándose fallos de seguridad derivados de cifrados débiles o la ausencia de autenticación robusta. En la fase 3, se establecieron los pasos necesarios para cumplir con los objetivos específicos de la investigación. Durante la fase 4, se utilizaron dispositivos SDR como Flipper Zero, RTL-SDR y Adalm Pluto para ejecutar pruebas de penetración, evaluando la eficacia de las medidas de seguridad implementadas en los sistemas de los portones automáticos. Finalmente, en la Fase 5 los resultados demostraron que estos dispositivos pueden tener fallos críticos de seguridad, especialmente en sistemas que carecen de autenticación robusta. Del análisis de siete motores eléctricos, se determinó que cinco de ellos presentaron un nivel de riesgo muy alto o medio, lo que equivale a que más del 70% de los escenarios evaluados evidenciaron vulnerabilidades significativas en su sistema seguridad. Los hallazgos subrayan la necesidad de adoptar medidas de seguridad proporcionales al nivel de riesgo, y se presentan recomendaciones específicas para mitigar posibles ataques y fortalecer la seguridad de estos dispositivos en entornos reales.

Palabras clave: Ethical hacking, SDR, portones eléctricos, vulnerabilidades, analizadores de espectro.

ABSTRACT

This research analyzes wireless security vulnerabilities in automatic gates, highlighting the risks associated with their daily use. The frequencies used by these devices were evaluated in different scenarios, applying the Offensive Security methodology in its different phases and complying with the guidelines established in the ISO/IEC/IEEE 29148 standard.
In Phase 1, the essential characteristics of wireless communication in electric gates were identified. Subsequently, for Phase 2, the risks associated with wireless controls were analyzed, highlighting security flaws arising from weak encryption or the absence of strong authentication. In Phase 3, the steps necessary to meet the specific research objectives were established. During Phase 4, SDR devices such as Flipper Zero, RTL-SDR and Adalm Pluto were used to run penetration tests, evaluating the effectiveness of the security measures implemented in the automatic gate systems. Finally, in Phase 5, the results showed that these devices can have critical security flaws, especially in systems that lack strong authentication. From the analysis of seven electric motors, it was determined that five of them presented a very high or medium level of risk, which means that more than 70% of the evaluated scenarios showed significant vulnerabilities in their security system. The findings underline the need to adopt security measures proportional to the level of risk, and specific recommendations are presented to mitigate possible attacks and strengthen the security of these devices in real environments.

Keywords: Ethical hacking, SDR , Electric gates, Vulnerabilities, Spectrum analyzers

LISTA DE SIGLAS

RF - Radiofrecuencia

DoS - Denegación de Servicio

RFID - Radio Frequency Identification (Identificación por Radiofrecuencia)

IoT - Internet of Things (Internet de las Cosas)

ASK - Amplitude Shift Keying (Modulación por Desplazamiento de Amplitud)

OOK - On-Off Keying (Modulación de Encendido-Apagado)

SDR -Radio Definida por Software

ULF - Ultra Low Frequency (Frecuencia Ultra Baja): 300 Hz – 3 kHz

VLF - Very Low Frequency (Frecuencia Muy Baja): 3 kHz – 30 kHz

LF - Low Frequency (Frecuencia Baja): 30 kHz – 300 kHz

MF - Medium Frequency (Frecuencia Media): 300 kHz – 3 MHz

HF - High Frequency (Frecuencia Alta): 3 MHz – 30 MHz

VHF - Very High Frequency (Frecuencia Muy Alta): 30 MHz – 300 MHz

UHF - Ultra High Frequency (Frecuencia Ultra Alta): 300 MHz – 3 GHz

SHF - Super High Frequency (Frecuencia Super Alta): 3 GHz – 30 GHz

EHF - Extremely High Frequency (Frecuencia Extremadamente Alta): 3GHz–300 GHz

THF - Tremendously High Frequency (Frecuencia Tremendamente Alta): 300 GHz – 3 THz

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 CAPÍTULO I. INTRODUCCIÓN

En este apartado se detallarán los aspectos fundamentales que configuran el proceso de desarrollo del proyecto. Se abordará la identificación de la problemática central de la investigación, la cual será respaldada con una justificación basada en los objetivos establecidos que formaran parte del alcance que tendrá su desarrollo.

1.1 Problema de investigación.

Dentro de los últimos años en el Ecuador, la delincuencia ha ido escalando de manera exponencial por diversos factores sociales. En la actualidad, el robo a condominios es un problema que afecta a muchas personas en el Ecuador. Dentro de la zona 1 del territorio ecuatoriano existen de igual manera diversos robos a domicilios, pero debido a que la ciudadanía no realiza su respectiva denuncia no existen datos a evaluar. Pero según un artículo de El Comercio, los robos en condominios han aumentado en un 30% en los últimos años (Díaz, 2019). Además, según un informe de la Policía Nacional del Ecuador, los robos en condominios son uno de los delitos más comunes en el país(Madrid, 2021) .En el primer semestre del 2022, se registraron 361 robos a domicilios en comparación con los 896 del mismo período del año anterior(*Fiscalía General Del Estado Cifras de Robos*, 2022).

En este contexto existen nuevas maneras que han surgido durante estos nuevos años para poder delinquir en diversos sectores tecnológicos (Borbúa et al., 2017). La vulnerabilidad que existe en todos los dispositivos inalámbricos es cada vez más recurrente y todas las personas que manejan estos aparatos pueden ser blancos de

personas maliciosas (Olmedo & Gavilánez, 2018). Los controles de portones eléctricos son dispositivos fáciles de vulnerar, lo que significa que alguien podría obtener acceso no autorizado a la propiedad privada simplemente copiando la señal del mando y utilizando un dispositivo similar para abrir el portón. Algunos mandos inalámbricos utilizan frecuencias estándar predecibles y fáciles de interceptar. Esto podría permitir que personas ajenas al lugar del establecimiento accedan al código de seguridad y abran el portón sin autorización(Briceño, 2021).

Esto puede ocasionar la pérdida de confianza en los usuarios en la seguridad del conjunto residencial lo que puede afectar a la reputación de esta, debido a que ya no siente seguridad en el lugar en donde residen (Salazar, 2023). Es importante tener en cuenta que algunos de estos problemas se deben a la falta de seguridad en los mandos inalámbricos debido a que son más antiguos o de baja calidad. (Castro et al., 2018)

1.2 Justificación

La realización de pruebas de penetración (pentesting) en los sistemas de acceso automático que utilizan mandos inalámbricos es esencial para verificar las vulnerabilidades de seguridad y evaluar la capacidad de resistencia de estos sistemas(Aguirre, 2020). Al simular ataques y evaluar la capacidad de detección y respuesta de los sistemas, se obtendrá información práctica y concreta sobre las vulnerabilidades existentes, lo cual permitirá una evaluación realista de su seguridad.

La Ley Orgánica de Protección de Datos Personales en Ecuador se centra en regular el tratamiento de los datos personales, estableciendo principios, derechos y obligaciones para su adecuado manejo y protección (*Ley de Protección de Datos Personales,* 2021). De acuerdo con la ley es muy importante la protección de los datos, en tal sentido de que se necesita tener seguridades en las señales que se transmiten en los controles de los dispositivos domésticos, la cual permitiría el aseguramiento de los usuarios, para que tengan un respaldo que sus datos los cuales deberían ser tratados de la manera más eficiente.

Sin embargo, es importante tener en cuenta que la seguridad de los datos es un componente fundamental en la protección de la privacidad y la información personal. En el contexto de las comunicaciones inalámbricas, la seguridad de los datos transmitidos a través de estas redes es crucial para proteger la privacidad y evitar posibles violaciones de datos.

Por tal motivo se realizará la elaboración de un informe detallado sobre las vulnerabilidades de seguridad presentes en los controles de garaje proporcionarán recomendaciones de seguridad específicas y permitirá identificar los riesgos resultantes de no implementar medidas adecuadas de protección((Marañón, 2020). Esto es crucial, ya que la falta de medidas de protección puede dar lugar a accesos no autorizados que podrían ocasionar robos, vandalismo y otros delitos.

1.3 Objetivos

1.3.1 Objetivo General

Analizar las vulnerabilidades de seguridad en las frecuencias inalámbricas utilizadas en los portones eléctricos, que permitan generar recomendaciones para asegurar y proteger la comunicación inalámbrica con el uso del dispositivo analizadores de espectro.

1.3.2 Objetivos Específicos

- Recopilar los datos relacionados con las redes inalámbricas utilizadas en portones automáticos, con el fin de identificar las vulnerabilidades de seguridad más frecuentes que presentan, en donde se investigara los métodos de seguridad empleados en la instalación de portones eléctricos.

- Evaluar, mediante pruebas de penetración con el uso de dispositivo interceptores de señales, las vulnerabilidades de seguridad resultantes de errores de diseño y configuración en los sistemas de acceso automático que utilizan los mandos inalámbricos.

- Implementar los principios y pautas establecidos en la metodología de análisis de riesgo Ofensive Security, en la cual se proporcionará recomendaciones de seguridad, esto con el fin de identificar y descartar las posibles consecuencias resultantes de no implementar medidas adecuadas de protección.

1.4 Alcance

La presente investigación tiene como objetivo analizar las vulnerabilidades de seguridad en las frecuencias inalámbricas utilizadas en los portones eléctricos, esto con el fin de generar recomendaciones para asegurar su integridad y protección. En lo cual se realizará el desarrollo de la investigación aplicada, la cual abordar un problema real y concreto relacionado con la seguridad de estos dispositivos. Para ello, se emplean conocimientos científicos y tecnológicos, como el uso de dispositivos analizadores de espectro y métodos de evaluación de riesgos, que permiten analizar detalladamente las frecuencias inalámbricas involucradas(Castro et al., 2018). La cual brindara soluciones prácticas para fortalecer la seguridad en la comunicación inalámbrica de los mandos a distancia. Para el desarrollo del proyecto se hará uso de la metodología de Análisis de Riesgo Offensive Security, con el motivo a las diversas pruebas que se plantean realizar para cumplir con los objetivos planteados, considerando las fases de Recolección de Información, Análisis de Vulnerabilidades, Definición de Objetivos Secundarios, Ataque y Análisis de Resultados(Monteros Túquerres, 2019).

En la fase de Recolección de Información, se establecerán los objetivos planteados para la investigación, como es analizar las vulnerabilidades de seguridad en las frecuencias inalámbricas utilizadas en los portones eléctricos. Se recopilará los datos relacionados con las frecuencias inalámbricas utilizadas, con el objetivo de identificar las vulnerabilidades de seguridad más frecuentes que presentan. Se llevará a cabo un proceso de recopilación de datos, que incluirá la revisión de fuentes relevantes, como documentación técnica que son el datasheet de los mecanismos automáticos (Ghanem & AlTawy, 2022).

En la fase de Análisis de Vulnerabilidades, se plantea realizar el segundo objetivo específico, con la finalidad de cumplir con la evaluación e identificación de las señales RF haciendo uso de dispositivos SDR. Esta fase desempeña un papel fundamental en el proceso de asegurar la comunicación inalámbrica en los portones eléctricos. Mediante el análisis exhaustivo de posibles vulnerabilidades en las frecuencias inalámbricas, se pueden identificar los puntos débiles y evaluar su impacto potencial de seguridad (Bottarelli et al., 2018).Se realizará un análisis de las posibles vulnerabilidades presentes en estas redes, evaluando los riesgos asociados y estudiando casos reales de ataques (Marañón, 2020). Además, se propondrán medidas de seguridad y buenas prácticas para implementar en las frecuencias inalámbricas, abordando aspectos como la gestión de contraseñas, la configuración adecuada de los dispositivos y la concientización de los usuarios sobre seguridad informática (Parrales et al., 2019).

En la fase de Definición de objetivos, que para esta tercera fase los objetivos se vuelven más concretos debido a que ya se tiene un análisis bibliográfico de cómo funcionan los dispositivos inalámbricos, lo que incrementa la posibilidad de éxito en los ataques hacia la comunicación inalámbrica de los controles de garaje. Con el fin de evaluar de manera precisa el riesgo real presente los sistemas de portones eléctricos.

Para la fase Ataque, se llevará a cabo pruebas de penetración (pentesting) con el objetivo de verificar las vulnerabilidades de seguridad resultantes de errores de diseño y configuración en los sistemas de acceso automático que utilizan los mandos inalámbricos (Reaves & Morris, 2012). Al implementar y cumplir con los requisitos de la metodología de Ofensive Security, se puede establecer un marco sólido para

identificar, evaluar y abordar los riesgos relacionados con la seguridad de la información (Irwin, 2021). Algunos de los controles de seguridad que se encuentran en la metodología pueden ser aplicables a la protección de los datos transmitidos a través de frecuencias inalámbricas, como el cifrado de datos, la autenticación de usuarios y la gestión de acceso (Kumar et al., 2022).

En la fase de Análisis de Resultados, que con base a la información recopilada se llevará a cabo la elaboración de un informe detallado sobre las vulnerabilidades de seguridad presentes en los controles de garaje, con el objetivo de proporcionar recomendaciones de seguridad y mecanismo de mitigación a los riesgos críticos encontrado. Se identificarán y documentarán las posibles vulnerabilidades presentes en estos controles, así como los posibles riesgos asociados a la falta de medidas de protección adecuadas.

2 CAPÍTULO II. MARCO TEÓRICO

En este capítulo, se identifica los aspectos fundamentales que constituyen la base académica esencial para llevar a cabo la investigación. Este fundamento se construye mediante un análisis bibliográfico de diferentes: autores, libros, revistas y sitios web. Las cuales están relacionadas a los fundamentos esenciales sobre el tema de las comunicaciones inalámbricas, las cuales utilizan los dispositivos de baja frecuencia como son los dispositivos SDR.

2.1 Comunicaciones inalámbricas

Las comunicaciones inalámbricas son aquellas en las que la transmisión de información entre un emisor y un receptor prescinde de conexiones físicas mediante cables, las cuales hacen uso de ondas electromagnéticas, que se propagan en el espacio para posibilitar el intercambio de datos(Chiasserini et al., 2020). Esta modalidad de comunicación, al desenvolverse en una porción específica y relativamente imperceptible del espectro electromagnético, escapa a la detección visual directa por parte de todos los seres humanos (Sachan, 2020b)

2.1.1 Señales inalámbricas

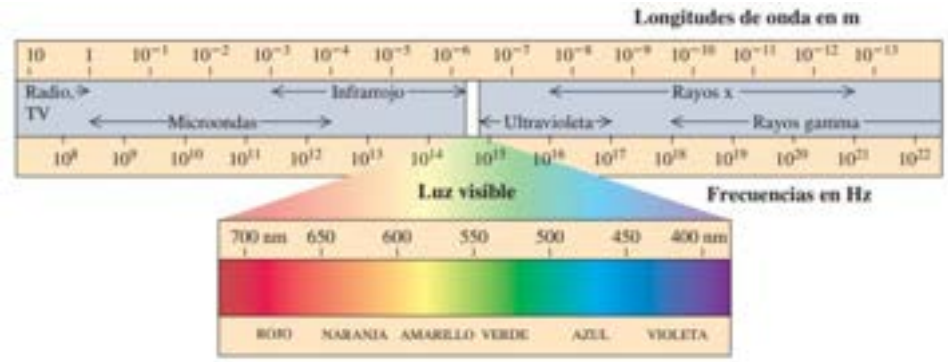
Las señales inalámbricas son un método esencial para la transmisión de información en las comunicaciones modernas. Utilizan ondas electromagnéticas, como microondas, ondas de radio e infrarrojos, para transportar datos, voz o video desde un origen a uno o varios destinos, sin la necesidad de cables físicos (Sachan, 2020a).

2.1.2 Espectro electromagnético

El espectro electromagnético es un rango continuo de frecuencias de ondas electromagnéticas, las cuales van desde las ondas de radio de baja frecuencia hasta los rayos gamma de alta frecuencia como se puede identificar en la Figura 1. Estas ondas se propagan a través del espacio en forma de oscilaciones de campos eléctricos y magnéticos. Según (Tanenbaum & & Wetherall, 2012), el espectro electromagnético es "un rango continuo de frecuencias de ondas electromagnéticas, desde las ondas de radio de baja frecuencia hasta los rayos gamma de alta frecuencia" (p. 123).

Figura 1

Gráfico sobre los rangos del espectro electromagnético



Fuente: Recuperado de https://repository.unimilitar.edu.co/bitstream/handle-10654/43674/Gonz%C3%A1lezSu%C3%A1rezfelipeOswaldo2022.pdf.pdf?sequence=1&isAllowed=y

Las ondas electromagnéticas tienen dos propiedades principales: frecuencia y longitud de onda. La frecuencia es el número de veces que una onda se repite en un segundo. La longitud de onda es la distancia entre dos crestas de una onda. La frecuencia y la longitud de onda están inversamente relacionadas. A mayor frecuencia, menor longitud de onda (Gutiérrez, 2017).

2.1.3 Espectro radioeléctrico

El espectro radioeléctrico es una parte del espectro electromagnético que se utiliza para las comunicaciones inalámbricas. Se extiende desde las ondas de radio de baja frecuencia hasta los rayos infrarrojos de alta frecuencia (García Abad, 2021). Según (Tanenbaum & & Wetherall, 2012). “El espectro radioeléctrico es una parte del espectro electromagnético que se utiliza para las comunicaciones inalámbricas" (p. 123).

Las ondas radioeléctricas son oscilaciones de campos eléctricos y magnéticos que se propagan a través del espacio en forma de ondas. Estas ondas se utilizan para transmitir información, como voz, datos o imágenes, a través de distancias largas. Las ondas radioeléctricas tienen dos propiedades principales: frecuencia y longitud de onda. La frecuencia es el número de veces que una onda se repite en un segundo. La longitud de onda es la distancia entre dos crestas de una onda(García Abad, 2021).

2.1.4 Bandas de operación

En el contexto de las comunicaciones inalámbricas, las bandas de operación son intervalos de frecuencias del espectro radioeléctrico que se asignan a un servicio o aplicación específico(Huidobro Moya, 2014). Las bandas de operación se utilizan para garantizar que los dispositivos inalámbricos no interfieran entre sí. Según la Unión Internacional de Telecomunicaciones, las bandas de operación son "intervalos de frecuencias del espectro radioeléctrico que se asignan a una o más redes o servicios de radiocomunicación”(ITU, 2015). Se puede identificar las distintas bandas de operación en la Tabla 1.

Tabla 1

Bandas de frecuencia según la UIT

Número de banda ITU	Símbolos (en inglés)	Gama de frecuencias (excluido el límite inferior, pero incluido el superior)	Banda
3	ULF	300-3 000 Hz	Ultra baja frecuencia
4	VLF	3-30kHz	Muy baja frecuencia
5	LF	30-300kHz	Baja frecuencia
6	MF	300-3 000 kHz	Frecuencia media
7	HF	3-30 MHz	Alta frecuencia
8	VHF	30-300 MHz	Muy alta frecuencia
9	UHF	300-3 000 MHz	Ultra alta frecuencia
10	SHF	3-30 GHz	Super alta frecuencia
11	EHF	30-300 GHz	Frecuencia extremadamente alta
12	THF	300-3 000 GHz	Frecuencia tremendamente alta
13		3-30 THz	
14		30-300 THz	
15		300-3 000 THz	

Fuente: Obtenido del sitio web https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.431-8-201508-I!!PDF-S.pdf

2.1.5 Modulación de portones eléctricos

Uno de los principales componentes de las comunicaciones inalámbricas de los portones eléctricos es la modulación utilizada para transmitir información hacia el receptor. Este proceso de transmisión se basa en técnicas de modulación, las cuales permiten enviar información mediante una señal portadora. Existen diversas técnicas

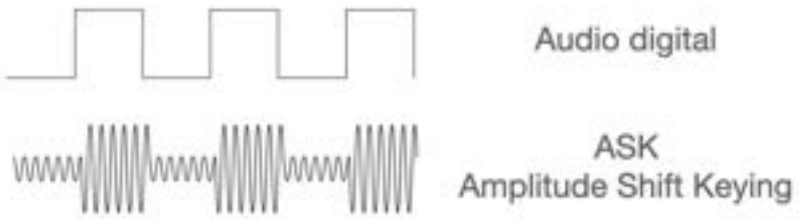
de modulación, tanto analógicas como digitales. En este caso, se analizarán las modulaciones digitales por desplazamiento de amplitud(Cañón, 2021).

2.1.5.1 Modulación ASK (Amplitud-Shift Keying)

La modulación por desplazamiento de amplitud (ASK, por sus siglas en inglés) es una técnica de modulación digital en la cual la amplitud de la señal portadora varía de acuerdo con la información de los datos de entrada. En otras palabras, los bits de datos binarios se representan mediante dos niveles diferentes de amplitud de la señal portadora como se identifica en la Figura 2, existen donde tipos de amplitud en la señal de Audio Digital (Ruiz, 2020).

Figura 2

Representación gráfica de la modulación digital ASK



Nota. Adaptado de "Sistema de comunicación digitales y analógicos" (p.304), por Ruiz, 2020.

- En ASK, un bit '1' se representa con una amplitud alta de la señal portadora, mientras que un bit '0' se representa con una amplitud baja (o nula).

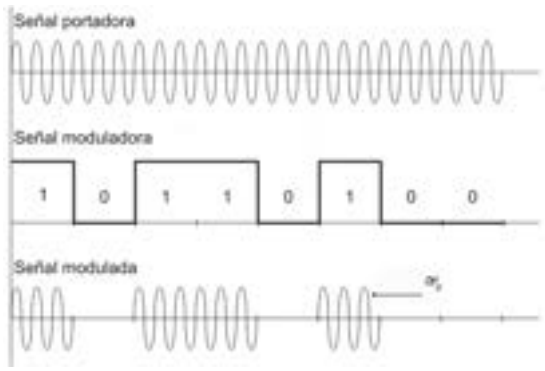
- La frecuencia y la fase de la portadora permanecen constantes durante el proceso de modulación.

2.1.5.2 Modulación OOK (On-Off Keying)

La modulación por encendido-apagado (OOK, por sus siglas en inglés) es una forma especial de ASK donde se utiliza solo dos niveles de amplitud: presencia o ausencia de la portadora. En otras palabras, OOK es una ASK con amplitud cero para representar el bit '0' (Echeagaray, 2020). En la Figura 3 se establece que cuando la señal es transmitida en la modulación OOK, los bits que son igual a 0 no existe ningún tipo de modulación.

Figura 3

Representación gráfica de la modulación OOK



Nota. Adaptado de “Sistema de comunicación digitales y analógicos” (p.304), por Ruiz, 2020.

2.1.6 Seguridad en ambientes inalámbricos

La capa física es la capa más baja en la arquitectura del protocolo OSI, que se utiliza para especificar las características físicas de la transmisión de señales.

Nuevamente, la naturaleza de transmisión de las comunicaciones inalámbricas hace que su capa física sea extremadamente vulnerable a ataques de escucha e interferencia, que son dos tipos principales de ataques inalámbricos a la capa física, como se muestra en la Tabla 2. Más específicamente, el ataque de escucha se refiere a un usuario no autorizado que intenta interceptar la transmisión de datos entre usuarios legítimo (Zou et al., 2016).

En las redes inalámbricas, siempre que haya un espía en el área de cobertura de transmisión del nodo de origen, el espía puede escuchar la sesión de comunicaciones inalámbricas. Para mantener la transmisión confidencial, normalmente se adoptan técnicas criptográficas que se basan en claves secretas para evitar que los ataques de escucha intercepten la transmisión de datos(A. Pérez, 2020).

Tabla 2

Principales ataques inalámbricos de capa física

Ataques en capa física	Características
Eavesdropping	Interceptación de información confidencial
Jamming	Interrupción de la transmisión legítima
Interferencia	Inyección de señales de ruido para interrumpir la comunicación.
Ataques de degradación de señal	Degradación de la calidad de la señal entre los dispositivos de la red inalámbrica
Spoofing	Creación de señales de radiofrecuencia falsas para obtener acceso no autorizado a información
DoS (Denegación de Servicio)	Inundación de la red con tráfico falso para sobrecargarla y denegar el servicio a usuarios legítimos

Fuente: Obtenido del sitio web https://ieeexplore.ieee.org/document/7467419

En este caso, incluso si se trata de un espía. Escucha la transmisión del texto cifrado, sigue siendo difícil extraer el texto sin formato del texto cifrado sin la clave secreta. Además, un nodo malicioso en redes inalámbricas puede generar fácilmente interferencias intencionales para interrumpir las comunicaciones de datos entre usuarios legítimos, lo que se conoce como ataque de interferencia (también conocido como ataque DoS)(Ghanem & AlTawy, 2022). El bloqueador tiene como objetivo impedir que los usuarios autorizados accedan a los recursos de la red inalámbrica y esto perjudica la disponibilidad de la red para los usuarios legítimos. Con este fin, las técnicas de espectro ensanchado son ampliamente reconocidas como un medio eficaz de defensa contra ataques DoS al difundir la señal de transmisión en un ancho de banda espectral más amplio que su banda de frecuencia original (A. Pérez, 2020).

2.2 Portones automáticos

Los portones automáticos consisten en aplicar un sistema electromecánico a una puerta para ejecutar la función de abrirlo y cerrarlo de forma automática. El sistema está compuesto de un motorreductor con una placa electrónica, que actúa bajo comando de un control remoto, normalmente inalámbrico a distancia(Norberto Morel, 2016).

2.2.1 Sistemas de control

El sistema de control de los portones eléctricos es un conjunto de componentes electrónicos que regulan la apertura y el cierre del portón. Este sistema se basa en algunos componentes clave, como el motor, el controlador y los sensores. El motor es el dispositivo que se encarga de mover el portón hacia arriba y hacia abajo. Este motor

está conectado a una fuente de energía eléctrica. El controlador es el dispositivo que se encarga de activar el mecanismo de apertura y cierre del portón (Norberto Morel, 2016).

Este control puede ser de diferentes tipos, como un control remoto o un teclado numérico. Los sensores son dispositivos que detectan la presencia de objetos o personas en la trayectoria del portón. Si detectan algún obstáculo, envían una señal al controlador para detener el movimiento del portón(Ghanem & AlTawy, 2022).

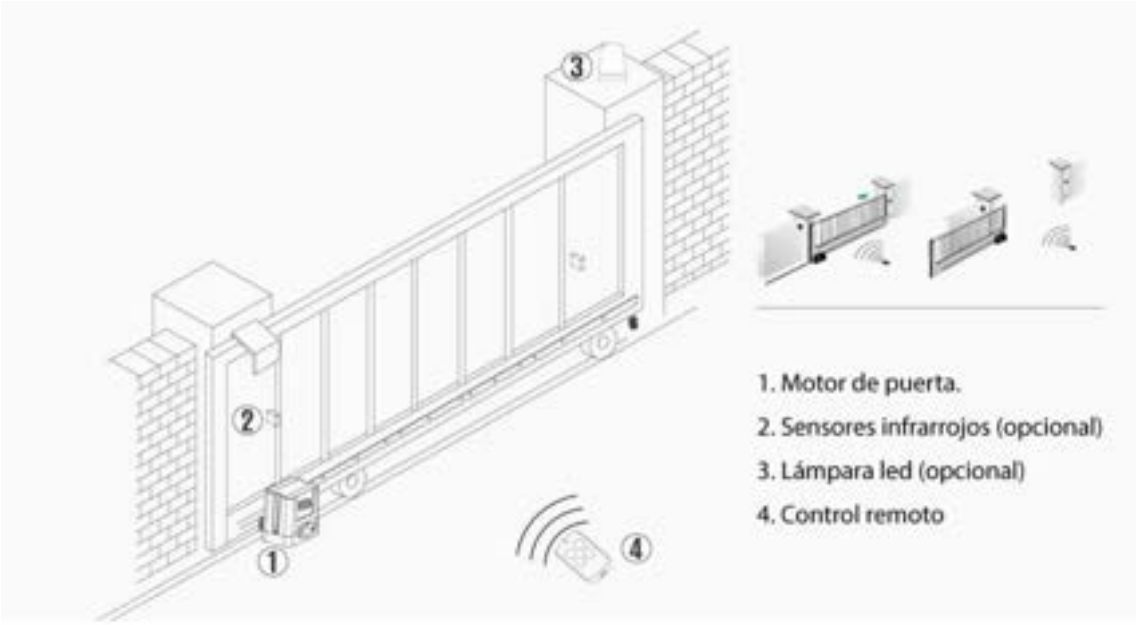
Los portones eléctricos pueden usar diferentes sistemas de apertura, como control remoto, tarjetas de acceso o sensores de proximidad. Además, todos los portones eléctricos deben contar con un sistema mecánico o manual de emergencia para poder abrirse en caso de fallo del sistema remoto o si hay una baja en la energía eléctrica (Norberto Morel, 2016).

2.2.2 Mecanismo de funcionamiento

El mecanismo de funcionamiento de los portones eléctricos se basa en la combinación de componentes mecánicos y electrónicos estos se los puede identificar en la Figura 4 del documento.

Figura 4

Mecanismo de funcionamiento de un portón automático



Fuente: Obtenido del sitio web https://www.portoneselectricosbucaramanga.com/motor-para-porton-corredizo-bulldog-1100/

- **Motor:** Es el encargado de proporcionar la fuerza necesaria para abrir y cerrar el portón. Puede ser eléctrico o hidráulico, y su elección depende del tamaño y peso del portón.
- **Controlador:** Es el cerebro del sistema, se encarga de recibir las señales de apertura y cierre, y de enviar las órdenes al motor para que realice la acción correspondiente. Puede ser controlado mediante un panel de control ubicado cerca del portón o a través de un sistema remoto.
- **Sensores:** Estos dispositivos son fundamentales para garantizar la seguridad en el uso de los portones automáticos. Los sensores detectan la presencia de

obstáculos o personas en el área de movimiento del portón, deteniendo su operación y evitando accidentes.

- **Mecanismos de desplazamiento:** El portón puede desplazarse de diferentes formas, como a través de un sistema de rieles o mediante brazos articulados. Estos mecanismos permiten que el portón se deslice o se abra hacia arriba de manera suave y controlada(Reaves & Morris, 2012).

Al activar el sistema mediante un control remoto o un dispositivo interno, una señal eléctrica es enviada al motor del portón. Este motor, que está conectado a un mecanismo de accionamiento, se encarga de mover las hojas del portón(Reaves & Morris, 2012).

2.2.3 Seguridad en dispositivos

Los códigos de acceso son una forma común de controlar el acceso a los portones eléctricos. Sin embargo, si estos códigos son demasiado simples o predecibles, pueden ser fácilmente descifrados por personas malintencionadas(Shah & Matlaga, 2019). Esto podría permitir a un intruso abrir el portón sin autorización.

Por ejemplo, si un código de acceso es una secuencia simple como “1234” o “0000”, o si es algo que podría estar fácilmente asociado con el propietario (como una fecha de nacimiento o una dirección), entonces podría ser fácilmente adivinado por alguien que intenta obtener acceso no autorizado.

Además, algunos sistemas de portones eléctricos pueden tener vulnerabilidades que permiten a los atacantes “escuchar” o interceptar el código mientras se transmite

desde el mando a distancia al sistema de control del portón. Si un atacante puede capturar este código, puede ser capaz de reutilizarlo para abrir el portón (MIGUEL LUIS & MANUEL, 2020).

Para mitigar estos riesgos, es importante seguir algunas mejores prácticas con respecto a los códigos de acceso:

- **Complejidad del código:** Asegúrate de que tu código de acceso sea lo suficientemente complejo. Evita secuencias obvias o información personal. En su lugar, utiliza una combinación aleatoria de números.
- **Cambio regular del código:** Es una buena idea cambiar tu código de acceso de forma regular. Esto puede ayudar a prevenir el acceso no autorizado si tu código ha sido comprometido1.
- **Sistemas de encriptación avanzada:** Algunos sistemas de portones eléctricos utilizan sistemas de encriptación avanzada para proteger las señales que se transmiten entre el mando a distancia y el sistema de control. Esto puede hacer que sea prácticamente imposible para un delincuente descifrar la señal (MIGUEL LUIS & MANUEL, 2020).

2.2.3.1 Vulnerabilidades (Hackeo o interceptación de la señal)

Existe el riesgo de que las señales inalámbricas sean interceptadas o alteradas por personas malintencionadas. Esto podría permitir a un intruso abrir el portón sin autorización.

El hackeo o la interceptación de la señal es una vulnerabilidad significativa en los sistemas de portones eléctricos que funcionan con mandos a distancia1. Los

delincuentes tecnológicamente avanzados pueden interceptar la señal que se transmite entre el mando a distancia y el sistema de control del portón. Una vez que se intercepta esta señal, los delincuentes pueden replicarla para abrir el portón sin autorización(Castro et al., 2018).

Además, algunos sistemas de portones eléctricos utilizan códigos de acceso simples que pueden ser fácilmente descifrados por personas malintencionadas. Esto también puede permitir a un intruso abrir el portón sin autorización, algunos de los códigos que existen son:

- **Códigos rodantes:** Algunos sistemas de portones eléctricos utilizan lo que se conoce como códigos rodantes. Esto significa que el código que se transmite entre el mando a distancia y el sistema de control cambia cada vez que se utiliza. Esto hace que sea mucho más difícil para un delincuente interceptar y replicar la señal.
- **Sistemas de encriptación avanzada:** Algunos sistemas de portones eléctricos utilizan sistemas de encriptación avanzada para proteger las señales que se transmiten entre el mando a distancia y el sistema de control. Esto puede hacer que sea prácticamente imposible para un delincuente descifrar la señal.
- **Actualizaciones regulares del software:** Mantener actualizado el software del sistema de control puede ayudar a proteger contra las últimas amenazas y vulnerabilidades(R. G. Pérez, 2018).

2.3 Dispositivos analizadores de espectro (SDR)

Radio definida por software o SDR, es aquello que caracteriza a las radios configurables dentro de un sistema de radio de comunicaciones, donde generalmente varios de los componentes físicos que se usarían en radio normal se implementan y configuran en varios entornos de software para cambiar sus parámetros de comunicación(Donat, 2021).

2.3.1 ADALM-PLUTO

ADALM-PLUTO (PlutoSDR) es un módulo de aprendizaje relacionado a la Radio Definida por Software, la radiofrecuencia (RF) y las comunicaciones inalámbricas, tiene como particularidad que el dispositivo puedo funcionar como receptor y transmisión como se puede ver la Figura 5. Es una herramienta de apoyo en el desarrollo académico y profesional de aplicaciones en base a la radiofrecuencia y las comunicaciones del mundo real que tienen su campo en el espectro radioeléctrico(Reyland, 2023).

Figura 5

Dispositivo Adalm - Pluto

Fuente: Obtenido del sitio web: https://www.analog.com/en/design-center/evaluationhardware-and-software/evaluation-boards-kits/ADALM-PLUTO.html

ADALM-PLUTO opera como un laboratorio portátil en las comunicaciones inalámbricas, tiene una variedad de software compatible que proporcionan una interfaz gráfica de usuario (GUI) amigable e intuitiva permitiendo el trabajo inteligente y exploratorio (Reyland, 2023).

Cuenta con canales de transmisión y recepción independientes con capacidad de operación Full Dúplex. Puede generar o recibir señales analógicas de radiofrecuencia en el rango de 325 MHz hasta 3.8 GHz que lo hace ideal para diversas aplicaciones (INCIBE, 2021).

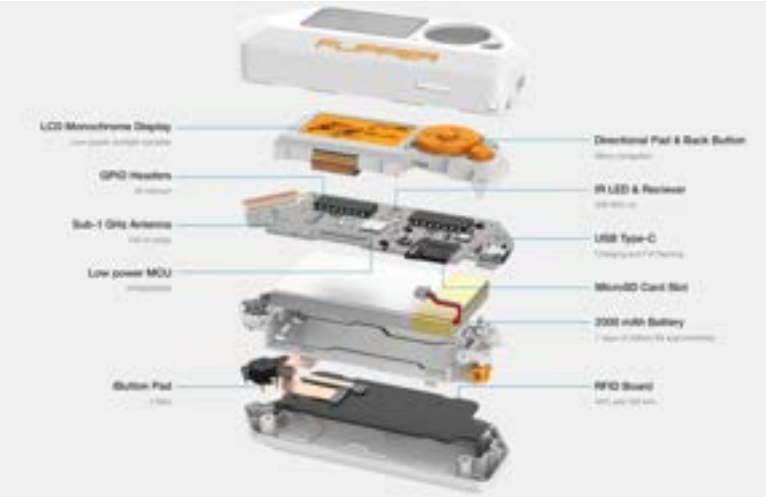
2.3.2 Flipper Zero

Flipper Zero es una multiherramienta portátil para pentesters y geeks en un cuerpo similar a un juguete. Le encanta piratear material digital, como protocolos de radio, sistemas de control de acceso, hardware y más. Es totalmente de código abierto y personalizable (Jiménez, 2020) .

Flipper Zero es una pequeña pieza de hardware con una curiosa personalidad en tanto a su software que asemeja la de un ciberdelfín. El dispositivo puede interactuar con sistemas digitales en la vida que son de uso cotidiano como son mandos a distancia, dispositivos NFC, entre otros. Explora cualquier tipo de sistema de control de acceso, RFID, protocolos de radio que como se puede apreciar en la Figura 6 posee internamente una antena de SUB-1 GHz a lo igual que pines de programación GPIO(flipperzero, 2024).

Figura 6

Dispositivo interno del flipper zero



Fuente: Obtenido del sitio web: https://flipperzero.one/

Este es el rango operativo para una amplia clase de dispositivos inalámbricos y sistemas de control de acceso, como controles remotos para puertas de garaje, barreras tipo brazo, sensores IoT y sistemas remotos sin llave. Flipper tiene una antena integrada de 433MHz y un chip CC1101, lo que lo convierte en un potente transceptor capaz de alcanzar un alcance de hasta 50 metros(Pastor, 2023).

2.3.3 RTL-SDR

RTL-SDR Un RTL-SDR es un dispositivo de bajo coste realmente sencillo de usar para diferentes aplicaciones si se tienen las consideraciones necesarias para su uso como son el hardware y software mínimo que se necesita para operar con estos dispositivos. Este dispositivo como se puede apreciar en la Figura 7 posee entrada USB, lo cual permite la comunicación directa con la computadora, de manera que receptara señales RF en cualquier software que sea compatible (Wyglinski et al., 2018).

Figura 7

Dispositivo RTL SDR

Fuente: Obtenido del sitio web: http://repositorio.uisrael.edu.ec/bitstream/47000/2067/1/UISRAEL-EC-ELDT-378.242-2019-032.pdf

En un inicio los RTL-SDR fueron diseñados para el uso como receptores DVB-T sin embargo, con el pasar de los años los investigadores pudieron ver que se pueden sacar un mejor provecho de estos y usarlos como parte de un sistema SDR. Con las mejoras realizadas a estos dispositivos de acuerdo con el modelo que se utilice podían trabajar en un rango de 25Mhz hasta 1,75 GHZ (Stewart et al., 2015).

En la Figura 8 se detallan las señales inalámbricas que se encuentran cercanas al sistema, estas son receptadas por una antena RF que se encuentra conectada al RTL-SDR, la antena además de recibir señales FM, también recibe señales de radio, señales GPS, así como señales 2G, 3G, 4G (señales celulares), algunas transmisiones que realizan ciertos sectores industriales, bandas de transmisión militar, bandas científicas, entre otros, es decir que el sistema permite la recepción de algunas de las señales que se encuentran en el rango de operación del sintonizador (Stewart et al., 2015).

Figura 8

Bandas de operación del RTL SDR

Fuente: Obtenido del sitio web: http://repositorio.uisrael.edu.ec/bitstream/47000/2067/1/UISRAEL-EC-ELDT-378.242-2019-032.pdf

2.3.4 GNU Radio

GNU Radio es un kit de herramientas de desarrollo de software libre y código abierto que proporciona bloques de procesamiento de señales para implementar Radios definidas por 30 software (SDR). Se puede utilizar con hardware de radiofrecuencia externo de bajo coste disponible para crear radios definidas por software, o sin hardware en un entorno de simulación(Reyland, 2023). Se utiliza ampliamente en la investigación, la industria, el mundo académico, el gobierno y los entornos de aficionados para apoyar tanto la investigación de las comunicaciones inalámbricas como los sistemas de radio del mundo real (Aranda, 2019).

2.4 Metodología Ofensive Security

Offensive Security es una metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad. Esta metodología se enfoca en la explotación real de las plataformas y es altamente intrusiva.

Las etapas de implementación de la metodología Offensive Security como ya se lo planteado en apartado del alcance posee 5 etapas como se puede identificar en la Figura 9. En el contexto de las comunicaciones inalámbricas, esta metodología puede ayudar a identificar vulnerabilidades en las redes inalámbricas y proponer soluciones para optimizar la seguridad y el control de acceso (Briceño, 2021).A continuación, se detallan los pasos que posee la metodología:

Figura 9

Fases de la metodología Offensive Security

Fuente: Adaptado del sitio web: https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

- Recolección de la información: Este proceso implica la exploración meticulosa de fuentes públicas y privadas para obtener una comprensión bibliográfica de las tecnologías utilizadas y los posibles factores del ataque (Isaza Villar, 2014).
- Análisis de vulnerabilidades: Para la segunda fase se examinan detenidamente los activos identificados en la fase uno para identificar debilidades potenciales en su seguridad. Esto puede implicar el uso de herramientas especializadas de escaneo y análisis de señales inalámbricas (Isaza Villar, 2014).
- Definición de objetivos secundarios: Para la tercera fase se procede a la definición de objetivos secundarios. Esta etapa implica establecer metas específicas que ayuden a realizar el objetivo principal, para este caso se tiene como metas el poder vulnerar los dispositivos mediante el uso de dispositivos analizadores de espectro (Isaza Villar, 2014).
- Ataques: Para la cuarta fase es donde se ejecutan las acciones planificadas para comprometer la seguridad del sistema objetivo. En la cual se procede a verificar todas las vulnerabilidades que puede tener el uso de sistemas automáticos (Isaza Villar, 2014).
- Análisis final y Documentación: Como última fase se lleva a cabo el análisis de resultados para evaluar el éxito del ejercicio de seguridad ofensiva. Se examinan las acciones realizadas, los sistemas comprometidos y la información obtenida para identificar las vulnerabilidades detectadas(Isaza Villar, 2014).

2.4.1 Herramientas y técnicas en Ofensive Security

Offensive Security ofrece un conjunto de herramientas o soluciones que tienen como objetivo identificar en tiempo real el grado de exposición que tiene una organización y cómo afectaría en cualquier incidente que se produjera. Algunas de las herramientas más utilizadas en las pruebas de penetración incluyen (Devoteam, 2022).

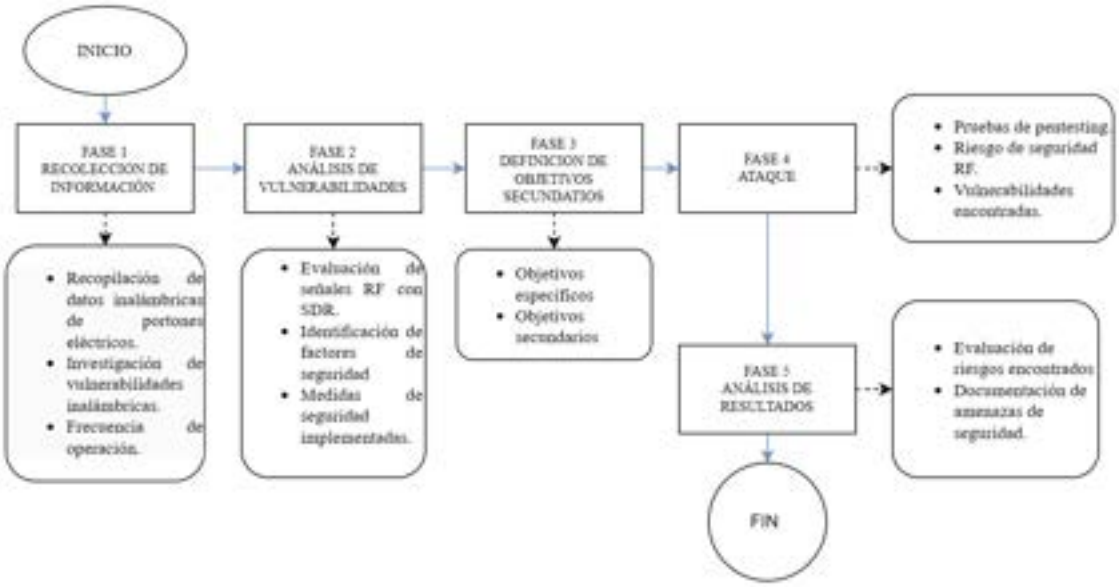
- Kali Linux**:** Un sistema operativo diseñado para pruebas de penetración y auditorías de seguridad.
- Metasploit: Un marco popular para desarrollar y ejecutar exploits contra objetivos remotos.
- Wireshark: Un analizador de protocolos de red para capturar y analizar el tráfico de red.
- Nmap: Una herramienta para escanear redes y descubrir hosts y servicios.

3 CAPÍTULO III. METODOLOGIA

En el tercer capítulo, se detalla el marco metodológico que se guiará esta investigación, el cual se fundamenta en el enfoque de Seguridad Ofensiva, también conocido como Offensive Security, como se ilustra en la Figura 10. Este enfoque se distingue por la realización de pruebas de penetración éticas, las cuales se llevarán a cabo en entornos reales y controlados. El propósito de estas pruebas es identificar y explotar posibles vulnerabilidades presentes en el uso de dispositivos automáticos para puertas. Para lo cual también se establecerán los requerimientos necesarios para cumplir con los respectivos objetivos establecidos para garantizar el éxito de la investigación.

Figura 10

Fases de la metodología Offensive Security



Fuente. Autoría

Dentro de las fases que se plantean realizar se encuentran establecidos varios puntos importantes que tendrá cada una de ellas, como se puede visualizar en la Figura 8. Entre ellos, los puntos críticos para la investigación serán la fase 2 y la fase 4, en las cuales se determinarán y simularán escenarios para encontrar las posibles vulnerabilidades en los dispositivos. Estos escenarios se establecerán de acuerdo con los requerimientos para cada caso de investigación de su respectiva vulnerabilidad.

3.1 Establecimiento de requisitos

Para el cumplimiento del siguiente apartado se establece las bases de los requerimientos necesarios para el proyecto, los cuales ayuden al cumplimiento de todos los objetivos que se plantearon desde un inicio en los capítulos anteriores. Esto se lo realiza para reconocer cada una de las necesidades encontradas, en este sentido se utilizará la norma ISO/IEC/IEEE 29148 como marco de referencia para poder definir tantos los requisitos del sistema de manera sistemático y estructura.

El uso de este estándar sirve como una guía detallada para el análisis de procesos técnicos, que van desde la definición del problema y el objetivo del sistema, hasta la identificación de las partes interesadas en conjunto con la especificación de requisitos funcionales. En este caso, se evalúan cada uno de los escenarios y sus respectivos SDR en cada uno de los casos de estudio. Por lo tanto, según el estándar, se identifican requisitos clave para los dispositivos SDR, los cuales incluirán la capacidad de analizar las frecuencias dentro del espectro electromagnético, así como también la habilidad para detectar vulnerabilidades que tendrá cada dispositivo.

3.1.1 Nomenclatura de requerimiento

La norma ISO/IEC/IEEE 29148 establece una nomenclatura estandarizada para identificar y organizar los requisitos de manera clara y consistente. Esta nomenclatura consta de varios componentes que proporcionan información sobre el tipo de requisito, su categoría y su nivel jerárquico dentro de la estructura del proyecto de investigación. Al utilizar esta nomenclatura establecida, se facilita el análisis y la gestión de los requisitos necesarios para el desarrollo del proyecto en lo cual se detalla a continuación.

- **SrRS:** Especificación de requerimientos por las partes interesadas.
- **SrRE:** Especificación de requerimientos para los escenarios de prueba.
- **SrRSo:** Especificación de requerimientos del software.
- **SrRH:** Especificación de requerimientos del hardware.

3.1.2 Stakeholders

Según la norma ISO/IEC/IEEE 29148, uno de los aspectos fundamentales del proceso de ingeniería de requisitos es la identificación y definición de stakeholders las cuales son las partes interesadas. En el proyecto en cuestión se consideran los distintos actores involucrados y estos se ordenarán según una secuencia jerárquica establecida como se identifica en la Tabla 3. Es importante identificar y definir adecuadamente a estas partes interesadas para comprender completamente los requisitos del proyecto y garantizar que sus necesidades y expectativas se cumplan adecuadamente.

Tabla 3

Establecimiento de las partes interesadas

N °	Stakeholders	Descripción
SrRS1	Ing. Jorge Jacome Logacho	Técnico en instalación de portones eléctricos
SrRS3	Ing. Pedro Terán	Técnico en instalación de portones eléctricos
SrRS2	Eduardo Vivar	Presidente del Conjunto Ciudad del Sol
SrRS4	Ing. Fabián Cuzme, MSc	Tutor del trabajo de grado
SrRS5	Ing. Luis Suárez, MSc.	Asesor
SrRS6	Smith Tandayamo	Autor

Nota. Se establecen las personas involucradas en el proyecto de investigación

3.1.3 Requerimiento de los escenarios

Dentro de los requerimientos del escenario, se establece la nomenclatura de SrRE la cual proporciona una estructura estandarizada para la documentación de los requisitos. En la Tabla 4 se presenta una visión general de los requerimientos que debe cumplir cada uno de los escenarios en los que se plantea realizar las pruebas de pentesting. Estos requerimientos se encuentran organizados de acuerdo con su prioridad, representada por un número de identificación único. Además, se definen las restricciones o limitaciones que puedan afectar el análisis de posibles vulnerabilidades del sistema.

Tabla 4

Requerimientos de los escenarios de pruebas

Nro.	Requerimiento	Prioridad		
		Alta	**Media**	**Baja**
SrRE1	El sistema debe tener la capacidad de operar dentro del umbral del espectro electromagnético requerido para analizar las frecuencias inalámbricas utilizando por los dispositivos analizadores de espectro.	X		
SrRE2	Dentro de los escenarios de prueba se debe identificar y reportar vulnerabilidades de seguridad en los sistemas de control de acceso basados en frecuencias inalámbricas.		X	
SrRE3	Se debe tener consentimiento de la persona responsable del sistema para realizar las pruebas de vulnerabilidades.	X		
SrRE4	Se debe mantener la confidencialidad de la información obtenida durante el análisis de vulnerabilidades encontradas durante las pruebas de penetración.	X		
SrRE5	Dentro de los escenarios de prueba de debe verificar que los sistemas automáticos estén funcionando correctamente con el uso del mando inalámbrico.			X

Nota. El establecimiento de los requerimientos presentados en la Tabla 4 proporciona un marco sólido para la realización de cada una de las pruebas de penetración en los diferentes escenarios planteados. Se debe tener en cuenta el uso adecuado de los dispositivos SDR y la confiabilidad de la información recopilada durante las pruebas.

3.1.4 Requerimientos del software

El siguiente punto de los requerimientos para el desarrollo de la investigación implica la selección cuidadosa del software adecuado. En esta etapa, se establecen diversos parámetros cruciales para elegir la mejor opción de software que se ajuste a

las necesidades del estudio, estos aspectos están identificados en la Tabla 5. Entre estos parámetros, es fundamental considerar que las aplicaciones sean capaces de operar dentro del rango del espectro electromagnético utilizado por los mandos inalámbricos.

Asimismo, es necesario que las aplicaciones brinden soporte para los distintos dispositivos SDR que se emplearán a lo largo de las pruebas de penetración. Es crucial destacar que estas herramientas deben permitir el análisis de la señal capturada de la trama de bits transmitida por los dispositivos, lo que posibilitará comprender el funcionamiento de los mecanismos de las puertas eléctricas accionadas por dichos mandos.

Además, es esencial que las aplicaciones estén disponibles para el sistema operativo Linux, especialmente para la distribución Kali Linux. Dado que la metodología a emplear para realizar las pruebas se basa en Kali Linux, la compatibilidad con este sistema operativo garantizará la integridad y eficacia de las pruebas realizadas en el contexto de la investigación. En este caso se establece las siglas SrRSo de acuerdo con la norma ISO/IEC/IEEE 29148 en la que se estableció para su nomenclatura de software.

Tabla 5

Requerimiento de software a emplear durante la investigación

Nro.	Requerimiento	Prioridad		
		Alta	**Media**	**Baja**
SrRSo1	Herramientas para escanear y analizar redes inalámbricas dentro del umbral de funcionamiento de los portones eléctricos.	X		
SrRSo2	Aplicaciones que permiten capturar la señal enviada por los mandos de los portones eléctricos.	X		
SrRSo3	Herramientas que puedan evaluar la señal enviada por los sistemas de portones eléctricos.		X	
SrRSo4	Programa que pueda funcionar tanto en sistemas operativos de Windows y Kali Linux.		X	
SrRSo5	Herramientas que tengas soporte para interactuar con los dispositivos SDR planteados.	X		
SrRSo6	Herramienta que pueda funcionar como transmisor de un mando inalámbrico		X	
SrRSo7	El programa debe ser open source para el fácil acceso de sus funciones.			X

Nota. Los criterios para la selección del software apropiado incluyen la capacidad de operar en el espectro electromagnético utilizado por los mandos inalámbricos, el soporte para SDR, la capacidad de análisis de señales y la disponibilidad para el sistema operativo Linux, en particular Kali Linux

3.1.5 Aplicaciones de software a utilizar de acuerdo con los requerimientos de software

Una vez que se han definido los parámetros que cada aplicación debe cumplir, se lleva a cabo una cuidadosa evaluación entre los diferentes programas disponibles. En este proceso, se considera detenidamente cuál sería la opción más adecuada al

momento de realizar el análisis de vulnerabilidades. En este caso se establecerá las aplicaciones en Tabla 6 que se plantea utilizar y su respectiva calificación.

Tabla 6

Calificación de los programas de acuerdo con los requerimientos de software

Herramientas	**GNU RADIO**	**MATLAB**	**AUDACITY**	**GQRX**	**SDRSharp**
SrRSo1	X	X	-	X	X
SrRSo2	X	-	-	X	X
SrRSo3	-	-	X	-	-
SrRSo4	-	-	X	X	-
SrRSo5	X	X	-	X	X
SrRSo6	-	X	-	-	-
SrRSo7	X	-	X	X	X
TOTAL	4	3	2	5	4

Nota. Considerando los requisitos planteados para la investigación, se identifica que la herramienta GQRX como la opción óptima para llevar a cabo las pruebas de vulnerabilidad. Esta elección se fundamenta en varios factores de acuerdo con la Tabla 6, entre los que destaca su accesibilidad y facilidad de instalación en entornos Linux.

GQRX ofrece una interfaz intuitiva que permite identificar y analizar señales inalámbricas en tiempo real, lo que resulta fundamental para el análisis de sistemas de portones eléctricos. De igual manera se puede establecer una frecuencia central en la que funcionan los mandos con un ancho de banda adecuado para poder guardar la secuencia de bits en un archivo wav.

En este caso, se tienen como segunda opción, de acuerdo con el puntaje, las aplicaciones GNU-Radio y SDRSharp. Estos programas comparten muchas características similares para analizar las señales del espectro de los controles inalámbricos, pero se escoge la opción de GNU-Radio debido a que también puede funcionar en entornos Linux.

Además de GQRX, se ha decidido utilizar MATLAB para la transmisión de datos debido a su facilidad de programación y versatilidad. MATLAB ofrece un entorno de desarrollo robusto que permite manipular todos los aspectos del código y analizar los datos de manera eficiente.

Como última aplicación requerida se encuentra Audacity, que, de acuerdo con el número de requerimiento SrRSo3, es la única aplicación capaz de identificar y manipular archivos de audio WAV. Estos archivos contendrán las tramas de bits de las señales inalámbricas de los mandos de portones eléctricos.

3.1.6 Requerimientos del hardware

Para el establecimiento del hardware que se deberá tener se debe considerar de igual manera la norma para la nomenclatura de cada uno de los puntos que en este caso es las SrRH. Dentro de estos requerimientos, se destaca la alta prioridad de que los dispositivos sean capaces de interceptar las señales inalámbricas emitidas por los mandos, así como de transmitir dichas señales para posibles ataques. Esta capacidad es fundamental para simular escenarios y evaluar la seguridad de los sistemas de portones eléctricos.

Además, es crucial que los dispositivos seleccionados cuenten con los controladores necesarios para su correcto funcionamiento con los programas elegidos anteriormente, todos estos aspectos están identificados en la Tabla 7. Estos controladores facilitan la comunicación entre el hardware y el software, permitiendo un uso eficiente de los dispositivos durante el análisis de vulnerabilidades.

Tabla 7

Establecimiento de los requerimientos de hardware

Nro.	Requerimiento	Prioridad		
		Alta	**Media**	**Baja**
SrRH1	El dispositivo SDR debe ser capaz de operar en las frecuencias utilizadas por los mandos de portones.	X		
SrRH2	El dispositivo debe tener la capacidad de poder transmitir señales inalámbricas.	X		
SrRH3	El dispositivo debe tener la capacidad de poder receptar las señales enviadas por los mandos inalámbricos.	X		
SrRH4	Debe contar con interfaces de conexión compatibles con la computadora.		X	
SrRH5	Es importante que el dispositivo sea compatible con el software de análisis utilizado para la investigación.		X	
SrRH6	El dispositivo debe ser de fácil acceso al público al instante de poder adquirirlo.			X
SrRH7	El dispositivo debe contar con una antena externa para tener mayor ganancia de la señal tanto transmitida como recibida.			X
SrRH8	Fácil uso para los usuarios y como de programabilidad.		X	
SrRH9	El dispositivo debe ser capaz de funcionar solo sin ningún complemento extra.		X	

Nota. Se establecen los principales requerimientos de hardware que debe cumplir el dispositivo SDR para realizar un análisis efectivo de vulnerabilidades en sistemas de portones eléctricos.

3.1.7 Dispositivos de hardware a utilizar de acuerdo con los requerimientos

Una vez establecidos los requerimientos que deben tener cada uno de los dispositivos, se procede a listar cada uno de ellos dentro de la Tabla 8 con su respectiva calificación. La elección del hardware adecuado no solo implica consideraciones técnicas que cada uno posea, sino también sobre las necesidades que tiene el proyecto de investigación para realizar los respectivos ataques.

Tabla 8

Calificación de los dispositivos de acuerdo con los requerimientos de hardware

Hardware	Adalm-Pluto	RTL-SDR	Flipper Zero
SrRH1	X	X	X
SrRH2	X	-	X
SrRH3	X	-	X
SrRH4	X	X	X
SrRH5	X	X	-
SrRH6	-	X	-
SrRH7	X	X	X
SrRH8	-	-	X
SrRH9	-	-	X
TOTAL	6	5	7

Nota. Se establece la calificación que tendrá cada uno de los dispositivos de acuerdo con los requerimientos anteriormente establecidos.

Flipper Zero destaca como un dispositivo con un potencial excepcional para el análisis de vulnerabilidades en sistemas de portones eléctricos. Su capacidad para

interceptar y replicar de manera eficiente las señales emitidas por los mandos inalámbricos lo posiciona como una herramienta sumamente útil. En comparación con otros dispositivos SDR listados en la Tabla 8, donde se especifica que solo este dispositivo cuenta con los puntos SrRH8 y SrRH9, que permiten realizar ataques de manera sencilla y autónoma sin necesidad de estar conectado a un ordenador, Flipper Zero obtiene una calificación superior debido a su versatilidad y facilidad para ejecutar tareas de análisis de vulnerabilidades.

Por otro lado, el hardware Adalm-Pluto es una opción especialmente poderosa para este tipo de análisis. Su versatilidad y capacidad de programación lo convierten en una herramienta robusta. Su estructura electrónica única le permite tanto interceptar como emitir señales, lo cual lo distingue de otros dispositivos SDR como el RTL-SDR. Esta capacidad de enviar señales es crucial para llevar a cabo pruebas de penetración y simular escenarios de ataques a los sistemas de portones eléctricos, permitiendo evaluar de manera más completa las vulnerabilidades existentes.

De igual manera se tiene como tercer dispositivo el uso de RTL-SDR que en este caso tiene el puntaje más bajo en comparación de otros dispositivos hardware. En comparación con los otros dispositivos SDR posee su principal ventaje que es su bajo costo, lo cual hace asequible para este tiene de investigaciones.

3.2 Fase 1: Recolección de información

En la fase inicial de la metodología se realiza la identificación de las distintas características que posee los sistemas de portones eléctricos, como son los rangos de frecuencias de operación que pueden ir variando, dependiendo del modelo del equipo

las cuales poseen distintas características inalámbricas. También se evalúa los distintos mecanismos que interactúan en la ejecución del sistema, ya que algunos son dispositivos más actuales que otros y esto puedo desembocar a posibles riesgos en su uso diario.

3.2.1 Identificación de sistemas de portones eléctricos y sus características.

Los sistemas de portones eléctricos representan una innovación significativa en el ámbito de la seguridad y la comodidad para propiedades residenciales. Estos sistemas ayudan automáticamente en la apertura y cierre del portón, lo cual ofrecen a los usuarios una forma conveniente de controlar el acceso a sus espacios sin la necesidad de intervención manual. Dentro de sus diferentes características que existen dentro de estos sistemas se tiene las que son comerciales y las que son con respecto a los sistemas de microcontroladores que son usadas para la apertura de los portones.

3.2.1.1 Características Comerciales de los portones

Estos sistemas están equipados con controles remotos fáciles de usar, los cuales garantizan una operación eficiente desde el interior de los vehículos o a su vez desde la comodidad del hogar. Además, algunos dispositivos más actuales poseen características de nuevas generaciones, como son: sensores de obstáculos y funciones de reversión automática, para proteger contra posibles accidentes o en este caso para lo que se está realizando la investigación evitar el ingreso de intrusiones no deseadas(Tanaka et al., 2018).

Como se puede identificar en la Figura 2 los principales componentes que posee los portones eléctricos y que se tomara en cuenta son el motor, llaves de desbloqueo y dispositivo receptor. El dispositivo receptor posee diferentes configuraciones de códigos de acuerdo con las necesidades del usuario, tanto que se puede programar diferentes acciones para cada código. Se puede programar el receptor para que abra la puerta del garaje al presionar un botón en el control remoto, abra el portón al presionar otro botón y encender las luces al presionar un tercer botón (Tanaka et al., 2018). De acuerdo con la investigación realiza se tiene las principales características que tiene estos dispositivos y se ofrecen a nivel comercial y de igual manera se establecen sus diferentes características en las Tabla 9:

- Tiempo de apertura (S)
- Peso máximo (kg)
- Alimentación (V AC)
- Ciclos (Constante)

Tabla 9

Características comerciales de portones eléctricos

Característica	Rango Mínimo - Máximo	Unidad	Descripción
Tiempo de apertura	5 - 15	Segundos	Tiempo que tarda el portón en abrirse completamente.
Peso máximo	300 - 2000	Kilogramos	Peso máximo que el motor del portón puede soportar.
Alimentación	110 - 220	Voltios AC	Voltaje de corriente alterna que requiere el motor del portón para funcionar.
Ciclos (Constante)	20 - 50	Por hora	Número de veces que el portón puede abrirse y cerrarse por hora sin sobrecalentarse.

Nota. Rango de valores generales sobre las características de portones eléctricos.

De acuerdo con los usuarios, se establecen diferentes características según sus necesidades en las cuales se puede identificar en la Tabla 9. En este caso, se han tenido en cuenta cuatro aspectos que son los que más llaman la atención a los usuarios. Estos van desde el tiempo que tarda en abrirse completamente el portón eléctrico, hasta el peso que la puerta tendrá para que el motor pueda moverla sin mucho esfuerzo (Tanaka et al., 2018).

La alimentación eléctrica necesaria para poner en marcha el mecanismo depende de si es a 110 o 220 voltios en corriente alterna (AC). Por último, se consideran los ciclos del mecanismo, que hacen referencia a cuántas veces pueden ser accionados los portones sin que sufran daños en el futuro (Tanaka et al., 2018).

3.2.1.2 Características de los sistemas de portones eléctricos

Dentro de los sistemas utilizados por los portones eléctricos, se encuentran diferentes características que poseen las placas. Estas se identifican en la Tabla 10, donde se menciona el entorno de desarrollo en el que se programa su código fuente, así como los diversos lenguajes de programación que se utilizan comúnmente para estas tareas. También se detalla la capacidad de memoria que pueden alojar estos sistemas. De igual manera, se enumeran los microcontroladores que se emplean habitualmente en los portones eléctricos.

Tabla 10

Descripción de características de los sistemas de portones

Característica	Descripción	Ejemplo
Entorno de programación	IDE utilizadas para la programación de las placas de los microcontroladores.	MPLAB IDE, AVR Studio
Capacidad de Memoria	Cantidad de memoria disponible en el microcontrolador que se utiliza para almacenar el firmware del sistema.	8,32,128 KB (kilobytes)
Lenguaje de Programación	El lenguaje de programación que se utiliza para escribir el código fuente del firmware.	Ensamblador Lenguaje, C++
Interfaces de Comunicación	Permiten que la tarjeta inalámbrica se conecte e intercambie datos con otros componentes del sistema, como sensores o actuadores.	UART, SPI, I2C
Microcontroladores	Circuito integrado o chip de programación en donde se almacena el código de programación de los dispositivos embebidos.	• Microchip PIC (PIC16F, PIC18F) • Atmel AVR (ATmega, ATtiny) • ARM Cortex-M • Renesas RL78

Nota. Ejemplos de los componentes y características usadas por los sistemas de portones eléctricos.

3.2.2 Recopilación de datos sobre las características de la tarjeta receptora del portón eléctrico.

Dentro del análisis realizado y la recolección de información recopilada durante la evaluación de los distintos dispositivos, es notable la particularidad de que estos sistemas operan mediante una tarjeta receptora de radio. Dicha tarjeta recibe la señal inalámbrica del control remoto y procede a activar la apertura del portón eléctrico. Si esta tarjeta no está incorporada dentro del mecanismo, no existe posibilidad que la puerta se abra. Estas tarjetas poseen diversas características para su

funcionamiento, las cuales varían dependiendo de la marca y, a su vez, de si son más nuevas o antiguas. En la Tabla 11 se detallan las distintas características que presentan estos dispositivos.

Dentro de los datos recopilados, tanto de manera bibliográfica en el Capítulo 2 como en el momento de investigar las características de los sistemas que serán objeto de estudio, se elaboró la siguiente Tabla 11.

Tabla 11

Características generales que posee un mando de portón eléctrico

Características	Valor	Descripción	Unidad
Alimentación	5	Voltaje de funcionamiento	Voltios DC
Temperatura	-10 a 55	Rango de temperatura ambiente	°C
Numero de canales	1 a 4	Número de transmisores que puede recibir	
Codificación	(Código fijo – Código variable)	Tipo de código	
Modulación	AM/ASK	Tipo de modulación	
Frecuencia portadora	± 433.92	Frecuencia de operación	MHz
Códigos	50	Número de códigos que puede almacenar	
Impedancia	50	Impedancia de la antena	
Sensibilidad	-107	Sensibilidad del receptor	dBm

Nota. Rango que se encuentran en distintos dispositivos de controles inalámbricos de portones.

3.2.3 Recopilación de información sobre los controles originales y genéricos

Dentro de la información relevante sobre el funcionamiento de los mecanismos de portones eléctricos, es crucial investigar los dispositivos que funcionan como actuadores. En el mercado, existen diversos mandos que pueden ser utilizados según las necesidades específicas de los usuarios y de igual manera la característica que puede tener el sistema, ya que no todos los mandos pueden funcionar correctamente con las diferentes marcas del mercado.

3.2.3.1 Mandos inalámbricos originales

Los dispositivos electrónicos de control de puertas suministrados por los fabricantes de sistemas están diseñados para garantizar un funcionamiento seguro y eficiente. Estos dispositivos tienen protocolos de comunicación confiables y mecanismos de seguridad integrados (Pujol, 2023). La principal razón es proteger la integridad de la señal transmitida y evitar el acceso no autorizado. Los controles originales están diseñados para funcionar bien con receptores compatibles.

Una de las principales características sobre estos controles, es el uso de algoritmos de cifrado avanzados para garantizar la confidencialidad de las comunicaciones entre el controlador y el host. Estos algoritmos de cifrado están diseñados para proteger contra la piratería y otros métodos de descifrado, proporcionando una capa adicional de seguridad (Pujol, 2023).

Otra ventaja de los dispositivos preinstalados es su capacidad de tener nuevas funciones y funciones de seguridad. Los desarrolladores siempre están buscando vulnerabilidades y amenazas emergentes y proporcionando nuevo software para

mitigar estos riesgos. Esto asegura la continuidad de las capacidades críticas. Y el sistema de salida electrónico está completamente protegido contra nuevas amenazas (Pujol, 2023).

3.2.3.2 Mandos inalámbricos genéricos

En este caso se tiene otro tipo de controles de acceso conocidos como mandos genéricos o universales, las cuales son desarrolladas por terceras empresas tratando de asemejar la versión original deseada. Estos dispositivos son creados a menudo para poder ser más económicos para los consumidores, aunque esto ocasión que pueden carecer de características de seguridad y funcionalidades comparables a las versiones originales (Pujol, 2023).

El principal problema de todas las versiones es la compatibilidad con los receptores del sistema portados. Porque no fue diseñado por el fabricante original. Por lo tanto, puede haber problemas de compatibilidad o interacción con otros sistemas. Otro aspecto importante de los controles universales es la falta de normas generales de seguridad. No todas las versiones tienen el mismo nivel de soporte y mantenimiento(Pujol, 2023). Esto puede ocasionar posibles vulnerabilidades de seguridad cuando surgen nuevas amenazas.

En base a las diferentes ventajas y desventajas que se tiene con el uso de mandos originales y genéricos se estableció la Tabla 12.

Tabla 12

Ventajas y desventajas de usar mandos originales o universales

Aspecto	Mandos Originales	Mandos Genéricos
Beneficios	Garantía de compatibilidad con el sistema	Costo generalmente más bajo
	Soporte técnico y servicio postventa del fabricante	Disponibilidad más amplia en el mercado
	Integración sin problemas con el receptor	Posibilidad de programación y configuración flexibles
	Cumplimiento de estándares de seguridad	Potencial para ofrecer características adicionales
Desventajas	Costo inicial más elevado	Posible falta de compatibilidad con algunos sistemas
	Limitada disponibilidad en el mercado	Menor calidad de construcción en algunos casos
	Dependencia del fabricante para actualizaciones	Soporte técnico y servicio postventa menos confiable
	Restricciones en la programación y configuración	Potenciales problemas de seguridad y autenticación
		Riesgo de comprar mandos no compatibles o defectuosos

Nota. Adaptado de (Pujol, 2023).

3.2.3.3 Características inalámbricas de mandos originales y genéricos

Se establecen las distintas características que presentan los mandos originales y los genéricos, los cuales desempeñan un papel importante en el correcto funcionamiento del mecanismo de apertura automática. La efectividad y la fiabilidad

de estos mandos dependen de diversas características inalámbricas, tales como la frecuencia de operación, la potencia de transmisión, el alcance y la seguridad(Kshetrimayum, 2009). En la Tabla 13 se especifican las principales características que estos mandos poseen, proporcionando una visión clara de sus capacidades y limitaciones.

Tabla 13

Características inalámbricas que poseen los mandos originales y genéricos

Característica	**Mando Original**	**Mando Genérico**
Frecuencia de Operación	Específica según la marca y modelo	Multifrecuencia, compatible con varias marcas
Rango de Frecuencia	433 MHz Estrecho (428-438 MHz)	433 MHz Amplio (423 – 444 MHz)
Potencia de Transmisión	10 - 20 mW	5 - 15 mW
Alcance	50 - 100 metros	30 - 80 metros
Método de Modulación	ASK/OOK específico de la marca	ASK/OOK adaptable

Nota. Adaptado de (Tanaka et al., 2018).

De acuerdo con la Tabla 13, se establecen las distintas características que diferencian entre un mando original y uno genérico. En particular, en la fila de Rango de Frecuencia, se observa que para un mando original su rango de operación estimado es de 428 a 438 MHz. En cambio, la frecuencia de operación de un mando genérico es mucho más amplia, abarcando desde 423 a 444 MHz, lo que le proporciona un mayor umbral para poder operar con distintas marcas comerciales. De igual forma se establece el alcance que estos dispositivos poseen tenían mayor distancia un mando original.

3.3 Fase 2: Análisis de vulnerabilidades

Para la fase 2 de la metodología se establece el análisis de vulnerabilidades que se tiene en los dispositivos automáticos, en lo cual se establecerán las diferentes vulnerabilidades o debilidades que tiene el uso de los controles inalámbricos. Estas vulnerabilidades pueden ser desde fabrica debido al tipo de dispositivo que se requiera instalar, la cual no tenga una buena tecnología para evitar ataques inalámbricos.

3.3.1 Falta de autenticación robusto

La ausencia de un mecanismo de autenticación sólido en el control de portones eléctricos representa una vulnerabilidad preocupante en la seguridad de estos sistemas. Algunos controladores utilizan códigos fijos o rodantes que pueden ser vulnerados fácilmente(Pedro J, 2023). Esta situación plantea un alto riesgo porque permite a posibles atacantes capturar y reproducir la misma señal RF por mandos ilegítimos, proporcionando así acceso no autorizado a las instalaciones. Esta vulnerabilidad es más crítica en entornos críticos como instalaciones industriales o comunidades residenciales donde la seguridad es importante.

Otra debilidad común en el control de portones eléctricos es la falta de cifrado o el uso de algoritmos de cifrado débiles. Cuando la comunicación entre el controlador y la puerta receptora carece de cifrado o utiliza métodos de cifrado débiles, como algoritmos de clave corta simétrica, los atacantes pueden interceptar y descifrar fácilmente los datos transmitidos. Este estado expone información confidencial, como

patrones de códigos de acceso o patrones de uso, comprometiendo seriamente la seguridad y la privacidad del sistema (Pedro J, 2023).

3.3.2 Cifrado débil o nulo

Otra debilidad común en el control de portones eléctricos es la falta de cifrado o el uso de algoritmos de cifrado débiles. Cuando la comunicación entre el actuador y la puerta receptora carece de cifrado o utiliza métodos de cifrado débiles los atacantes pueden interceptar y descifrar fácilmente los datos transmitidos. Esto expone información confidencial, como patrones de códigos de acceso como es la trama de bits que se envía, comprometiendo seriamente la seguridad y la privacidad del sistema. La implementación de un cifrado sólido garantiza la confidencialidad de las comunicaciones y protege los datos confidenciales contra la interceptación o el acceso no autorizado(Alfonso, 2022).

3.3.3 Falta de actualizaciones de seguridad

La falta de actualizaciones de seguridad regulares por parte de los fabricantes de mandos de portones eléctricos representa un riesgo significativo. A medida que surgen nuevas vulnerabilidades y técnicas de ataque, los dispositivos antiguos que no reciben parches de seguridad se vuelven cada vez más vulnerables. Los atacantes pueden aprovechar estas vulnerabilidades conocidas para obtener acceso no autorizado, comprometiendo la seguridad del sistema de control de acceso (Pedro J, 2023).

3.3.4 Riesgos de apertura mutua y vulnerabilidades de seguridad

Los sistemas de seguridad de los portones tienen fallas que permiten que se abran desde propiedades ajenas, incluso si el dueño legítimo no los activó. Esta vulnerabilidad puede ocurrir por errores en el diseño o al instante de la instalación de los sistemas. Los riesgos asociados a esta falla son preocupantes. Primero, existe el riesgo de que personas no autorizadas ingresen a tu propiedad al abrir el portón desde la casa vecina. Si un delincuente descubre esta vulnerabilidad, podría entrar fácilmente a tu hogar sin ser detectado, lo que aumenta las posibilidades de robos u otros delitos.

Además, esta situación compromete tu privacidad y la de tus vecinos. Al permitir el acceso no autorizado, se pone en riesgo la seguridad de quienes viven allí y de sus pertenencias.

3.3.5 Empleo de herramientas de escaneo de frecuencias inalámbricas.

En este caso se puede identificar que las frecuencias que operan los mandos inalámbricos de los portones son de 433.95 MHz como se documentó en la fase de recolección de información. Por lo tanto, se puede emplear un analizados de espectro (SDR) para identificar el espectro generado al instante de accionar el mecanismo.

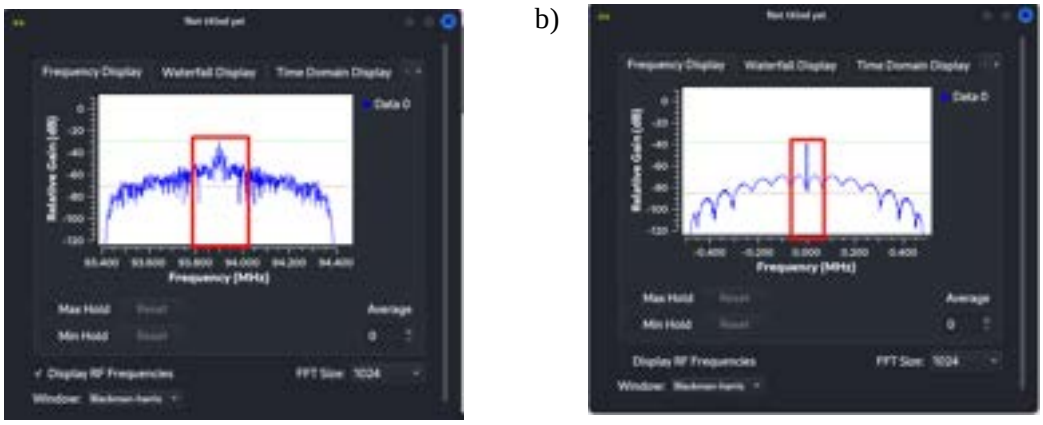
Como resultado se tiene que mediante el uso de estos dispositivos se puede obtener la información sobre los paquetes que se envían al momento de iniciar el mecanismo, mediante el uso del software de GNU-Radio como se puede identificar en la Figura 11a representa la señal de un mando inalámbrico genérico, mientras que la

Figura 11b es de una señal de un mando original en la cual se puede distinguir que tiene menos ruido de transmisión.

Figura 11

Captura del espectro de un mando inalámbrico genérico y original

a) b)



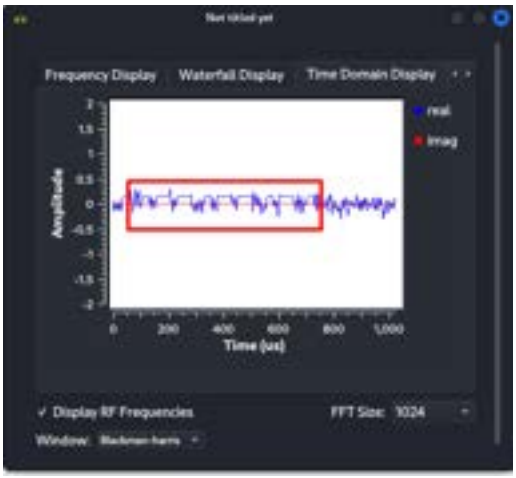
Nota: a) Señal de un mando genérico b) Señal de un mando inalámbrico original

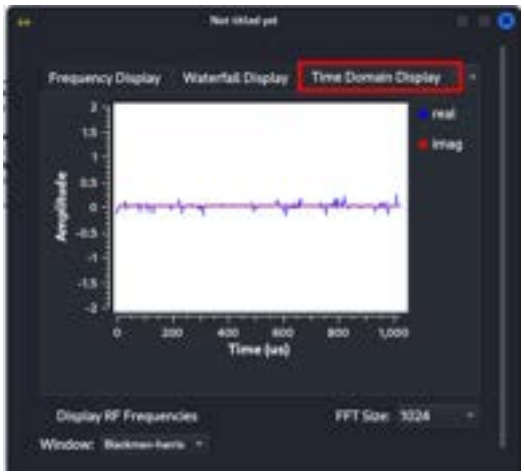
En una breve exploración sobre sobre la transmisión de datos del mando inalámbrico, se puede identificar que la señal enviada hacia el motor de un portón eléctricos puede ser interceptada por los dispositivos SDR, lo cual ocasiona cierto riesgo de vulnerabilidad sobre los datos enviados, como se puede identificar en la Figura 12a.

La señal que se puede lograr capturar en el dominio del tiempo es más evidente los bits de datos que son transmitidos por un mando genérico, caso contrario es mucho más difícil poder identificar los patrones de bits en un mando original como se puede identificar en el Figura 12b.

Figura 12

Pantalla sobre los datos en el dominio del tiempo

a) 

b) 

Nota: a) Señal de un mando genérico b) Señal de un mando inalámbrico original.

3.4 Fase 3: Definición de objetivos secundarios

Para la fase 3 se establecen lo que son los objetivos secundarios que se plantearon para el proyecto de investigación.

3.4.1 Objetivos específicos

- Recopilar datos sobre redes inalámbricas en portones automáticos para identificar vulnerabilidades.
- Evaluar posibles vulnerabilidades mediante pruebas de penetración con dispositivos interceptores de señales SDR.
- Implementación de principios y pautas de Offensive Security para proporcionar recomendaciones de seguridad sobre el uso de estos dispositivos.

3.4.2 Objetivos secundarios

Se establecen los objetivos secundarios que se tendrá para el análisis de vulnerabilidades de los portones eléctricos.

- Identificar los distintos tipos de dispositivos de portones eléctricos de diferentes marcas usadas, incluyendo sus especificaciones técnicas y métodos de comunicación inalámbrica utilizados.
- Analizar los protocolos de comunicación inalámbrica empleados por los dispositivos de portones eléctricos, identificando posibles vulnerabilidades en su diseño y configuración.
- Realizar técnicas y herramientas utilizadas por los posibles atacantes para comprometer la seguridad de los sistemas.
- Establecer pautas y recomendaciones de seguridad específicas para mejorar la protección de los sistemas de portones eléctricos tomando en consideración a las marcas vulneradas.

3.5 Fase 4: Ataque

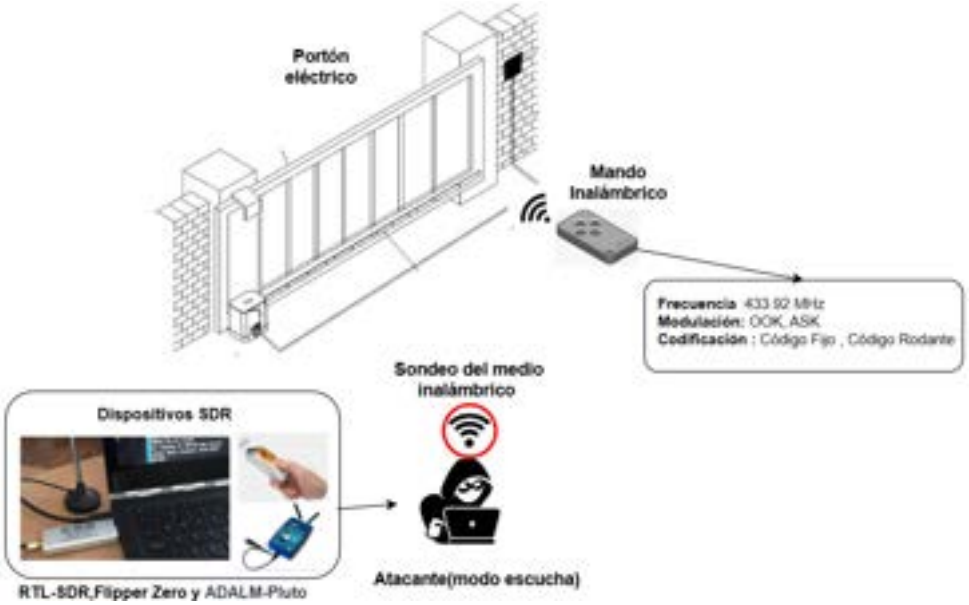
En la fase 4 se realizarán todos los ataques de penetración o intercepción de las señales inalámbricas de los mandos inalámbricos. Para ello, se llevarán a cabo pruebas en distintos puntos donde se haga uso de dichos dispositivos, con el fin de obtener una muestra más amplia sobre qué dispositivos son más seguros que otros.

3.5.1 Planteamiento del escenario de ataque

Para el planteamiento del escenario de ataque, se dispone del uso de los dispositivos SDR. Estos dispositivos se configurar en modo de escucha con el objetivo de capturar las señales inalámbricas emitidas por los mandos a distancia cuando se accionen los motores de los portones eléctricos. Una vez que los portones entren en funcionamiento al ser activados por los mandos inalámbricos, los dispositivos SDR estarán en condiciones de interceptar y registrar las transmisiones de radiofrecuencia. Este proceso permitirá analizar en detalle el comportamiento y las características de las señales inalámbricas empleadas por estos sistemas de control remoto, con el fin de identificar posibles vulnerabilidades y evaluar su nivel de seguridad. Este escenario se puede visualizar de mejor manera en la Figura 13. Todos los ataques generados fueron aprobados y supervisados por los dueños de los portones eléctricos como se evidencia en al Anexo C.

Figura 13

Planteamiento del escenario de ataque



Nota. Creación del planteamiento del escenario de prueba de vulnerabilidades para cada uno de los ataques.

Uno de los aspectos importantes que se deben tomar en consideración son las características inalámbricas que poseen los mandos a distancia y los portones eléctricos. Un factor clave es la frecuencia de operación, que en este caso se encuentra dentro del rango de los 433.92 MHz. Todos los dispositivos de radio definida por software (SDR) utilizados en el escenario de ataque deberán configurarse para operar en esta frecuencia específica, con el fin de poder interceptar y decodificar correctamente las señales transmitidas.

Además, resulta fundamental establecer la modulación adecuada en los dispositivos SDR, ya que esta determina la forma en que se codifican los datos en la onda portadora.

3.5.2 Ataque 1: Uso del dispositivo Flipper Zero

En el caso del primer ataque, se utilizará el dispositivo Flipper Zero, el cual deberá tener actualizado y flasheado el firmware más adecuado para las necesidades del proyecto. Esto se debe a que en diferentes regiones existen restricciones en el uso de ciertas porciones del espectro electromagnético, lo que podría arrojar un error de frecuencia no permitida en la región 9 a la que pertenece Sudamérica. Para evitar este inconveniente, se ha cargado en el dispositivo un firmware que habilita todas las frecuencias a nivel mundial, independientemente de las limitaciones regionales como se muestra en la siguiente Figura 14.

Figura 14

Actualización del dispositivo Flipper Zero

Nota. Interfaz de inicio de la aplicación de Flipper Zero.

Dentro de las opciones del dispositivo que deberá ir al apartado de Sub-GHz para poder comenzar con las pruebas de vulnerabilidades como se puede identificar en la Figura 15. Dentro de esta opción se podrá realizar todos los ataques dentro del rango de los Sub-GHz que diversos aparatos funcionan.

Figura 15

Opción de Sub-GHz

Es necesario determinar las características que poseen los portones eléctricos, específicamente la frecuencia central de operación y el tipo de modulación utilizado, con el fin de poder capturar las señales de manera más eficaz. En la Figura 16 se

identifica la frecuencia y la modulación que se utilizara, para lo cual es importante poder identificar cual es la frecuencia central en que se maneja cada marca para transmitir la señal.

Figura 16

Establecimiento de la modulación y frecuencia de operación

Se procede a escáner la señal enviada por los mandos que de acuerdo con la distancia en que se encuentre esta señal será más intensa, con esto se puede verificar que el mando está funcionando en la frecuencia establecida anteriormente, donde se encuentra representado en la Figura 17. Mientras más intensa sea la ganancia de la antena se podrá capturar de mejor manera la señal transmitida.

Figura 17

Escaneo de la señal enviada por el mando inalámbrico

En la siguiente opción, se procede a capturar la señal en forma de bits de datos para poder almacenarlos en la memoria del dispositivo. Como se puede identificar en la Figura 18, cada vez que se pulsa un botón del mando, se captura una trama de bits dentro del dispositivo, en donde se puede capturar todos los botones que posee el control si estos llegaran a ser accionados simultáneamente.

Figura 18

Captura de señal inalámbrica

En este caso se procede a replicar la señal captura con el fin de lograr abrir el portón automático de una manera no autorizada, como se puede identificar la Figura 19 el dispositivo comienza a transmitir la señal captura en la misma frecuencia central almacenada dándole clic en el botón de central.

Figura 19

Ataque con el dispositivo Flipper Zero

Para finalizar el proceso, se comienza a explorar la vulnerabilidad existente en los sistemas, verificando si el portón puede ser accionado ilegítimamente por un usuario no autorizado, como se evidencia en la Figura 20.

Figura 20

Ataque realizado con el dispositivo Flipper Zero

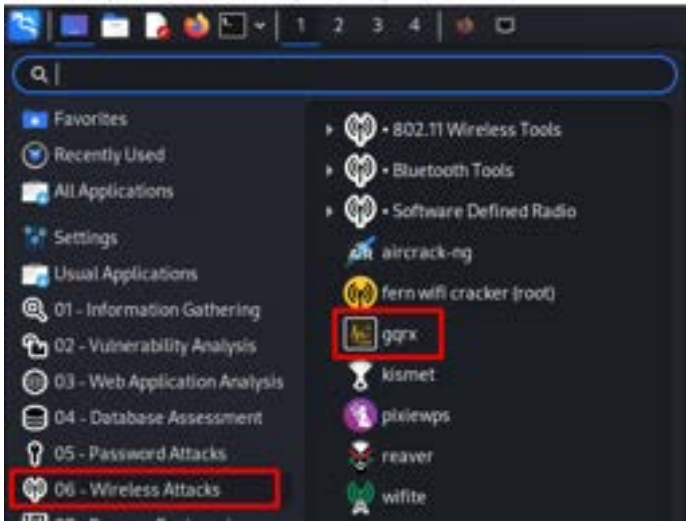
3.5.3 Ataque 2: Uso del dispositivo RTL-SDR

Aplicando la metodología de Offensive Security, se establece que las pruebas de ataque deben realizarse con el uso de herramientas de Kali Linux. En este caso, se tiene como primer programa planteado, como parte del requerimiento de software, el uso de GQRX, el cual no viene instalado con los complementos de inicio de Kali Linux. Este programa debe descargarse e instalarse desde los repositorios oficiales.

Dentro de las distintas opciones que ofrece el Sistema Operativo, se escoge la opción de Wireless Attacks como se identifica en la Figura 21, en la cual se encuentra el programa antes mencionado para comenzar con las pruebas de penetración.

Figura 21

Software GQRX en el entorno de Kali Linux



Para poder configurar el programa, primero se debe establecer la frecuencia de operación en la que se plantea realizar el análisis como se identifica en la Figura 22. En este caso, esa frecuencia es también denominada la frecuencia central, por lo general, para la detección de las señales inalámbricas de los mandos, está operando alrededor de los 433.950 MHz.

Figura 22

Establecimiento de la frecuencia central

La sección de Opciones del receptor dentro del bloque de GQRX es una parte esencial para configurar la recepción de la señal del mando inalámbrico. Permite modificar varias configuraciones para optimizar la recepción de la señal y evitar ciertas interferencias. Este bloque se identifica en la Figura 23.

Dentro de las primeras opciones se encuentra la de Frequency, que en este caso es la frecuencia central en la que está configurado el dispositivo SDR. Para el análisis, se establece la frecuencia central de 433 MHz. Esta frecuencia puede variar dependiendo de las marcas de los mandos. La opción del Ancho del filtro (Filter Width) permite pasar las frecuencias por medio de un filtro pasa banda, con la finalidad de eliminar el ruido ambiental. En esta configuración se establece el tamaño del espectro que será sintonizado con la opción Wide.

La otra opción de filtro es Filter Shape, la cual ayuda a atenuar las frecuencias que no están dentro del rango deseado a partir de la frecuencia central. En este caso, se escoge la opción Normal debido a que el ancho de banda es adecuado para el análisis.

La opción de Modo es de suma importancia para este análisis, ya que se debe escoger, dentro de todas las opciones disponibles, la más idónea para manejar la señal. En este caso, se selecciona la opción AM-Sync, debido a que es eficaz para la frecuencia de 433.950 MHz, gracias a su capacidad para manejar desvanecimientos, mejorar la calidad del audio y obtener así una recepción clara y estable.

La opción de AGC (Automatic Gain Control) permite ajustar automáticamente el nivel de ganancia del receptor SDR. En este caso, se mantiene la opción Medium para poder tener una ganancia moderada. La opción de Squelch, también conocida como control de silencio, permite medir el nivel de señal mínima que puede ser recibida por el receptor antes de emitir audio, con la finalidad de eliminar el ruido de fondo. En este caso, se establece un umbral de -61.3 dB, lo cual permite desechar todo el ruido que esté por debajo de ese valor y solo las señales que estén por encima de los decibeles establecidos podrán ser escuchadas. Como último parámetro, se tiene la opción de Reductor de Ruido, que permite eliminar ruidos impulsivos o interferencias. Para este caso, no se utiliza ninguna opción debido a que dentro de la frecuencia central no existen este tipo de interferencias.

Figura 23

Bloque de configuraciones Receiver Options

Para este caso se tienen las configuraciones del bloque FFT Settings dentro de GQRX, lo cual se refiere a los ajustes relacionados con la Transformada Rápida de Fourier (FFT, por sus siglas en inglés), que es un algoritmo matemático utilizado para

calcular el espectro de frecuencia de la señal recibida y mostrarlo en la interfaz gráfica principal de GQRX.

Como primer parámetro a configurar está FFT Size, que determina el número de muestras utilizadas para calcular cada FFT. Un valor más alto aumenta la resolución de frecuencia, pero disminuye la tasa de actualización del espectro. Se debe tener en cuenta los recursos disponibles, debido a que un número mayor representa más carga para el procesamiento de la máquina virtual.

En la figura 24 se identifica la configuración de Rate, la cual hace referencia a que el espectro de frecuencia se actualiza a 30 fps, representando cuántos fotogramas por segundo se actualizan. Este tipo de configuraciones tiene una desventaja, ya que un mayor número de fps implica una mayor carga para el procesador y puede llegar a colapsar el sistema operativo. La opción de WF Span permite controlar el rango de frecuencias que son visibles en la pantalla en cascada. Para este caso se establece en auto para poder monitorear un amplio rango de frecuencias.

La opción de Window permite seleccionar el tipo de ventana que se aplica a los datos de la muestra de la señal, con la finalidad de mejorar la calidad del espectro. Para este caso se utiliza Blackman-Harris dentro de todas las otras opciones, debido a que ayuda a la supresión del ruido, reduciendo las interferencias del ambiente. Para la opción de Plot Mode y Plot Scale se mantienen las configuraciones establecidas, ya que solo permiten visualizar de mejor manera el espectro de la señal.

Para la opción de Show se escoge solo la opción de Max, la cual ayuda a identificar el pico máximo en la recepción de datos. Conjuntamente, la opción de Split Plot ayuda a dividir la visualización del gráfico en varias secciones. Las opciones de Plot dB y WF dB se mantienen en su valor máximo. Estas opciones ayudan a mejorar la gráfica con respecto a los decibelios e influyen en la adquisición de las muestras.

La opción de WF Mode ayuda a optimizar los modos de visualización del espectro, donde el eje horizontal corresponde a la frecuencia y el eje vertical al tiempo. En este caso se escoge la opción de Max, que permite identificar el nivel máximo de una señal durante el periodo de pruebas. Es útil para identificar picos de señal que ocurren brevemente y que podrían no ser visibles en otros modos. Como última opción se establece la opción Center, que centra el espectro con respecto a la frecuencia central.

Figura 24

Bloque de configuraciones de FFT

Para este análisis, es importante el bloque de audio de la Figura 25. En estas configuraciones, se puede capturar la señal deseada y guardarla en un archivo de formato de audio (wav). Teniendo previamente establecidos los parámetros para la captura de la señal, como las configuraciones del espectro de la señal y su ancho de banda que se desea analizar, se procede a guardar el archivo utilizando la opción de REC.

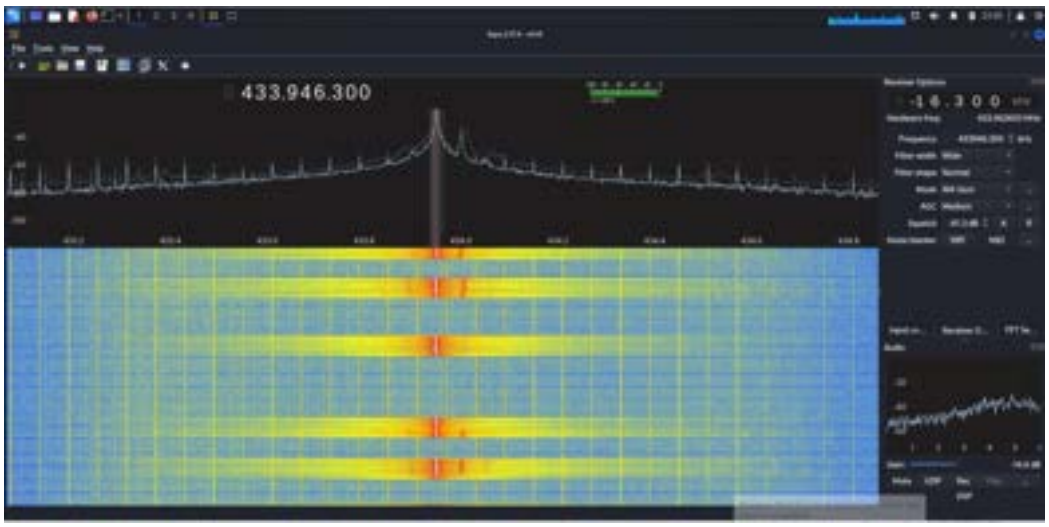
Figura 25

Bloque de configuración de Audio

En este caso, se realiza el ataque utilizando el dispositivo RTL-SDR, el cual, con la ayuda del software GQRX, logra capturar la señal inalámbrica cuando se utilizan los mandos de los portones eléctricos. Se pueden identificar los patrones de cada uno de los pulsos generados por el mando inalámbrico de color rojo en la Figura 26. Esta señal capturada se almacena en un archivo de audio de acuerdo con el ancho de banda establecido en su frecuencia central. Esto permite identificar las tramas de bits enviadas por los controles para poder accionar el dispositivo.

Figura 26

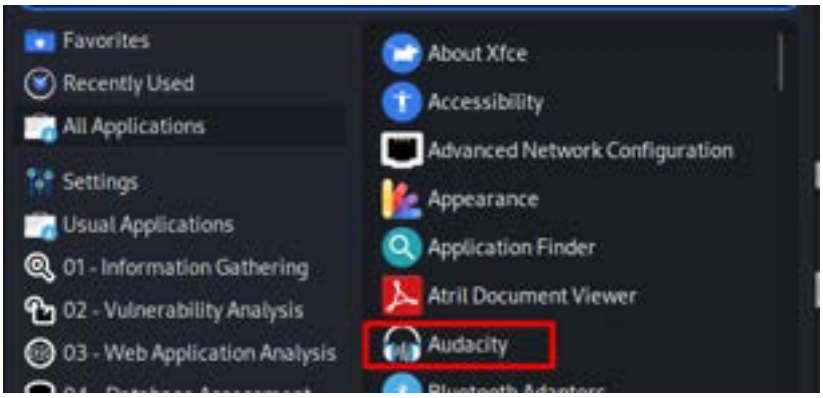
Captura de las señales generadas con el dispositivo RTL-SDR



Los datos obtenidos no se pueden visualizar claramente. Para resolver esto, se utiliza el software Audacity para identificar los bits capturados en el proceso anterior y, además, eliminar las partes del archivo de audio que contienen ruido e interferencias debido a la transmisión. Dentro del entorno de Kali Linux se puede encontrar también este tipo de aplicación como se identifica en la Figura 27, la cual es de mucha ayuda para el análisis de señales.

Figura 27

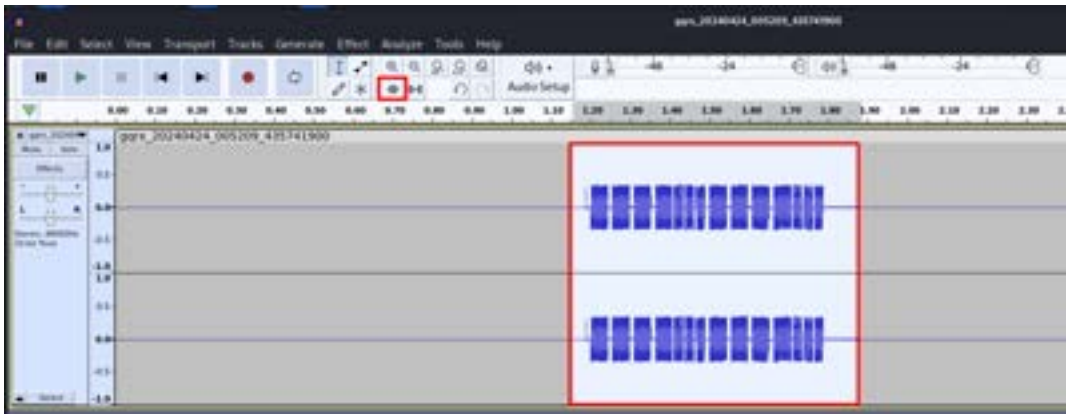
Software de Audacity



En este caso uno vez instalado del programa se procede a abrir el archivo wav que se captura de la señal de los mandos en el software GQRX. En este caso se puede identificar la señal que se captura de los mandos y se procede a depurar las partes del archivo que no son necesarias mediante el uso de recortes de audio como se evidencia en la Figura 28.

Figura 28

Captura de la señal inalámbrica del mando



Como resultado se puede apreciar la señal enviada por los mandos inalámbricos, en la cual se puede distinguir de mejor manera la trama de bits enviados para poder accionar el motor de los portones eléctricos, así generando una brecha de seguridad para los usuarios.

3.5.4 Ataque 3: Uso de Adalm Pluto

El tercer ataque implica el uso del dispositivo Adalm Pluto en conjunto con la herramienta de software Matlab. El objetivo de este ataque es emplear la programación para llevar a cabo un ataque de penetración, logrando activar los portones eléctricos

de manera no autorizada. Adalm Pluto es una poderosa herramienta para realizar transmisiones de datos y, lo cual teniendo los con los parámetros necesarios, puede replicar cualquier tipo de señal de RF dentro de su umbral de funcionamiento.

De igual manera, el dispositivo cuenta con soporte dentro del entorno de programación de Matlab, lo cual facilita su uso. En la Figura 29 se identifican los paquetes necesarios para instalar los controladores en el ordenador anfitrión, asegurando así su funcionamiento sin errores de conexión.

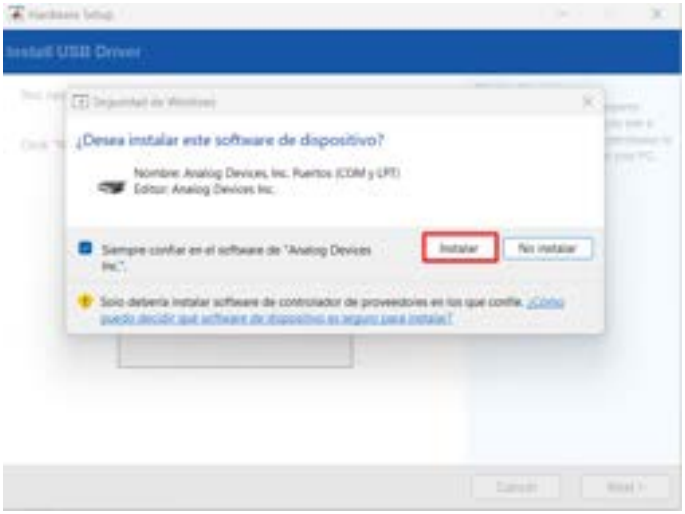
Figura 29

Toolbox de Matlab

Se procede a instalar los controladores necesarios para su funcionamiento. Como se identifica en la Figura 30, se establecen los puertos COM, en este caso el puerto 1, y de igual manera el LPT, que hace referencia al puerto paralelo, lo cual ayuda a que la transmisión sea más rápida.

Figura 30

Instalación de controladores COM



En la Figura 31 se comprueba que la instalación del controlador de Pluto con el sistema de Matlab es correcta. De igual manera, en los pasos posteriores se verifica que las funciones tanto de transmisión como de recepción de señales funcionan con normalidad.

Figura 31

Verificación del funcionamiento del controlador

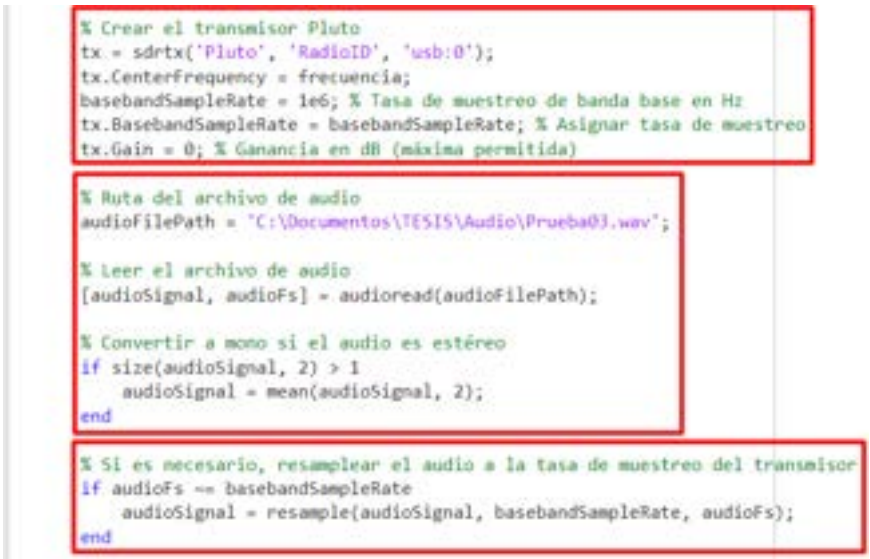
3.5.4.1 Programación del código en MATLAB

Para el tercer ataque, se realiza la programación en la cual se establecerán diferentes parámetros y variables para lograr una transmisión lo más eficiente posible. En este caso, se crea una interfaz gráfica en App Designer, una herramienta propia de MATLAB para desarrollar aplicaciones con código.

Se debe tener una carpeta donde se almacenen todos los archivos WAV guardados durante el análisis del segundo ataque. Estas señales se procesarán para ser transmitidas posteriormente. Como se muestra en la Figura 32, se establece la variable de la frecuencia central, que es de 433.92 MHz. Se crea una instancia del transmisor Pluto y se configuran los parámetros esenciales como la frecuencia central, la tasa de muestreo de la banda base y la ganancia. Además, se garantiza que la tasa de muestreo de la señal coincida con la tasa de muestreo requerida para la transmisión. Esto se hace con el fin de mantener la calidad e integridad de la señal.

Figura 32

Configuración y establecimiento de parámetros de transmisión



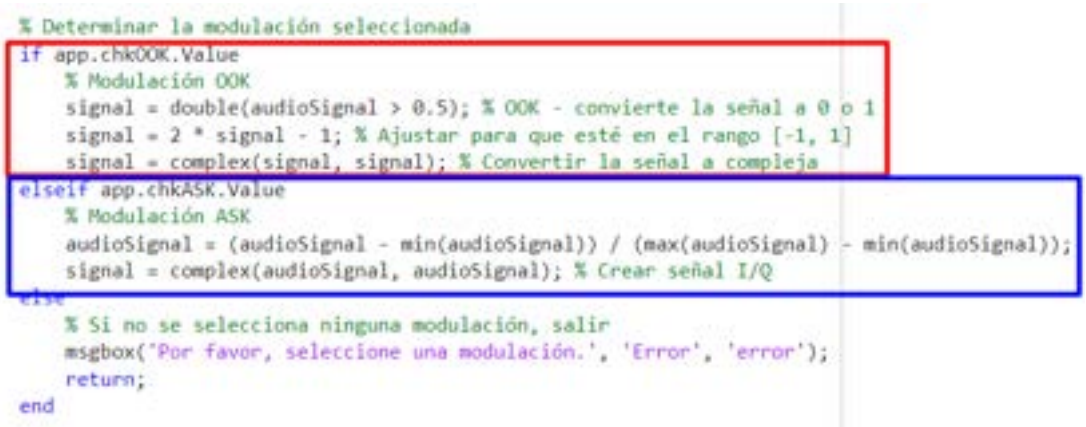
```
% Crear el transmisor Pluto
tx = sdrtx('Pluto', 'RadioID', 'usb:0');
tx.CenterFrequency = frecuencia;
basebandSampleRate = 1e6; % Tasa de muestreo de banda base en Hz
tx.BasebandSampleRate = basebandSampleRate; % Asignar tasa de muestreo
tx.Gain = 0; % Ganancia en dB (máxima permitida)

% Ruta del archivo de audio
audioFilePath = 'C:\Documentos\TESIS\Audio\Prueba03.wav';

% Leer el archivo de audio
[audioSignal, audioFs] = audioread(audioFilePath);

% Convertir a mono si el audio es estéreo
if size(audioSignal, 2) > 1
    audioSignal = mean(audioSignal, 2);
end

% Si es necesario, resamplear el audio a la tasa de muestreo del transmisor
if audioFs ~= basebandSampleRate
    audioSignal = resample(audioSignal, basebandSampleRate, audioFs);
end
```

Se establece el tipo de modulación que se va a utilizar para transmitir una señal de audio, basado en la selección del usuario. Teniendo entre las opciones de modulación OOK, ASK y AM. En la cual se establece el código para que la señal de audio de procese a una binaria (1 o 0), que dependiente de los parámetros de tenga la señal portadora establezca el nivel del umbral de transmisión en el caso de la modulación OOK.

Caso contrario para la modulación ASK se realiza la misma lógica anterior, pero normaliza la señal de audio para que los valores estén entre 0 y 1. Para mejorar la eficiencia de transmisión en esta modulación se realiza el paso de crear una señal I/Q donde la parte real y la parte imaginaria son iguales a la señal de audio normalizada. Este proceso se identifica en la Figura 33.

Figura 33

Establecimiento de los parámetros de modulación



```
% Determinar la modulación seleccionada
if app.chkOOK.Value
    % Modulación OOK
    signal = double(audioSignal > 0.5); % OOK - convierte la señal a 0 o 1
    signal = 2 * signal - 1; % Ajustar para que esté en el rango [-1, 1]
    signal = complex(signal, signal); % Convertir la señal a compleja
elseif app.chkASK.Value
    % Modulación ASK
    audioSignal = (audioSignal - min(audioSignal)) / (max(audioSignal) - min(audioSignal));
    signal = complex(audioSignal, audioSignal); % Crear señal I/Q
else
    % Si no se selecciona ninguna modulación, salir
    msgbox('Por favor, seleccione una modulación.', 'Error', 'error');
    return;
end
```

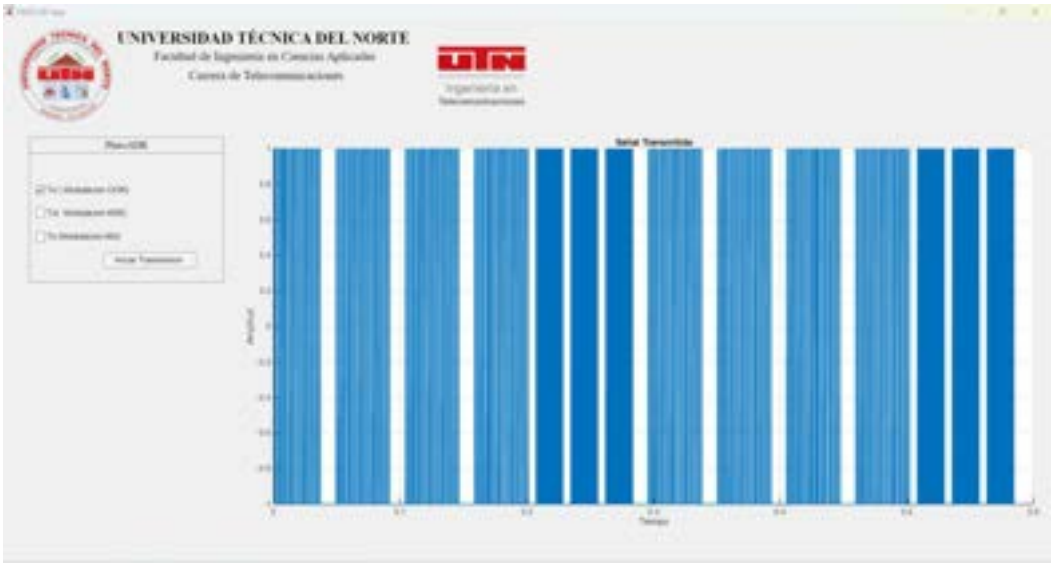
3.5.4.2 Ejecución de la interfaz grafica

Teniendo en cuenta el código realizado, se procede a verificar su funcionamiento. Como primer paso, se realiza la transmisión de datos utilizando la modulación OOK, que es un tipo de modulación digital ampliamente utilizada en comunicaciones de baja frecuencia.

En este caso, se emplea para abrir sistemas de portones automáticos. Como se identifica en la Figura 33, su característica principal es la presencia o, en su defecto, la ausencia de la señal portadora, donde un bit '1' se representa por la presencia de la señal portadora y un bit '0' se representa por la ausencia de esta. Por lo tanto, su índice de modulación es alto.

Figura 34

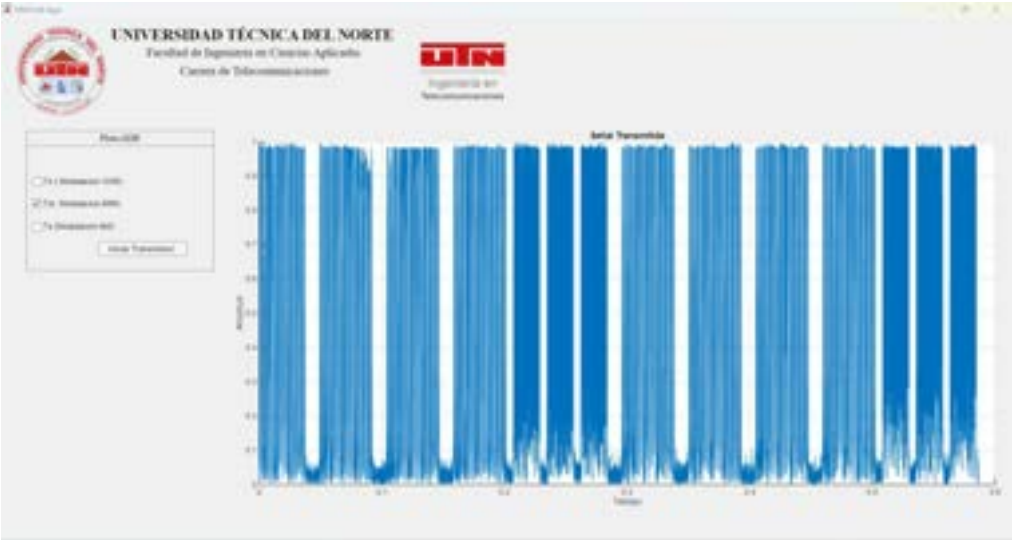
Transmisión por modulación OOK



Para el segundo caso, se tiene la modulación por desplazamiento de amplitud (ASK), que es un tipo de modulación digital ampliamente utilizada en comunicaciones de baja frecuencia. Esta modulación se considera una variación de la modulación OOK. Su principal característica es que posee dos tipos de amplitudes junto con la portadora. Cuando la amplitud es alta, representa un "1" y cuando la amplitud es baja, representa un "0". En la Figura 35 se identifica que la señal transmitida posee la misma trama que la señal anterior, pero presenta una amplitud baja con la señal portadora en ciertos instantes de tiempo.

Figura 35

Transmisión de datos por modulación ASK



4 CAPÍTULO IV RESULTADOS Y ANÁLISIS

Dentro de la metodología aplicada, se establece en el capítulo IV la fase 5 sobre el análisis de resultados. En esta fase se evaluarán las distintas vulnerabilidades encontradas en los sistemas automáticos y se definirán, de acuerdo con su nivel de protección, diversas recomendaciones técnicas para prevenir ciertos ataques.

4.1 Fase 5: Análisis de resultados

En esta fase se detallan los resultados obtenidos de los ataques realizados para identificar las vulnerabilidades de seguridad en portones eléctricos, esto utilizando diversas herramientas y técnicas. Se llevaron a cabo tres ataques distintos empleando dispositivos SDR como Flipper Zero, RTL-SDR en conjunto con GQRX, y MATLAB con el dispositivo ADALM-Pluto. Las marcas evaluadas fueron en total 4 con diferentes modelos, los cuales presentan distintos niveles de seguridad en sus características inalámbricas.

4.1.1 Resumen de resultados de los ataques generados

En cada uno de los escenarios planteados se establecieron tres diferentes tipos de ataques. Dependiendo de la seguridad del motor analizado, estos podrán ser vulnerados o, en su defecto, no podrán ser atacados en cada uno de los ataques propuestos.

4.1.1.1 Ataque 1: Uso de Flipper Zero

En la Tabla 14 se evalúan los resultados obtenidos sobre la seguridad de diversos portones eléctricos con el uso del dispositivo Flipper Zero. Este dispositivo fue utilizado en siete escenarios distintos con las mismas condiciones para evaluar la efectividad del Flipper Zero en la vulneración de dichos sistemas.

Se obtuvieron como resultados que las marcas Lift Máster y Pecinnin no pudieron ser vulneradas por el dispositivo Flipper Zero. Esto se debe a que ambas poseen mecanismos de defensa para sus comunicaciones inalámbricas, las cuales son el uso de código rodante, lo que ofrece una mayor seguridad contra la clonación de señales. En el Anexo A se detallan cada una de las vulnerabilidades encontradas para cada escenario.

Como se evidencia en la Tabla 14, la situación fue distinta para 3 escenarios que si se logró vulnerar sus dispositivos. En diferentes escenarios de prueba, se logró capturar la señal emitida por los mandos y retransmitirla al motor, permitiendo así obtener acceso no autorizado.

Tabla 14

Tabla de resumen de resultados obtenidos para el primer ataque

Aspecto	Descripción
Dispositivo Utilizado	Flipper Zero
Objetivo del Ataque	Vulnerar portones eléctricos de diferentes marcas con el uso del Flipper Zero
Descripción del Ataque	Se utilizó el Flipper Zero para emular y analizar señales de RF de los mandos de portones eléctricos
Número de escenarios	7 escenarios evaluadas
Análisis	Observó que la mayoría de las marcas no implementan seguridad robusta en sus señales de control
Impacto	Posibilidad de abrir portones eléctricos sin autorización en marcas vulnerada
Resultados	• Vulneradas: 4 escenarios • No Vulnerada: 3 escenarios

4.1.1.2 Ataque 2: Captura de datos con RTL-SDR

Para el siguiente ataque se utilizaron distintos programas conjunto con el dispositivo RTL-SDR, para analizar un sondeo del medio inalámbrico al accionar un motor automático. El objetivo era interceptar y capturar las señales enviadas por los mandos para identificar los datos transmitidos. Este procedimiento se evaluó en siete escenarios distintos de pruebas.

Como resultado, se logró vulnerar a la mayoría de los escenarios con un total de 5 vulnerados, identificando en el espectro inalámbrico los datos necesarios para abrir el motor. Esto se debe a que su comunicación utiliza un código fijo lo que ocasión a ser más susceptible de ser clonado. En cambio, como se especifica en la Tabla 15 solo 2 escenarios no fueron vulnerables a este tipo de ataques, ya que su frecuencia cambia constantemente. Esto se especifica con mayor profundidad en el Anexo A.3.

Tabla 15

Tabla de resume sobre los resultados obtenidos para el segundo ataque

Aspecto	Descripción
Dispositivo Utilizado	• RTL-SDR • Software: GQRX y Audacity
Objetivo del Ataque	Interceptar y capturar señales de mandos inalámbricos de portones eléctricos
Descripción del Ataque	Configuración de RTL-SDR con GQRX para escuchar y guardar señales inalámbricas para identificar los datos enviados.
Número de escenarios	7 escenarios evaluadas
Análisis	El ataque permite interceptar y analizar señales RF de mandos inalámbricos, demostrando la falta de cifrado en las marcas vulneradas.
Impacto	Facilita la reproducción de señales de control, posibilitando la apertura no autorizada de portones
Resultados	• Vulneradas: 5 escenarios • No Vulnerada: 2 escenarios

4.1.1.3 Ataque 3: Transmisión de datos con ADALM-PLUTO

Por último, se tiene los resultados del ataque 3, en el cual, mediante la programación en Matlab y el uso del dispositivo ADALM-PLUTO, se procedió a retransmitir las señales capturadas durante el ataque 2. Esto se realizó con el fin de vulnerar la seguridad de los portones y obtener acceso no autorizado.

Como resultado de los ataques se tiene la Tabla 16, en la cual se establece que existen diferentes marcas de portones que se logró accionar su mecanismo y realizar su apertura para 4 escenarios. Las cuales al no tener un código rodante para su transmisión ocasiona que puedan ser accionados mediante la transmisión de su señal captura de días anteriores.

Tabla 16

Resultados obtenidos para el tercer ataque

Aspecto	Descripción
Dispositivo Utilizado	• ADALM-PLUTO • Software: MATLAB
Objetivo del Ataque	Replicar y transmitir señales de portones eléctricas capturadas para abrir portones eléctricos
Descripción del Ataque	Uso de MATLAB y ADALM-Pluto para procesar y transmitir señales en diferentes modulaciones.
Número de escenarios	7 escenarios evaluados
Análisis	Validación de la capacidad para realizar ataques de repetición utilizando señales RF capturadas
Impacto	Posibilidad de programar códigos que permitan abrir los portones eléctricos replicando señales legítimas de un mando original.
Resultados	• Vulneradas: 4 escenarios • No Vulnerada: 3 escenarios

4.2 Evaluación de Riesgos de Seguridad Inalámbrica

De acuerdo con los resultados obtenidos en cada uno de los escenarios de pruebas realizados, se establece la evaluación del riesgo. La seguridad de la información es un aspecto crítico en la protección de sistemas de control de acceso, como los portones eléctricos.

El análisis de riesgos sigue los pasos establecidos por el Instituto Nacional de Ciberseguridad (INCIBE), la cual se basa en la metodología MAGERIT. Esta metodología, de acceso público, se adapta a las necesidades de la investigación y permite identificar, evaluar y gestionar los riesgos asociados a posibles ataques inalámbricos. A través de este enfoque, se busca identificar el valor del impacto que tiene la confidencialidad, integridad y disponibilidad de los sistemas vulnerados, de acuerdo con los principios fundamentales del modelo de seguridad conocido como el triángulo CIA(INCIBE, 2021).

4.2.1 Identificación de Activos

De acuerdo con el análisis de riesgo establecido, el primer paso es la identificación de los activos, los cuales se refieren a los componentes o recursos necesarios para el funcionamiento de un sistema o proceso involucrados en cada uno de los escenarios de pruebas realizados. Para este analices el activo defino es el sistema de portón automático, los activos a analizar son el motor, el mando a distancia y la tarjeta de comunicación inalámbrica como se identifica en la Tabla 17.

Tabla 17

Características de activos del sistema de portones eléctricos

Tipo	Descripción	Tipo	Critico
Portón	Compuertas para la apertura al inmueble	Físico	SI
Mando	Dispositivo inalámbrico para abrir o cerrar el portón eléctrico	Físico	SI
Tarjeta inalámbrica	Sistema embebido para la recepción de la señal de RF y mecanismo de apertura	Físico	SI

4.2.2 Cálculo de la Probabilidad de Ocurrencia

Para determinar la probabilidad de ocurrencia en los distintos escenarios de la investigación, es necesario mencionar que esta se establece mediante un análisis de cuán probable es que ocurra una vulnerabilidad en cada uno de los escenarios planteados. De acuerdo con (Ricardo, 2019) : "El cálculo de la probabilidad se establece a través del cálculo de los casos favorables y los casos posibles", como se lo establece en la Ecuación 1.

$$Probabilidad\ de\ Ocurrencia = \left(\frac{Casos\ favorables}{Casos\ posibles}\right) \times\ 100\ \% \qquad \textbf{(1)}$$

Datos:

- Casos favorables: 1-3 (define el número de los ataques que tuvieron éxito)
- Casos posibles: 3 (cantidad de total ataques realizados)

Para determinar la probabilidad de ocurrencia, los escenarios se agruparon en tres categorías. En la primera categoría, el número de casos favorables fue 1. En la segunda categoría, se identificaron 2 casos favorables, y en la tercera categoría, el número de casos favorables fue 3. La clasificación se lo realiza con la finalidad de

facilitar el análisis de la probabilidad de ocurrencia en cada escenario, permitiendo una evaluación más organizada y precisa.

4.2.2.1 Escenario 3 y 4

Para los escenarios 3 y 4, según las vulnerabilidades detectadas durante los ataques, los casos favorables fueron 33.33, lo que implica que la probabilidad de ocurrencia en estos casos es del 33.33 %, como se presenta en la Ecuación 2.

$$Probabilidad\ de\ Ocurrencia = \left(\frac{1}{3}\right) \times\ 100\ \%\ =\ 33.33\ \% \qquad \textbf{(2)}$$
$$Probabilidad\ de\ Ocurrencia\ =\ \mathbf{33.33}\ \%$$

4.2.2.2 Escenario 5

En cuanto al escenario 5, los datos indican que, de acuerdo con las pruebas realizadas, los casos favorables fueron solo 1, lo que, según la fórmula, resulta en una probabilidad de ocurrencia del 66.66 %, tal como se establece en la Ecuación 3.

$$Probabilidad\ de\ Ocurrencia = \left(\frac{2}{3}\right) \times\ 100\ \%\ =\ \mathbf{66.66}\% \qquad \textbf{(3)}$$
$$Probabilidad\ de\ Ocurrencia\ =\ \mathbf{66.66}\ \%$$

4.2.2.3 Escenario 1,2,6 y 7

De acuerdo con los datos obtenidos en los ataques realizados en los escenarios 1, 2, 6 y 7, se concluye que los casos favorables fueron 3. Por lo tanto, la probabilidad de ocurrencia es del 100 %, como se muestra en la Ecuación 4.

$$Probabilidad\ de\ Ocurrencia = \left(\frac{3}{3}\right) \times\ 100\ \%\ =\ 100\ \% \qquad \textbf{(4)}$$

$$Probabilidad\ de\ Ocurrencia\ =\ \mathbf{100}\ \%$$

De acuerdo con la probabilidad de ocurrencia encontrada en los distintos escenarios, se establece la Tabla 18 para determinar el valor tanto cualitativo y cuantitativo de cada uno de los casos, siguiente la metodología establecida por la organización INCIBE.

Tabla 18

Tabla sobre el valor de probabilidad de ocurrencia en cada uno de los escenarios

Valor de Probabilidad	Escenarios	Cuantitativo	Cualitativo	Descripción
33.33 %	3 y 4	1	Baja	La probabilidad de que los ataques realizados puedan penetrar la seguridad del sistema es casi nula.
66.66 %	5	2	Media	Existe la probabilidad de que los ataques generados puedan ocasionar inseguridad en los sistemas de los portones automáticos.
100 %	1,2,6 y 7	3	Alta	La probabilidad de que los ataques realizados puedan vulnerar los sistemas de RF es relativamente alta.

4.2.3 Impacto de los Ataques de acuerdo con el triángulo CIA

Para determinar el impacto que podría tener un ataque inalámbrico, se tomará en cuenta las consecuencias que puede existir en cada escenario planteado, en caso de que el ataque sea exitoso. Este impacto se determina mediante los efectos que pueda tener sobre la confidencialidad, integridad y disponibilidad del sistema, los cuales son los pilares del triángulo CIA.

La confidencialidad se refiere a la protección de la información contra el acceso no autorizado; la integridad hace referencia a asegurar que los datos no sean alterados de manera no autorizada; y, por último, la disponibilidad garantiza que los sistemas estén operativos y accesibles cuando el usuario los necesite (Kiser, 2021).

Se establecen criterios para evaluar los ataques realizados en cada escenario, considerando cuales sistemas fueron vulnerados. El objetivo es analizar el impacto de estas fallas y comprender la problemática asociada a la vulneración de los sistemas, lo que genera riesgos de seguridad en función de los principios del triángulo CIA.

4.2.3.1 Primer Ataque: Flipper Zero

- **Confidencialidad:** En el primer ataque realizado la confidencialidad puede ser vulnerada fácil mente, debido a que un atacante pueda capturar y emule las señales de RF enviadas por los mandos a distancia de los portones eléctricos. Si la señal es capturada, el atacante puede operar el portón sin autorización, lo que viola la confidencialidad del lugar en donde suceda el ataque.

- **Integridad:** Aunque el enfoque principal del ataque es comprometer la confidencialidad de los sistemas de los usuarios, durante este ataque se obtienen los datos necesarios para poder retransmitir la señal. Esto implica un riesgo adicional al comprometer también la integridad del sistema.
- **Disponibilidad:** Si un atacante interfiere con las señales de RF, podría impedir que los usuarios legítimos accedan al sistema, lo que resultaría en un estado de bloqueo que afectaría la disponibilidad del portón.

4.2.3.2 Segundo Ataque: RTL-SDR con Software GQRX y Audacity

- **Confidencialidad:** El segundo ataque compromete la confidencialidad del sistema al poder interceptar y capturar las señales inalámbricas enviadas por los mandos a distancia. Que en los escenarios que el sistema no posea una comunicación cifrada, estas señales pueden ser fácilmente interceptadas y utilizadas por personas no autorizadas para operar el portón.
- **Integridad:** En este ataque queda más vulnerable la integridad del sistema, debido a que las señales capturadas puedan ser reproducidas o en su defecto manipuladas, lo que ocasiona que el sistema acepte comandos no autorizados como si fueran legítimos.
- **Disponibilidad:** En este caso, la disponibilidad no se ve afectada, ya que el atacante únicamente puede analizar la señal capturada, sin comprometer el funcionamiento del sistema automático. Esto significa que, aunque el atacante tenga acceso a la información de la señal, no puede interferir en la operatividad del sistema.

4.2.3.3 Tercer Ataque: ADALM-PLUTO con MATLAB

- **Confidencialidad:** Similar a los otros ataques, la confidencialidad se ve comprometida porque el ataque permite replicar y transmitir señales legítimas, lo que permite a un atacante operar el portón sin autorización.
- **Integridad:** La integridad se ve afectada, ya que el sistema acepta señales replicadas por el software como si fueran válidas, permitiendo acciones no autorizadas, las cuales no fueron emitidas por los usuarios legítimos.
- **Disponibilidad:** La disponibilidad se ve comprometida si el sistema es manipulado con señales repetidas, lo que puede llevar a un comportamiento inesperado del sistema, como la denegación de acceso a usuarios legítimos o el bloqueo del sistema.

4.2.1 Cálculo del Valor de Impacto

Para determinar el cálculo del impacto que puede generar la vulneración en cada uno de los escenarios planteados, se hace referencia a la evaluación de las consecuencias que tendrían los activos en caso de sufrir una vulneración o daños en su sistema. Para lo cual se tiene como pauta los criterios analizados del triángulo CIA para determinar el valor cualitativo y cuantitativo.

En este caso, se asignan valores a cada característica del triángulo CIA que van de 1 a 3. El valor de impacto cuantitativo se obtiene sumando estos tres valores. Para el valor cualitativo, se establecieron tres niveles de seguridad inalámbrica: bajo, medio y alto, según el resultado del valor cuantitativo de cada escenario como se identifica en la Tabla 19.

Tabla 19

Tabla de resumen sobre los valores cuantitativos y cualitativos para el valor de impacto

CIA	Cuantitativo	Cualitativo
Confidencialidad	1-3	Bajo (1): Riesgo mínimo, poco impacto Medio (2): Riesgo moderado, impacto potencial Alto (3): Riesgo crítico, impacto significativo
Integridad	1-3	Bajo (1): Riesgo mínimo, poco impacto Medio (2): Riesgo moderado, impacto potencial Alto (3): Riesgo crítico, impacto significativo
Disponibilidad	1-3	Bajo (1): Riesgo mínimo, poco impacto Medio (2): Riesgo moderado, impacto potencial Alto (3): Riesgo crítico, impacto significativo
Valor Total	3-9	**Bajo** = 3-4; **Medio** = 5-7; **Alto** = 8-9

Nota. Los valores cuantitativos se suman para determinar el impacto total, y se clasifican cualitativamente dependiendo del rango de valor de impacto obtenido para determinar si es Bajo, Medio o Alto.

En la ecuación 5 se establece cómo se determina el valor cuantitativo del impacto, el cual se obtiene mediante la suma total de los valores asignados a los tres pilares del triángulo CIA. Estos valores se asignan de acuerdo con las vulnerabilidades inalámbricas identificadas en cada escenario evaluado.

$$Valor\ de\ Impacto = \frac{\begin{matrix} Valor\ Confidencialidad(1-3) \\ +\quad Valor\ Integridad(1-3) \\ Valor\ de\ la\ Disponibilidad\ (1-3) \end{matrix}}{Valor\ Total} \qquad \textit{(5)}$$

$$Valor\ del\ Impacto\ = \mathbf{3-9}$$

Como resultado de los cálculos en cada caso se tiene la Tabla 20, en la cual se establen los valores cuantitativos y cualitativos para el valor del impacto en cada uno de los escenarios.

Tabla 20

Tabla de resultados obtenido sobre el valor de impacto cualitativo y cuantitativo

Escenario	Triangulo CIA		Cuantitativo	Cualitativo
1	Confidencialidad	3	9	Alto
	Integridad	3		
	Disponibilidad	3		
2	Confidencialidad	3	9	Alto
	Integridad	3		
	Disponibilidad	3		
3	Confidencialidad	1	3	Bajo
	Integridad	1		
	Disponibilidad	1		
4	Confidencialidad	1	3	Bajo
	Integridad	1		
	Disponibilidad	1		
5	Confidencialidad	1	5	Medio
	Integridad	3		
	Disponibilidad	1		
6	Confidencialidad	3	9	Alto
	Integridad	3		
	Disponibilidad	3		
7	Confidencialidad	3	9	Alto
	Integridad	3		
	Disponibilidad	3		

Nota: De acuerdo con el valor asignado en cada escenario de acuerdo con el triángulo CIA, se procede a sumar su nota en cada uno de los casos para obtener el valor cuantitativo y posteriores asignar un valor cualitativo como se especificó en la Tabla 19.

4.2.2 Cálculo de Valor de Riesgo

Se tiene los distintos datos sobre el cálculo del análisis de riesgo, para este caso se tiene los valores de manera cuantitativa y cualitativa para cada uno de los escenarios planteados.

4.2.2.1 Valor de Riesgo Cuantitativo

El cálculo del valor de riesgo que para este caso será cuantitativo, se establece mediante la multiplicación del valor del Impacto por la Probabilidad de ocurrencia que este pueda tener en cada uno de los escenarios. Esta fórmula está representada en la Ecuación 6, en la cual indica un riesgo alto cuando el activo es valioso y existe una alta probabilidad de que el ataque sea exitoso. Por otra parte, si el valor del riesgo es bajo o casi nulo, puede considerarse aceptable sin muchas recomendaciones de seguridad.

$$Valor\ del\ Riesgo = Probabilidad\ de\ Ocurrencia\ \times Impacto \qquad \textbf{(6)}$$

Datos:

- Probabilidad de Ocurrencia: 1-3(Valor de los casos exitosos por lo menos una vez al año)
- Impacto: 1-9 (Valor del impacto de acuerdo con el triángulo CIA)

Por último, para determinar el valor de riesgo, los escenarios se agruparon en tres categorías que presentaron el mismo valor tanto de su probabilidad de ocurrencia como del valor de impacto. Esta agrupación se lo realizo con la final facilitar el cálculo

de riesgo en cada escenario y van desde los escenarios que tiene menor valor de riesgo hasta los que presenta un riesgo alto.

4.2.2.2 Escenario 3 y 4

En los escenarios 3 y 4, el valor de la probabilidad de ocurrencia es 1. Asimismo, el valor de impacto en estos escenarios es también 3, lo que da como resultado un valor de riesgo igual a 1, como se muestra en la Ecuación 7.

$$Valor\ del\ Riesgo = 1\ \times\ 3 = \mathbf{3} \qquad \textbf{(7)}$$
$$Valor\ del\ Riesgo\ =\ \mathbf{3}$$

4.2.2.3 Escenario 5

En el escenario 5, de acuerdo con los datos obtenidos sobre la probabilidad e impacto, ambos tienen un valor de 5. Esto da como resultado un valor de riesgo igual a 4 para este escenario de prueba, como se muestra en la Ecuación 8.

$$Valor\ del\ Riesgo = 2\ \times\ 5 = 10 \qquad \textbf{(8)}$$
$$Valor\ del\ Riesgo\ =\ \mathbf{10}$$

4.2.2.4 Escenario 1,2,6 y 7

Finalmente, se evalúan los escenarios restantes: 1, 2, 6 y 7. En estos casos, los valores de impacto y probabilidad obtenidos son ambos iguales a 3, lo que genera un valor de riesgo igual a 9, tal como se muestra en la Ecuación 9.

$$Valor\ del\ Riesgo = 3\ \times\ 9 = 27 \qquad \textbf{(9)}$$
$$Valor\ del\ Riesgo\ =\ \mathbf{27}$$

Se tiene como resulta la Tabla 21, en donde se detallan los valores obtenidos del análisis de valor de Riesgo cuantitativo en cada uno de los escenarios planteados con los datos de su valor de probabilidad y de impacto.

Tabla 21

Tabla de resumen sobre los cálculos del Valor del Riesgo Cuantitativo

Escenario	Valor de Probabilidad	Valor de Impacto	Valor de Riesgo
1	3	9	27
2	3	9	27
3	1	3	3
4	1	3	3
5	2	5	10
6	3	9	27
7	3	9	27

Nota: La siguiente Tabla se estable todos los valores obtenidos en cada uno de los escenarios planteados para determinar su valor de riesgo.

Teniendo como referencia los datos obtenidos de la Tabla 21 se estable el rango del valor de Riesgo que se tiene para cada uno de los escenarios planteados, dependiendo del resultado obtenido para el valor cualitativo.

- **Bajo y Muy Bajo:** 1 – 9 (resultado de valor de riesgo)
- **Medio y Alto:** 10 – 18 (resultado de valor de riesgo)
- **Muy Alto:** 19 – 27 (resultado de valor de riesgo)

4.2.2.5 Valor de Riesgo Cualitativo

Para el cálculo cuantitativo del valor de riesgo, se hace referencia a la Tabla 22, la cual se modificó de la organización INCIBE. En dicho cálculo, se utilizan los valores de impacto y probabilidad obtenidos en los análisis anteriores, que permiten determinar el nivel de riesgo asociado a cada amenaza identificada en cada para cada uno de los escenarios.

Tabla 22

Tabla de análisis de Riesgo Cuantitativo

CALCULO DE RIESGO		**IMPACTO**		
		Bajo	**Medio**	**Alto**
PROBABILIDAD	**Baja**	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy Alto

Fuente: Obtenido del sitio web: https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo

El resultado del análisis de riesgo cualitativo se presenta en la Tabla 23, donde se detallan los escenarios evaluados junto con los valores asociados a las amenazas identificadas. Estos valores son el resultado de la combinación entre el nivel de probabilidad y el nivel de impacto, permitiendo así una evaluación integral de los riesgos presentes en cada escenario analizado.

De igual forma, se asigna un color para representar el valor de riesgo calculado, utilizando una escala de colores de intensidad en el análisis de riesgo que varía según el nivel cualitativo. Para un riesgo muy bajo se asignó el color azul; para un riesgo

bajo, el color verde; el riesgo medio se identifica con el color amarillo; el riesgo alto, con el color naranja; y el riesgo muy alto, con el color rojo.

Tabla 23

Tabla de resumen sobre los cálculos del Valor del Riesgo Cualitativo

Escenario	Valor de Probabilidad	Valor de Impacto	Valor de Riesgo
1	Alta	Alto	Muy alto
2	Alta	Alto	Muy alto
3	Baja	Bajo	Muy bajo
4	Baja	Bajo	Muy bajo
5	Media	Medio	Medio
6	Alta	Alto	Muy alto
7	Alta	Alta	Muy alto

Nota: Para obtener el Valor de Riesgo se utiliza la referencia de la Tabla 22, en la cual dependiendo del valor la Probabilidad y el Impacto, se tendrá un valor cualitativo.

Como resultado final, se presenta la Tabla 24, que consolida los valores de riesgo cuantitativos y cualitativos de los distintos escenarios analizados. Esto permite una comprensión más precisa de los riesgos identificados y su impacto en la seguridad de los sistemas evaluados, proporcionando una visión completa sobre la vulnerabilidad y el nivel de riesgo presente en cada caso estudiado.

Tabla 24

Resultados obtenidos de los diferentes ataques realizados de acuerdo con Valor de Riesgo

Escenario	Valor de Riesgo	Grado de Riesgo	Relación con el Triángulo CIA	
1	27	Muy Alto	Confidencialidad	SI
			Integridad	SI
			Disponibilidad	SI
2	27	Muy Alto	Confidencialidad	SI
			Integridad	SI
			Disponibilidad	SI
3	3	Muy Bajo	Confidencialidad	NO
			Integridad	NO
			Disponibilidad	NO
4	3	Muy Bajo	Confidencialidad	NO
			Integridad	NO
			Disponibilidad	NO
5	10	Medio	Confidencialidad	NO
			Integridad	SI
			Disponibilidad	NO
6	27	Muy Alto	Confidencialidad	SI
			Integridad	SI
			Disponibilidad	SI
7	27	Muy Alto	Confidencialidad	SI
			Integridad	SI
			Disponibilidad	SI

Nota. Esta tabla ofrece una visión integral del nivel de riesgo asociado a cada uno de los escenarios analizados, facilitando una evaluación comparativa de las diferentes marcas que presentan vulnerabilidades. Además, detalla el impacto potencial que estas vulnerabilidades tienen en los pilares del triángulo CIA.

Los resultados mostraron que el valor de impacto varía entre los distintos modelos de portones eléctricos. Los escenarios con altos valores tanto en probabilidad como en impacto presentaron un riesgo significativo, como se observó en los escenarios 1, 2, 6 y 7, donde el valor de riesgo cuantitativo fue de 27, correspondiente a un nivel cualitativo de riesgo muy alto. En contraste, los escenarios 3 y 4, con

menores valores de seguridad, registraron un riesgo cualitativo muy bajo, con un valor de riesgo de 3.

4.3 Tratamiento de Riesgos (Recomendaciones)

De acuerdo con las vulnerabilidades identificadas y el nivel de seguridad establecido en la Tabla 24, se establecen recomendaciones específicas para cada uno de los escenarios analizados, basadas en el nivel de riesgo encontrado. En este caso se establecen diversas seguridades propias de las marcas de los portones, pero no son implementadas en un primer instante por la variable de costos. De igual manera se establece un prototipo que puede ser implementado y a su vez es mucho más económico que las recomendaciones anteriores. Como parte de los objetivos planteados se realiza un informe para cada uno de los niveles de riesgo encontrados en cada escenario, que se detallado en la sección de ANEXO B.

4.3.1 Riesgo Muy Alto

De acuerdo con los resultados obtenidos, se ha determinado que existen cuatro escenarios con una seguridad inalámbrica baja. Esto sugiere que, con los diferentes tipos de ataques realizados, pueden comprometer la seguridad de los usuarios al acceder a sus instalaciones. En establecen diferentes opciones para poder mitigar las vulnerabilidades encontradas las cuales son comerciales y en su defecto una placa programable desde cero que puede ser adaptada a los sistemas de portones eléctricos.

Se propone como solución comercial la implementación de una nueva tarjeta inalámbrica, la cual puede ser instalada de manera adecuada en los motores que presentaron un alto nivel de riesgo. Sin embargo, esta no se instala desde el inicio debido a la necesidad de reducir costos. En la sección del ANEXO B.1 se establecen con mayor detalle él informe de auditaría para un nivel de riesgo Muy Alto.

4.3.1.1 Opción 1: Receptora no clonable

El dispositivo receptor no clonable H90 es un receptor que utiliza un sistema de código rodante para asegurar la transmisión de señales. Este sistema de seguridad se usa en controles remotos para portones eléctricos, dando una capa adicional de seguridad contra la clonación de señales.

Seguridad: Para clonar un dispositivo con Rolling code, un atacante necesitaría conocer la semilla y el algoritmo específico, lo cual es casi imposible sin acceso físico al dispositivo y a sus componentes internos. Pero su desventaja que solo está diseñado para un par de mandos inalámbricos.

- **Costo:** 40 $
- **Mando:** 19 $ (Precio por unidad)

4.3.1.2 Opción 2: Receptora lineal

Los receptores lineales son dispositivos que se utilizan para controlar la apertura y cierre de puertas automáticas y portones eléctricos. Funcionan mediante la recepción de señales de control enviadas desde un mando a distancia, las cuales activan el mecanismo del motor para mover la puerta.

Seguridad: Estos dispositivos suelen incorporar tecnologías de seguridad para evitar accesos no autorizados, como el uso de códigos rodantes que cambian cada vez que se utiliza el mando, haciendo más difícil la clonación de la señal.

- **Costo:** 90$
- **Mando:** 25 $ (Precio por unidad)

4.3.1.3 Opción 3: Receptora Star 1000

El receptor STAR1000 de la marca LiftMaster es un dispositivo avanzado diseñado para control de acceso en aplicaciones comerciales, tales como puertas y portones eléctricos.

Seguridad: Este receptor destaca por su capacidad y seguridad mejorada gracias a la tecnología Security+ 2.0. El STAR1000 permite la programación individual y en bloque, lo que simplifica la gestión de múltiples controles remotos. Esto es útil en entornos donde se necesitan añadir o eliminar varios usuarios a la vez.

- **Costo:** 188 $
- **Mando:** 35 $ (Precio por unidad)

4.3.1.4 Opción 4: Diseño de placa no comercial

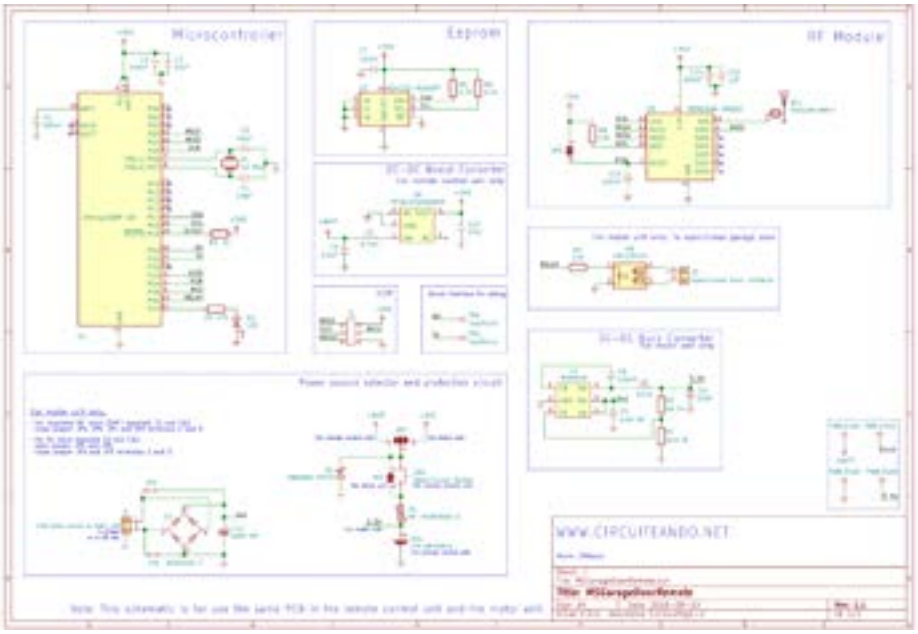
Como recomendación para mitigar este tipo de riesgo, se plantea el uso de un nuevo prototipo de tarjeta inalámbrica, que cuenta con un sistema de comunicación mucho más robusto. Este prototipo está programado con modulación FSK en vez de OOK, así como con una encriptación de hardware de 128 bits y hasta 128 claves de 32 bytes que se rotan continuamente(JG Reyes, 2019).

Esta tecnología de código rodante es la que está implementada en los otros mecanismos de portones eléctricos que no lograron ser vulnerados durante este análisis. En el Anexo 7.2.1 se establece los diferentes beneficios, presupuesto y análisis que tendrá el poder adaptar el prototipo a los sistemas que han tenido un resultado alarmante.

De igual manera en la Figura 37 se tiene de referencia el esquemático de las diferentes conexiones que son necesarias para poder realizar, tanto el mando inalámbrico, como el circuito receptor para el sistema del motor.

Figura 36

Esquemático electrónico de conexión



Fuente: Obtenido del sitio web: https://www.circuiteando.net/2019/01/msgaragedoorremote-parte-1-seguridad.html

De igual manera se tiene la Figura 38, que representa el diseño esquemático en PCB del mando inalámbrico, la cual están diseñada en 3D para poder identificar cada uno de los componentes electrónicos utilizados como también sus respectivas pistas.

Figura 37

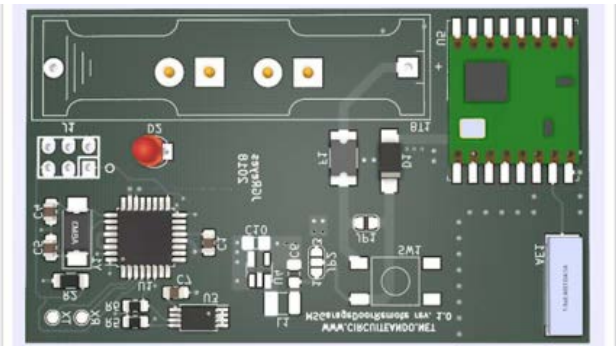
PCB frontal del mando inalámbrico

Fuente: Obtenido del sitio web: https://www.circuiteando.net/2019/01/msgaragedoorremote-parte-2-pcb-montaje.html

En la Figura 39 se tiene la placa PCB de la unidad inalámbrica para el motor igualmente modela en tercera dimensión para apreciar sus componentes.

Figura 38

PCB frontal de la unidad del motor

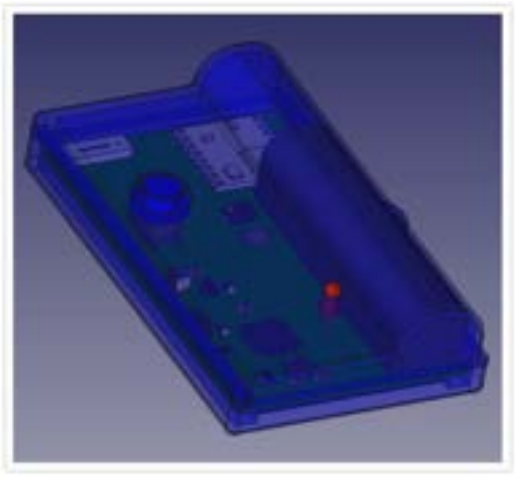


Fuente: Obtenido del sitio web: https://www.circuiteando.net/2019/01/msgaragedoorremote-parte-2-pcb-montaje.html

En la Figura 40 se tiene el diseño de la caja del mando inalámbrico que puede ser exportada en el software FreeCAD.

Figura 39

Caja impresa para el mando inalámbrico

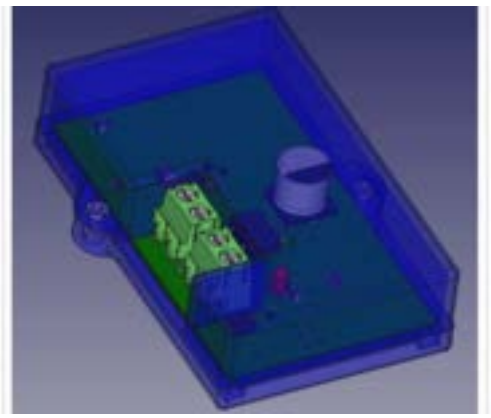


Fuente: Obtenido del sitio web: https://www.circuiteando.net/2019/01/msgaragedoorremote-parte-2-pcb-montaje.html

En la Figura 41 se tiene el diseño de la caja de la unidad del portón eléctrico que de igual manera puede ser exportada FreeCAD.

Figura 40

Caja impresa para la unidad del motor inalámbrico



Fuente: Obtenido del sitio web: https://www.circuiteando.net/2019/01/msgaragedoorremote-parte-2-pcb-montaje.html

En la Figura 42 se tiene una referencia de como tendría que ir las conexiones de la unidad del motor nueva para el sistema antigua en donde se tiene que verificar las respectivas entradas de poder y de igual manera de acción del portón.

Figura 41

Unidad nueva para los portones antiguos

Fuente: Obtenido del sitio web: https://www.circuiteando.net/2019/01/msgaragedoorremote-parte-2-pcb-montaje.html

4.3.2 Riesgo Medio

En el segundo caso de riesgo analizado, se encontró que en cinco escenarios el ataque 2 logró interceptar la señal inalámbrica del mando. Sin embargo, solo el escenario 4 se clasifica como de riesgo medio, ya que, aunque se capturaron los datos transmitidos, estos no lograron accionar el portón eléctrico.

Se determinó que los datos enviados no tienen ningún tipo de encriptación para prevenir este ataque. En este caso se establece utilizar una receptora no clonable que no permite que ningún tipo de ataque pueda interceptar las señales enviadas por los portones. Ya que estas tarjetas inalámbricas tienen la particularidad de poseer el Rolling Code, pero no son implementadas en un primer instante por un ahorro en su instalación. En la sección del ANEXO B.2 se establecen el informe de auditaría para el caso de un nivel de riesgo Medio.

4.3.3 Riesgo Muy Bajo

Para el caso de los dispositivos con un riesgo inalámbrico bajo, se tiene como resultado que en dos escenarios este tipo de riesgo no presentó vulnerabilidades. Ninguno de los ataques realizados pudo vulnerar ni interceptar los datos transmitidos. En este caso, los motores eléctricos demostraron ser altamente resistentes a los intentos de interceptación y manipulación de la señal por parte de los dispositivos SDR.

De acuerdo con los modelos investigados, estos presentan una seguridad inalámbrica robusta debido a su seguridad Security+ 2.0, lo que nos hace referencia a que posee la tecnología de código cambiante para asegurar que la señal transmitida sea única y segura cada vez que se utiliza. En la sección del ANEXO B.3 se detalla con mayor detalle las vulnerabilidades encontradas para un nivel de riesgo Muy Bajo.

5 Conclusiones y recomendaciones

5.1 Conclusiones

En definitiva, se encontraron varias vulnerabilidades en los sistemas de portones eléctricos analizados por los distintos dispositivos SDR. Las frecuencias de operación de estos dispositivos demostraron ser inseguras en su comunicación inalámbrica, presentando distintos niveles de riesgo, especialmente en aquellos dispositivos que no emplean tecnologías de código rodante o encriptación.

Los métodos de ataques utilizados por los dispositivos SDR como: Flipper Zero, RTL-SDR y ADALM-PLUTO, fueron efectivos en la mayoría de los escenarios planteados. La captura y retransmisión de señales de RF permitió acceder a los establecimientos privadas sin autorización de los dueños ocasionando que tengan un nivel de riesgo muy alto.

De acuerdo con los distintos ataques generados en los siete escenarios distintos, se evidencio que cinco presentaban un nivel de riesgo alto o moderado, lo que indica que más del 70% de los casos evaluados evidenciaron vulnerabilidades significativas en sus sistemas de seguridad.

La mayoría de portones eléctricos que poseen un nivel de riesgo muy alto es porque su bajo costo de adquisición, en donde los clientes opta por la opción más económica obviando temas de seguridad que puede instalarse desde un inicio.

La metodología Offensive Security demostró ser eficaz en la identificación de vulnerabilidades derivadas a la falta de seguridad inalámbrica que poseen los sistemas. Esta metodología permitió establecer con los niveles de riesgos asociados a cada escenario, facilitando la generación de recomendaciones de seguridad.

5.2 Recomendaciones

Se sugiere que los fabricantes de portones eléctricos implementen la tecnología de código rodante en sus mandos inalámbricos. Esta tecnología ha demostrado ser eficaz para evitar la clonación de señales y proporciona un nivel de seguridad más elevado frente a ataques.

Es fundamental que tanto fabricantes como usuarios gestionen adecuadamente los sistemas de portones eléctricos. Se recomienda establecer un período de actualización continua, no mayor a un año, tanto para el software como para el hardware, con el objetivo de proteger los dispositivos contra vulnerabilidades conocidas y nuevas amenazas emergentes.

Se recomienda llevar a cabo programas de concientización y capacitación sobre seguridad inalámbrica para los usuarios de portones eléctricos. Estos programas deben incluir información sobre la importancia del manejo correcto de los mandos para que no puedan clonados ni vulnerados por personas ajenas a sus establecimientos.

6 Referencias Bibliográficas

Aguirre, L. A. (2020). *Hacking & cracking. Redes inalámbricas wifi*. Marcombo.

Alfonso, L. (2022). *Luis Alfonso Ortega Olivares*. https://www.puertasautomaticasortega.com/blog/copiar-el-control-remoto-de-porton-electrico-es-seguro/

Aranda, M. Á. F. G. de. (2019). *Introducción a SDR con GNU Radio*. Marcombo.

Borbúa, R. V., Reyes, R. P., & Herrera, L. R. (2017). 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*, 31. https://doi.org/10.17141/urvio.20.2017.2571

Bottarelli, M., Epiphaniou, G., Ismail, D. K. Ben, Karadimas, P., & Al-Khateeb, H. (2018). Physical characteristics of wireless communication channels for secret key establishment: A survey of the research. *Computers & Security*, *78*, 454–476. https://doi.org/https://doi.org/10.1016/j.cose.2018.08.001

Briceño, E. V. (2021). *Seguridad de la información*. 3Ciencias.

Cañón, J. (2021). *Técnicas de modulación digital*. https://jorgecanon.com/tecnicas-de-modulacion-digital/

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., Quimiz, Á. L. M., & Merino, M. A. C. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. 3Ciencias.

Chiasserini, C. F., Gribaudo, M., & Manini, D. (2020). *Modelado analítico de sistemas de comunicación inalámbrica*. ISTE Group.

Devoteam. (2022). *Cybersecurity Auditing Devoteam Cyber Trust*. https://www.integritysec.es/offensive-security.html

Díaz, V. (2019). *Dos vehículos fueron robados de un condominio en el norte de Quito*. https://www.elcomercio.com/actualidad/seguridad/vehiculos-robo-condominio-san-carlos.html

Donat, W. (2021). *Explore Software Defined Radio*. Pragmatic Bookshelf.

Echeagaray, G. (2020). *Vdocuments.mx sistemas de comunicacion digitales y analogicos couch 7e*. https://www.academia.edu/42825776/Vdocuments_mx_sistemas_de_comunicacion_digitales_y_analogicos_couch_7e

Fiscalía General del Estado Cifras de robos. (2022). https://www.fiscalia.gob.ec/estadisticas-de-robos/

flipperzero. (2024). *Flipper Zero — Portable Multi-tool Device for Geeks*. https://flipperzero.one/

García Abad, A. (2021). *Campos electromagnéticos y medios de enlace entre receptor y transmisor: Guía de actividades*.

https://www.google.com.ec/books/edition/Campos_electromagn%C3%A9ticos_y_medios_de_en/iwt8zgEACAAJ?hl=es

Ghanem, A., & AlTawy, R. (2022). Garage Door Openers: A Rolling Code Protocol Case Study. *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, 1–6. https://doi.org/10.1109/PST55820.2022.9851991

Gutiérrez, O. E. (2017). *Comunicaciones moviles y redes inalámbricas*. Universitas.

Huidobro Moya, J. M. (2014). *Telecomunicaciones. Tecnologías, Redes y Servicios. 2ª edición actualizada*. https://www.google.com.ec/books/edition/Telecomunicaciones_Tecnolog%C3%ADas_Redes_y/CrA-DwAAQBAJ?hl=es&gbpv=0

INCIBE. (2021). *¡Fácil y sencillo! Análisis de riesgos en 6 pasos | Empresas | INCIBE*. https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo#:~:text=C%C3%A1lculo%20del%20riesgo,RIESGO%20%3D%20PROBABILIDAD%20x%20IMPACTO.

Irwin, L. (2021). How to implement and maintain an ISO 27001-compliant ISMS. In *IT Governance Blog En*. https://www.itgovernance.eu/blog/en/how-to-implement-an-isms-aligned-with-iso-27001-2

Isaza Villar, M. A. (2014). *Metodologías y Herramientas de Ethical Hacking*. https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

ITU. (2015). *Nomenclatura de las bandas de frecuencias y de las longitudes de onda empleadas en telecomunicaciones*.

JG Reyes. (2019). *MSGarageDoorRemote (Parte 2): PCB, montaje y demás.* https://www.circuiteando.net/2019/01/msgaragedoorremote-parte-2-pcb-montaje.html

Jiménez, J. (2020). *Flipper Zero, el tamagochi para hackers*. RedesZone. https://www.redeszone.net/reportajes/tecnologias/flipper-zero-tamagochi-hackers/

Kiser, Q. (2021). *Redes Informáticas: Una Guía Compacta para el principiante que Desea Entender los Sistemas de Comunicaciones, la Seguridad de las Redes, Conexiones de Internet, Ciberseguridad y Piratería*. Amazon Digital Services LLC - Kdp.

Kshetrimayum, R. (2009). An introduction to UWB communication systems. *IEEE Potentials*, *28*, 9–13. https://doi.org/10.1109/mpot.2009.931847

Kumar, M. S., Ramanathan, R., & Jayakumar, M. (2022). Key less physical layer security for wireless networks: A survey. *Engineering Science and Technology, an International Journal*, *35*, 101260. https://doi.org/https://doi.org/10.1016/j.jestch.2022.101260

Ley de Protección de Datos Personales. (2021). https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Madrid, R. (2021). *Bandas ingresan a parqueaderos de condominios para robar piezas de vehículos en Quito*. https://www.elcomercio.com/actualidad/seguridad/bandas-delictivas-condominios-robo-piezas-vehiculos.html

Marañón, G. Á. (2020). *Cómo protegernos de los peligros de Internet*. Los Libros De La Catarata.

MIGUEL LUIS, C. F., & MANUEL, G. A. S. B. (2020). *Instalaciones domóticas (Edición 2020)*. Editorial Paraninfo.

Monteros Túquerres, Á. I. (2019). *Diseño y elaboración de prácticas de laboratorio para la materia de fundamentos de comunicaciones usando radio definida por software* [Quito, 2019.]. http://bibdigital.epn.edu.ec/handle/15000/20182

Norberto Morel. (2016). *Técnico electricista 22 - Portones eléctricos, CCTV y cámaras IP*. https://books.google.com.ec/books?id=E-IaDQAAQBAJ

Olmedo, J. I., & Gavilánez, F. L. (2018). Análisis de los Ciberataques Realizados en América Latina. *INNOVA Research Journal*, *3*, 180–189. https://doi.org/10.33890/innova.v3.n9.2018.837

Parrales, W. M. A., Rodríguez, T. C. C., Cevallos, M. E. V., Santana, H. L. M., Pilozo, Á. R. D., Arias, F. J. T., Suárez, J. A. F., & Castro, V. F. R. (2019). *La ciberseguridad práctica aplicada a las redes, servidores y navegadores web*. 3Ciencias.

Pastor, J. (2023). *Desbloquea teléfonos, abre un BMW y cambia el precio de la gasolinera: Flipper Zero, el "tamagotchi para...* Xataka. https://www.xataka.com/seguridad/flipper-zero-tamagotchi-para-hackers-que-se-esta-haciendo-viral-tiktok-hay-buenas-razones-para-ello

Pedro J. (2023). *La seguridad de los portones eléctricos: ¿qué tan confiables son? - Portones automaticos chile*. https://portonesautomaticoschile.cl/que-tan-seguros-son-los-portones-electricos/#:~:text=%C2%BFSon%20vulnerables%20los%20portones%20autom%C3%A1ticos,las%20medidas%20de%20seguridad%20adecuadas.

Pérez, A. (2020). *La seguridad de las redes*. ISTE Group.

Pérez, R. G. (2018). *Mantenimiento preventivo de sistemas domóticos e inmóticos. ELEM0111*. IC Editorial.

Pujol, J. (2023). *Guía Completa para Copiar y Elegir Mandos de Garaje*. Tienda de electrónica online - TODOELECTRONICA. https://www.todoelectronica.com/blog-electronica/guia-completa-para-copiar-y-elegir-mandos-de-garaje.html

Reaves, B., & Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. *International Journal of Critical Infrastructure Protection*, *5*(3), 154–174. https://doi.org/https://doi.org/10.1016/j.ijcip.2012.10.001

Remote Control-LiftMaster. (2022). https://www.liftmaster.com/891lm-remote-control/p/G891LMMC

Reyland, J. M. (2023). *Software Defined Radio: Theory and Practice*. Artech House.

Ricardo, V. I. (2019). *Cálculo de Probabilidades 2*. Editorial UNED.

Ruiz, O. (2020). *Sistemas de Comunicación Digitales y Analógicos 7ma Edicion Leon W. Couch Lib*. https://www.academia.edu/43773829/Sistemas_de_Comunicaci%C3%B3n_Digitales_y_Anal%C3%B3gicos_7ma_Edicion_Leon_W_Couch_Lib

Sachan, V. K. (2020a). *Comunicaciones Inalámbricas: Principios, Diseños y Aplicaciones*. Amazon Digital Services LLC - KDP Print US.

Sachan, V. K. (2020b). *Fundamentos de las comunicaciones inalámbricas 5G*. https://www.google.com.ec/books/edition/Fundamentos_de_las_comunicaciones_inal%C3%A1/GKCazQEACAAJ?hl=es

Salazar, A. (2023). *Minutos de terror vivieron habitantes de un conjunto residencial en Tumbaco, en el nororiente de Quito*. El Universo. https://www.eluniverso.com/noticias/seguridad/robo-tumbaco-conjunto-fortuna-terror-vecinos-heridos-armados-policia-nota/

Stewart, R. W., Barlee, K. W., & Atkinson, D. S. W. (2015). *Software Defined Radio Using MATLAB & Simulink and the RTL-SDR*. Department of Electronic and Electrical Engineering, University of Strathclyde.

Tanaka, H., Suzuki, H., Watanabe, A., & Naito, K. (2018). *Evaluation of a secure end-to-end remote control system for smart home appliances*. unknown. https://www.researchgate.net/publication/324098371_Evaluation_of_a_secure_end-to-end_remote_control_system_for_smart_home_appliances

Tanenbaum, A. S. , & & Wetherall, D. J. (2012). *Redes de computadoras*. *5a.ed.*

Wyglinski, A. M., Getz, R., Collins, T., & Pu, D. (2018). *Software-Defined Radio for Engineers*. Artech House.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, *104*(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521

7 Anexos

A continuación, se presentan todos los anexos necesarios realizados para la investigación, los cuales incluyen los análisis técnicos de cada uno de los escenarios y ataques efectuados.

7.1 Anexo A: Evaluación de ataques según cada escenario

Se detallan los hallazgos encontrados en cada uno de los siete escenarios de prueba, con los tres ataques realizados a cada uno de ellos.

7.1.1 ANEXO A.1: Escenario 1

Como primer escenario de pruebas, se presentan los siguientes resultados de acuerdo con cada uno de los ataques realizados en la Fase 4. En este caso, se realizaron varias pruebas de penetración para el modelo de portón eléctrico descrito en la Tabla 14.

Tabla 25

Modelo de portón eléctrico para el Escenario 1

Modelo	**Característica**
[redacted]	Modelo de motor
[redacted]	Modelo del Control
[redacted]	Tarjeta de RX

7.1.1.1 Resultados del Ataque 1

En el primer ataque, se implementó el primer escenario, donde se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de [redacted] Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, el ataque se llevó a cabo dentro de un perímetro máximo de 7 metros de distancia del motor, obteniendo una captura perfecta de la señal inalámbrica del control. Más allá de esta distancia, la señal es mucho menos intensa tanto para transmitir como para recibir.

7.1.1.2 Resultados del Ataque 2

Para el segundo ataque del primer escenario, se realizó una prueba de vulnerabilidad en un motor de la marca Roger (H30). Se utilizó el mando [redacted] con una frecuencia de operación de 433.92 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, se identificaron con facilidad los datos transmitidos por el mando Roger, creando así una brecha de seguridad en la confiabilidad de los datos.

7.1.1.3 Resultados del Ataque 3

Para el tercer ataque del primer escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 433.92 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, se logró retransmitir la señal capturada del segundo ataque para accionar el sistema del portón

eléctrico a una distancia de 5 metros del motor utilizando el dispositivo ADALM-PLUTO.

7.1.2 ANEXO A.2: Escenario 2

Para el segundo escenario de pruebas, se presentan los siguientes resultados de acuerdo con cada uno de los ataques realizados en la Fase 4. En este caso, se llevaron a cabo varias pruebas de penetración para el modelo de portón eléctrico descrito en la Tabla 15.

Tabla 26

Modelo de portón eléctrico para el Escenario 2

Modelo	**Característica**
[redacted]	Modelo de motor
[redacted]	Modelo del Control

7.1.2.1 Resultados del Ataque 1

En el primer ataque, se implementó el primer escenario, donde se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 433.92 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, el ataque se llevó a cabo dentro de un perímetro máximo de 7 metros de distancia del motor, obteniendo una captura perfecta de la señal inalámbrica del control. Más allá de esta distancia, la señal es mucho menos intensa tanto para transmitir como para recibir.

7.1.2.2 Resultados del Ataque 2

Para el segundo ataque del segundo escenario, donde se realizó la prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con la frecuencia de operación de 433.92 MHz. Se pudo evidenciar que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso se logró identificar con facilidad los datos transmitidos del mando Roger creando así brecha de seguridad de la confiabilidad de los datos transmitidos dentro de un radio igual a los 5 metros.

7.1.2.3 Resultados del Ataque 3

Para el tercer ataque del segundo escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 433.92 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, se logró retransmitir la señal capturada del segundo ataque para accionar el sistema del portón eléctrico a una distancia de 5 metros del motor utilizando el dispositivo ADALM-PLUTO.

7.1.3 ANEXO A.3: Escenario 3

Para el tercer escenario de pruebas, se presentan los siguientes resultados de acuerdo con cada uno de los ataques realizados en la Fase 4. En este caso, se llevaron

a cabo varias pruebas de penetración para el modelo de portón eléctrico descrito en la Tabla 16.

Tabla 27

Modelo de portón eléctrico para el Escenario 3

Modelo	**Característica**
[redacted]	Modelo de motor
[redacted]	Modelo del Control

7.1.3.1 Resultados del Ataque 1

En el primer ataque dentro de las pruebas del tercer escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con la frecuencia de operación del fabricante de 315 MHz. Se evidenció que no hubo ningún tipo de impacto, ya que no se logró el objetivo del ataque. En este caso, se realizaron diversas pruebas en diferentes frecuencias, sin lograr un efecto negativo en la integridad de la transmisión de los datos.

De acuerdo con (*Remote Control-LiftMaster,* 2022), el mando [redacted] es compatible con sistemas de seguridad Security+ 2.0, lo que significa que utiliza tecnología de código cambiante para asegurar que la señal transmitida sea única y segura cada vez que se utiliza. Esta tecnología, también conocida como rolling code, genera un nuevo código de seguridad cada vez que se presiona el botón del mando. Esto previene que los atacantes puedan interceptar y reutilizar la señal, ya que el código cambia con cada uso, haciendo imposible predecir el siguiente código válido. Además,

Security+ 2.0 ofrece una encriptación avanzada que protege aún más la comunicación entre el mando y el receptor, asegurando que la señal no pueda ser fácilmente descifrada. Esta combinación de tecnología de código cambiante y encriptación robusta proporciona un alto nivel de seguridad, reduciendo significativamente el riesgo de acceso no autorizado y garantizando que solo los usuarios legítimos puedan operar el sistema.

7.1.3.2 Resultados del Ataque 2

Para el segundo ataque del tercer escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 315 MHz. En este caso, no se logró realizar la captura con los dispositivos RTL-SDR, ya que los sistemas poseen FHSS (Frequency-Hopping Spread Spectrum), que ayuda a cambiar rápidamente de frecuencia dentro de un rango específico durante la transmisión. Esto dificulta la interceptación de la señal y su análisis en el software GQRX. Para los sistemas [redacted] el rango de frecuencia es de 902–928 MHz, proporcionando una comunicación segura y confiable atreves de su aplicación móvil(*Remote Control-LiftMaster,* 2022).

7.1.3.3 Resultados del Ataque 3

Para el tercer ataque del séptimo escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 315 MHz. Se evidenció que no se logró el objetivo del ataque. Esto debido a la tecnología FHSS que no permite la captura de datos para poder ser enviados mediante el dispositivo ADALM-PLUTO.

7.1.4 ANEXO A.4: Escenario 4

Para el cuarto escenario, se presentan los siguientes resultados de acuerdo con cada uno de los ataques realizados en la Fase 4. En este caso, se llevaron a cabo varias pruebas de penetración para el modelo de portón eléctrico descrito en la Tabla 17.

Tabla 28

Modelo de portón eléctrico para el Escenario 4

Modelo	**Característica**
[redacted]	Modelo de motor
[redacted]	Modelo del Control

7.1.4.1 Resultados del Ataque 1

En el primer ataque dentro de las pruebas del cuarto escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con la frecuencia de operación técnica del motor de triple banda de 310, 315 y 390 MHz. Se evidenció que no hubo ningún tipo de impacto, ya que no se logró el objetivo del ataque. En este caso, se realizaron diversas pruebas en diferentes frecuencias, sin que ninguna tuviera un efecto negativo en la integridad de la transmisión de los datos.

De acuerdo con (*Remote Control-LiftMaster*, 2022) el mando [redacted] es compatible con sistemas de seguridad Security+ 2.0, lo que significa que utiliza tecnología de código cambiante para asegurar que la señal transmitida sea única y segura cada vez que se utiliza.

7.1.4.2 Resultados del Ataque 2

Para el segundo ataque del cuarto escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted]. Se utilizó el mando [redacted] con una frecuencia de operación de 315 MHz. En este caso, no se logró realizar la captura con los dispositivos RTL-SDR, ya que los sistemas poseen FHSS (Frequency-Hopping Spread Spectrum), que ayuda a cambiar rápidamente de frecuencia dentro de un rango específico durante la transmisión. Esto dificulta la interceptación de la señal y su análisis en el software GQRX. Para los sistemas MyQ, el rango de frecuencia es de 902–928 MHz, proporcionando una comunicación segura y confiable(*Remote Control-LiftMaster*, 2022).

7.1.4.3 Resultados del Ataque 3

Para el tercer ataque del séptimo escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 315 MHz. Se evidenció que no se logró el objetivo del ataque. Esto debido a la tecnología FHSS que no permite la captura de datos para poder ser enviados mediante el dispositivo ADALM-PLUTO.

7.1.5 ANEXO A.5: Escenario 5

Para el quinto escenario de pruebas, se presentan los siguientes resultados de acuerdo con cada uno de los ataques realizados en la Fase 4. En este caso, se llevaron a cabo varias pruebas de penetración para el modelo de portón eléctrico descrito en la Tabla 18.

Tabla 29

Modelo de portón eléctrico para el Escenario 5

Modelo	Característica
[redacted]	Modelo de motor
[redacted]	Modelo del Control

7.1.5.1 Resultados del Ataque 1

En el primer ataque dentro de las pruebas del cuarto escenario, se realizó una prueba de vulnerabilidad en un motor de la marca Peccinin (Light 500). Se utilizó el mando genérico Digital RF 3C con una frecuencia de operación de 433.95 MHz. Se evidenció que el impacto no se produjo, ya que no se logró el objetivo del ataque. En este caso, se realizaron diversas pruebas sin que ninguna tuviera un efecto negativo en la integridad de la transmisión de los datos. Los controles remotos del motor Peccinin Light 500 utilizan tecnología de código variable, lo cual significa que cada vez que se utiliza el control remoto, se genera un código único y diferente, evitando así que los códigos puedan ser clonados o interceptados por intrusos.

7.1.5.2 Resultados del Ataque 2

Para el segundo ataque del quinto escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando genérico [redacted] con una frecuencia de operación de 433.95 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, se identificaron con facilidad los datos transmitidos por el mando Peccinin, creando así una brecha de seguridad en la confiabilidad de los datos.

7.1.5.3 Resultados del Ataque 3

Para el tercer ataque del séptimo escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 433.95 MHz. Se evidenció que no se logró el objetivo del ataque. Esto debido a que los motores poseen la tecnología de código cambiante, evitando que se pueda clonar los mandos que no están configurados en el sistema del motor.

7.1.6 ANEXO A.6: Escenario 6

Para el sexto escenario de pruebas, se presentan los siguientes resultados de acuerdo con cada uno de los ataques realizados en la Fase 4. En este caso, se llevaron a cabo varias pruebas de penetración para el modelo de portón eléctrico descrito en la Tabla 19.

Tabla 30

Modelo de portón eléctrico para el Escenario 6

Modelo	Característica
[redacted]	Modelo de motor
[redacted]	Modelo del Control

7.1.6.1 Resultados del Ataque 1

En el primer ataque dentro de las pruebas del sexto escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando genérico [redacted] con una frecuencia de operación de 433.95

MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, el ataque se llevó a cabo dentro de un perímetro máximo de 7 metros de distancia del motor, obteniendo una captura perfecta de la señal inalámbrica del control. Más allá de esta distancia, la señal es mucho menos intensa tanto para transmitir como para recibir.

7.1.6.2 Resultados del Ataque 2

Para el segundo ataque del sexto escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando genérico [redacted] con una frecuencia de operación de 433.92 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, se identificaron con facilidad los datos transmitidos por el mando, creando así una brecha de seguridad en la confiabilidad de los datos.

7.1.6.3 Resultados del Ataque 3

Para el tercer ataque del sexto escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando genérico [redacted] con una frecuencia de operación de 433.92 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, se logró retransmitir la señal capturada del segundo ataque para accionar el sistema del portón eléctrico a una distancia de 5 metros del motor utilizando el dispositivo ADALM-PLUTO.

7.1.7 ANEXO A.7: Escenario 7

Para el séptimo escenario de pruebas, se presentan los siguientes resultados de acuerdo con cada uno de los ataques realizados en la Fase 4. En este caso, se llevaron a cabo varias pruebas de penetración para el modelo de portón eléctrico descrito en la Tabla 20.

Tabla 31

Modelo de portón eléctrico para el Escenario 7

Modelo	**Característica**
[redacted]	Modelo de motor
[redacted]	Modelo del Control

7.1.7.1 Resultados del Ataque 1

En el primer ataque del séptimo escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando [redacted] con una frecuencia de operación de 433.925 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, el ataque se llevó a cabo dentro de un perímetro máximo de 5 metros de distancia del motor, obteniendo una captura perfecta de la señal inalámbrica del control. Más allá de esta distancia, la señal es mucho menos intensa tanto para transmitir como para recibir.

7.1.7.2 Resultados del Ataque 2

Para el segundo ataque, del primer escenario, donde se realizó la prueba de vulnerabilidad en un motor de la marca Roger (BG30/1004/HS). Se utilizó el mando

APA368 con la frecuencia de operación de 433.92 MHz. Se pudo evidenciar que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso se logró identificar con facilidad los datos transmitidos del mando Roger creando así brecha de seguridad de la confiabilidad de los datos.

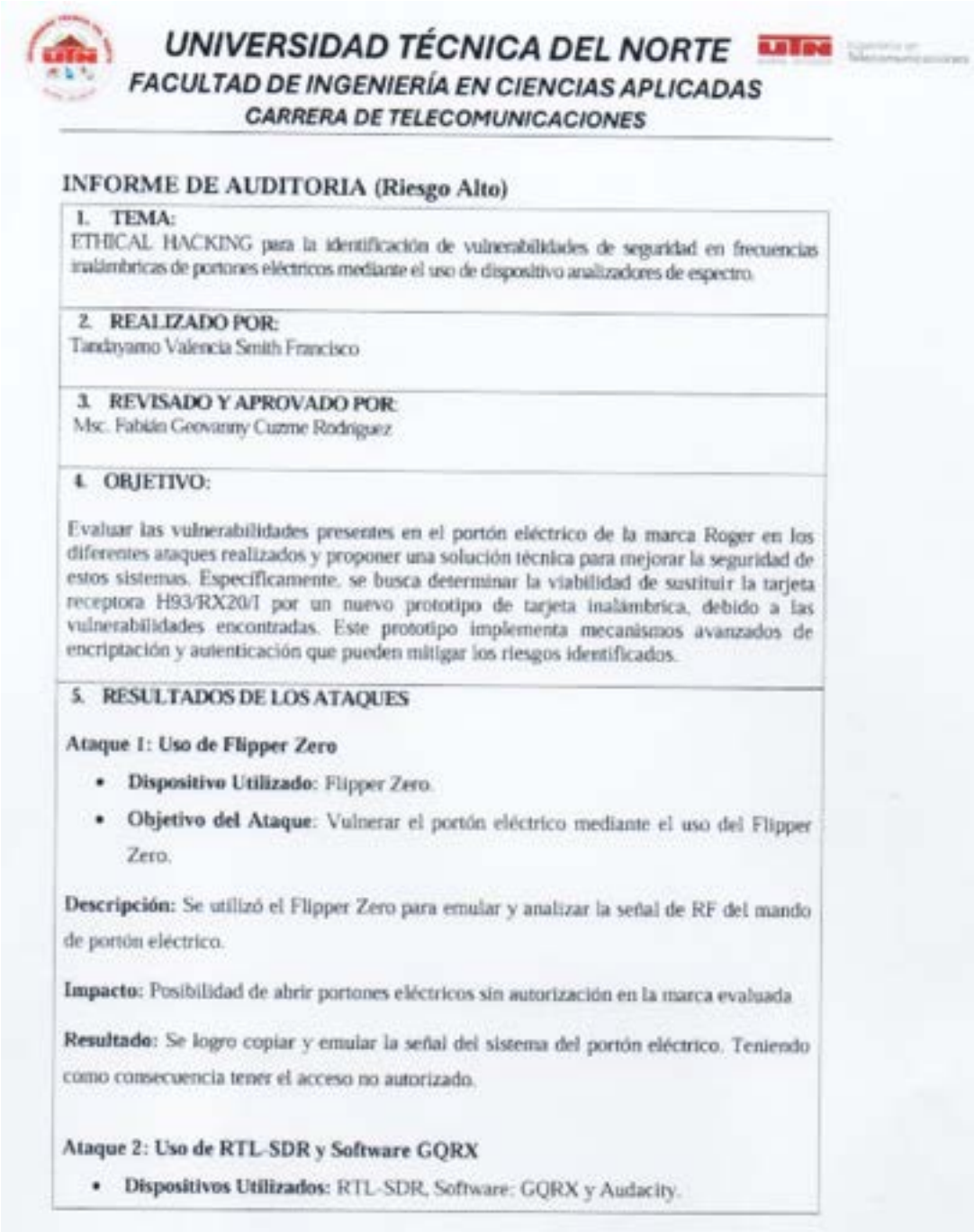
7.1.7.3 Resultados del Ataque 3

Para el tercer ataque del séptimo escenario, se realizó una prueba de vulnerabilidad en un motor de la marca [redacted] Se utilizó el mando genérico [redacted] con una frecuencia de operación de 433.92 MHz. Se evidenció que el impacto fue negativo, ya que se logró el objetivo del ataque. En este caso, se logró retransmitir la señal capturada del segundo ataque para accionar el sistema del portón eléctrico a una distancia de 5 metros del motor utilizando el dispositivo ADALM-PLUTO.

7.2 ANEXO B: Informe de Auditoria

En el Anexo 7 se presentan los informes de auditoría correspondientes a cada uno de los casos analizados. Estos informes se clasifican en tres tipos distintos, dependiendo del grado de riesgo identificado durante las pruebas de penetración realizadas.

7.2.1 ANEXO B.1: INFORME DE AUDITORIA (Riesgo Alto)



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

INFORME DE AUDITORIA (Riesgo Alto)

1. TEMA:
ETHICAL HACKING para la identificación de vulnerabilidades de seguridad en frecuencias inalámbricas de portones eléctricos mediante el uso de dispositivo analizadores de espectro.

2. REALIZADO POR:
Tandayamo Valencia Smith Francisco

3. REVISADO Y APROVADO POR:
Msc. Fabián Geovanny Cuzme Rodríguez

4. OBJETIVO:

Evaluar las vulnerabilidades presentes en el portón eléctrico de la marca Roger en los diferentes ataques realizados y proponer una solución técnica para mejorar la seguridad de estos sistemas. Específicamente, se busca determinar la viabilidad de sustituir la tarjeta receptora H93/RX20/T por un nuevo prototipo de tarjeta inalámbrica, debido a las vulnerabilidades encontradas. Este prototipo implementa mecanismos avanzados de encriptación y autenticación que pueden mitigar los riesgos identificados.

5. RESULTADOS DE LOS ATAQUES

Ataque 1: Uso de Flipper Zero

- **Dispositivo Utilizado**: Flipper Zero.
- **Objetivo del Ataque**: Vulnerar el portón eléctrico mediante el uso del Flipper Zero.

Descripción: Se utilizó el Flipper Zero para emular y analizar la señal de RF del mando de portón eléctrico.

Impacto: Posibilidad de abrir portones eléctricos sin autorización en la marca evaluada

Resultado: Se logro copiar y emular la señal del sistema del portón eléctrico. Teniendo como consecuencia tener el acceso no autorizado.

Ataque 2: Uso de RTL-SDR y Software GQRX

- **Dispositivos Utilizados:** RTL-SDR, Software: GQRX y Audacity.

- **Objetivo del Ataque:** Interceptar y capturar señales de mandos inalámbricos de portones eléctricos.

Descripción: Configuración de RTL-SDR con GQRX para escuchar y guardar señales inalámbricas para identificar los datos enviados.

Impacto: Facilita la reproducción de señales de control, posibilitando la apertura no autorizada de portones.

Resultado: El ataque permite interceptar y analizar señales RF de mandos inalámbricos, demostrando la falta de cifrado en las marcas vulneradas.

Ataque 3: Uso ADALM PLUTO

- **Dispositivos Utilizados:** ADALM-PLUTO, Software: MATLAB
- **Objetivo del Ataque:** Replicar y transmitir señales del mando inalámbrico capturado para abrir portones eléctricos.

Descripción: Uso de MATLAB y ADALM-Pluto para procesar y transmitir señales en diferentes modulaciones de operación

Impacto: Posibilidad de programar códigos que permitan abrir los portones eléctricos replicando señales legítimas de un mando original.

Resultado: El ataque permitió replicar la señal RF del mando inalámbrico

- **Resultado General**

	Resultado
Ataque 1	SI
Ataque 2	SI
Ataque 3	SI

6. RECOMENDACIÓN

En este caso, hay un nivel alto de riesgo en el sistema inalámbrico del portón eléctrico, en el que existen diferentes formas de mitigar este tipo de riesgo. Luego, se plantea el uso de estos dispositivos como costos para implementarse.

6.1. Opción 1: Receptora no clonable

El dispositivo receptor no clonable H90 es un receptor que utiliza un sistema de código rodante (rolling code) para asegurar la transmisión de señales. Este sistema de seguridad se usa en controles remotos para portones eléctricos, dando una capa adicional de seguridad contra la clonación de señales.

Seguridad: Para clonar un dispositivo con rolling code, un atacante necesitaría conocer la semilla y el algoritmo específico, lo cual es casi imposible sin acceso físico al dispositivo y a sus componentes internos. Pero su desventaja que solo está diseñado para un par de mandos inalámbricos.

- **Costo**: 40 $
- **Mando**: 19 $

6.2. Opción 2: Receptora lineal

Los receptores lineales son dispositivos que se utilizan para controlar la apertura y cierre de puertas automáticas y portones eléctricos. Funcionan mediante la recepción de señales de control enviadas desde un mando a distancia, las cuales activan el mecanismo del motor para mover la puerta.

Seguridad: Estos dispositivos suelen incorporar tecnologías de seguridad para evitar accesos no autorizados, como el uso de códigos rodantes (rolling code) que cambian cada vez que se utiliza el mando, haciendo más difícil la clonación de la señal.

- **Costo**: 90$
- **Mando**: 25 $

6.3. Opción 3: Receptora Star 1000

El receptor STAR1000 de la marca LiftMaster es un dispositivo avanzado diseñado para control de acceso en aplicaciones comerciales, tales como puertas y portones eléctricos.

Este receptor destaca por su capacidad y seguridad mejorada gracias a la tecnología Security+ 2.0. El STAR1000 permite la programación individual y en bloque, lo que simplifica la gestión de múltiples controles remotos. Esto es útil en entornos donde se necesitan añadir o eliminar varios usuarios a la vez.

- Costo: 188 $
- Mando: 17 $

6.4. Opción 4: Diseño de placa no comercial

De acuerdo con los hallazgos encontrados por los diferentes ataques realizados, se logró identificar que el sistema de comunicación inalámbrica puede ser objeto de diversos problemas de seguridad. Por lo tanto, se recomienda una mejora en el sistema inalámbrico implementado un nuevo prototipo de tarjeta inalámbrica que contiene mayor seguridad.
En la siguiente tabla se especifica los componentes y cantidades necesarias para realizar el prototipo.

Componente	Referencia	Valor	Cantidad	Precio Unitario (USD)	Precio Total (USD)
Antena cerámica	AE1	ACAG1204-868-T	2	1.50	3.00
Celda de batería	BT1	1.5V AAA	1	0.50	0.50
Capacitor no polarizado	C1, C2, C7, C8, C13, C14	100nF	11	0.05	0.55
Capacitor no polarizado	C3	10uF	2	0.10	0.20
Capacitor no polarizado	C4, C5	18pF	4	0.10	0.40

Capacitor no polarizado	C15	1uF	2	0.10	0.20
Capacitor no polarizado	C6	2.2uF	1	0.10	0.10
Capacitor no polarizado	C9	2.2uF 50V	1	0.20	0.20
Capacitor polarizado	C12	220uF 50V	1	0.50	0.50
Capacitor no polarizado	C10, C11	22uF	2	0.10	0.20
Puente de diodos	D3	DF1501S-T	1	0.50	0.50
LED genérico	D2	LED	2	0.05	0.10
Diodo Schottky	D1	RB068LAM-40TFTR	2	0.10	0.20
Fusible reseteable	F1	MF-MSMF050-2	2	0.50	1.00
Terminal de tornillo	J2	-	1	0.20	0.20
HEADER 3x2	J1	ICSP	2	0.10	0.20
Terminal de tornillo	J3	-	1	0.20	0.20

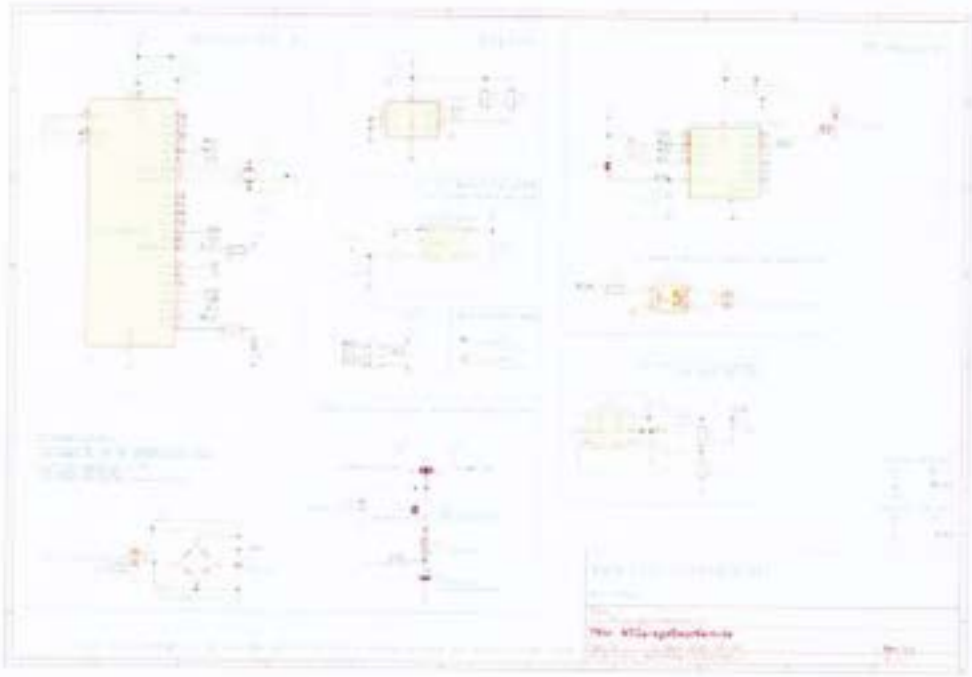
Jumper normalmente abierto	JP4, JP5	Jumper_NO_Small	2	0.05	0.10
Jumper soldable 2-polos	JP1, JP3	SolderJumper	2	0.05	0.10
Jumper soldable 3-polos	JP2	SolderJumper	1	0.05	0.05
Inductor	L2	12uH	1	0.50	0.50
Inductor	L1	4.7uH	1	0.50	0.50
Resistor	R2	1k	2	0.05	0.10
Resistor	R4	22.1k 1%	1	0.05	0.05
Resistor	R5, R6	4.7k	4	0.05	0.20
Resistor	R1, R7	470	3	0.05	0.15
Resistor	R3	51k 1%	1	0.05	0.05
Pulsador	SW1	Open/Close Button	1	0.20	0.20
Microcontrolador	U1	ATmega328P-AU	2	2.00	4.00
Relay de estado sólido	U6	CPC1017N	1	1.00	1.00
EEPROM serial	U3	M24C32-RDW6TP	2	0.50	1.00
Módulo transceptor RF	U5	RFM69HW-868S2	2	2.50	5.00

Convertidor DC-DC	U2	TPS560430	1	1.00	1.00
Convertidor Boost	U4	TPS613221ADBVR	1	1.00	1.00
Cristal 16 MHz	Y1	-	2	0.20	0.40
Resistor	R8	10k	2	0.05	0.10
				Total	23.90

Se igual manera se tiene los gastos adicionales como es el montaje de todo el circuito y la programación. También se requiere las cajas impresas para proteger todo el circuito, teniendo así un valor aproximado final.

Total, costo aproximado sobre componentes electrónicos:	$23.90
Gasto de mano de obra: $	$ 80
Gasto de impresión de cajas PCB: $	**$** 45
Total, final	**$148.9**

El diseño del prototipo se encuentra en la siguiente Figura. en donde se establecen todas sus respectivas conexiones.



Nota: Fuente: https://gitlab.com/JGReyes/msgaragedoorremote/-/blob/master/MSGarageDoorRemote(Schematic).pdf

La placa propuesta posee las siguientes características.

- **Frecuencia de Operación**: La placa opera en 433.92 MHz, compatible con el motor Roger (H30).
- **Modulación**: Utiliza FSK con encriptación AES, mejorando la seguridad.
- **Control de Señales:** Puede generar y enviar comandos encriptados, lo cual es esencial para prevenir ataques de repetición y otros tipos de intrusiones.
- **Seguridad:** Implementación de códigos rodantes, lo que añade una capa adicional de seguridad.

7. ANÁLISIS COMPARATIVO

La evaluación se estructura en dos cuadros principales: el análisis físico y el análisis lógico. Estos cuadros proporcionan una visión clara de las características de cada tarjeta y las adaptaciones necesarias para asegurar una integración exitosa del prototipo en el sistema existente.

- **Cuadro de Análisis Físico**

El primer cuadro compara aspectos físicos como la alimentación, dimensiones, montaje y conexiones. Se destaca la compatibilidad de la alimentación y la necesidad de ajustes menores, así como la verificación de espacio y adaptación de conexiones para asegurar un montaje firme y seguro.

Aspecto	Tarjeta H93/RX20/1	Prototipo de Circuiteando.net	Compatibilidad / Requisitos
Alimentación	5V DC	3.3V o 5V	Compatible con ajustes menores (adaptador de voltaje)
Dimensiones y Montaje	34 x 31 x 12 mm	Personalizado según diseño	Verificar espacio disponible en el cuadro de control
Conexiones	Pines específicos para control	Pines GPIO para control de motor y lectura de sensores y energización de la placa.	Adaptación física necesaria para asegurar conexiones firmes y seguras

- **Cuadro de Análisis Lógico**

El segundo cuadro aborda el análisis lógico, incluyendo el protocolo de comunicación, los mecanismos de seguridad y las pruebas funcionales. Se subraya la necesidad de implementar un receptor adecuado para el protocolo encriptado y la mejora significativa en seguridad que ofrece el prototipo.

Aspecto	Tarjeta H93/RX20/I	Prototipo de Circuiteando.net	Compatibilidad / Requisitos
Protocolo de Comunicación	Código Fijo. AM/ASK, 433.92 MHz	Comunicación encriptada y autenticación. FSK 868 MHz	Compatible
Mecanismos de Seguridad	Codificación de código fijo	Encriptación avanzada, anti clonación	Prototipo ofrece mejoras significativas en seguridad
Pruebas Funcionales	Control de apertura y cierre mediante señales digitales	Control mediante señales digitales	Requiere pruebas exhaustivas para asegurar compatibilidad y funcionamiento correcto

7.1. Pasos para la Implementación:

Dimensiones y Montaje:

- **Paso:** Medir las dimensiones del PCB del prototipo.
- **Acción:** Asegurarse de que hay suficiente espacio en el cuadro de control H70/104AC para montar la placa. Utilizar separadores o soportes si es necesario.

Conexiones:

- **Paso:** Identificar los terminales de control del motor y los sensores de fin de carrera en el cuadro de control H70/104AC.
- **Acción:** Conectar los pines GPIO de la placa del prototipo a estos terminales utilizando cables y conectores compatibles. Asegurarse de que las conexiones son firmes y seguras.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Protocolo de Comunicación:

- **Paso:** Verificar la compatibilidad del protocolo de comunicación del prototipo con el receptor de RF del portón.
- **Acción:** Programar la placa del prototipo para que utilice el mismo protocolo y frecuencia de operación que el receptor de RF del portón.

Implementación de Mecanismos de Seguridad:

- **Paso:** Programar el microcontrolador del prototipo para que implemente mecanismos de encriptación y autenticación avanzados.
- **Acción:** Verificar que las señales encriptadas sean correctamente interpretadas y aceptadas por el receptor de RF del portón.

La tarjeta H93/RX20/1 puede ser sustituida por el prototipo de tarjeta inalámbrica, siempre que se realicen las adaptaciones necesarias en la alimentación y las conexiones propuestas en los pasos anteriores. La implementación de los mecanismos de seguridad avanzados del prototipo proporciona una protección superior contra ataques de suplantación y jamming, asegurando una operación segura y confiable del sistema del portón eléctrico de la marca Roger.

Ing. Fabián Cuzme MSc
DIRECTOR

Tandayamo Smith

Vivar Eduardo
Presidente Urbanización

7.2.2 ANEXO B.2: INFORME DE AUDITORIA (Riesgo Medio)

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE TELECOMUNICACIONES

INFORME DE AUDITORIA (Riesgo Medio)

1. TEMA:

ETHICAL HACKING para la identificación de vulnerabilidades de seguridad en frecuencias inalámbricas de portones eléctricos mediante el uso de dispositivo analizadores de espectro.

2. REALIZADO POR:

Tandayamo Valencia Smith Francisco

3. REVISADO Y APROVADO POR:

Msc. Fabián Geovanny Cuzme Rodríguez

4. OBJETIVO:

Evaluar las vulnerabilidades presentes en el portón eléctrico de la marca Peccinnin (Light 500) en los diferentes ataques realizados y proponer una solución técnica para mejorar la seguridad de estos sistemas en caso de existir algún tipo de vulnerabilidad encontrada.

5. RESULTADOS DE LOS ATAQUES

Ataque 1: Uso de Flipper Zero

- **Dispositivo Utilizado:** Flipper Zero.
- **Objetivo del Ataque**: Vulnerar el portón eléctrico mediante el uso del Flipper Zero.

Descripción: Se utilizó el Flipper Zero para emular y analizar la señal de RF del mando de portón eléctrico.

Impacto: Posibilidad de abrir portones eléctricos sin autorización en la marca evaluada

Resultado: No se logró copiar y emular la señal del sistema del portón eléctrico.

Ataque 2: Uso de RTL-SDR y Software GQRX

- **Dispositivos Utilizados:** RTL-SDR, Software: GQRX y Audacity.
- **Objetivo del Ataque:** Interceptar y capturar señales de mandos inalámbricos de portones eléctricos.

Descripción: Configuración de RTL-SDR con GQRX para escuchar y guardar señales inalámbricas para identificar los datos enviados.

Impacto: Facilita la reproducción de señales de control, posibilitando la apertura no autorizada de portones.

Resultado: El ataque permitió interceptar la señal RF del mando inalámbrico.

Ataque 3: Uso ADALM PLUTO

- **Dispositivos Utilizados**: ADALM-PLUTO, Software: MATLAB
- **Objetivo del Ataque**: Replicar y transmitir señales del mando inalámbrico capturado para abrir portones eléctricos.

Descripción: Uso de MATLAB y ADALM-Pluto para procesar y transmitir señales en diferentes modulaciones de operación

Impacto: Posibilidad de programar códigos que permitan abrir los portones eléctricos replicando señales legítimas de un mando original.

Resultado: El ataque no permitió replicar la señal RF del mando inalámbrico

- **Resultado General**

	Resultado
Ataque 1	NO
Ataque 2	SI
Ataque 3	NO

6. RECOMENDACIÓN

6.1. Implementación receptora no clonable

El dispositivo receptor no clonable H90 es un receptor que utiliza un sistema de código rodante (rolling code) para asegurar la transmisión de señales. Este sistema de seguridad se usa en controles remotos para portones eléctricos, dando una capa adicional de seguridad contra la clonación de señales.

Seguridad: Para clonar un dispositivo con rolling code, un atacante necesitaría conocer la semilla y el algoritmo específico, lo cual es casi imposible sin acceso físico al dispositivo y a sus componentes internos. Pero su desventaja que solo está diseñado para un par de mandos inalámbricos.

- **Costo:** 40 $
- **Mando:** 19 $

6.2. Opción 2: Receptora lineal

Los receptores lineales son dispositivos que se utilizan para controlar la apertura y cierre de puertas automáticas y portones eléctricos. Funcionan mediante la recepción de señales de control enviadas desde un mando a distancia, las cuales activan el mecanismo del motor para mover la puerta.

Seguridad: Estos dispositivos suelen incorporar tecnologías de seguridad para evitar accesos no autorizados, como el uso de códigos rodantes (rolling code) que cambian cada vez que se utiliza el mando, haciendo más difícil la clonación de la señal.

- **Costo:** 90$
- **Mando:** 25 $

Se recomienda priorizar la implementación de un dispositivo con tecnología de código rodante, ya sea a través del receptor H90 o una receptora lineal. Ambos ofrecen mejoras significativas en seguridad al dificultar la reproducción de señales no autorizadas. La elección dependerá del presupuesto disponible y del número de mandos que se requiera controlar.

Ing. Fabián Cuzme MSc
DIRECTOR

Tandayamo Smith

Pedro Terán

7.2.3 ANEXO B.3: INFORME DE AUDITORIA (Riesgo Bajo)

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE TELECOMUNICACIONES

INFORME DE AUDITORIA (Riesgo bajo)

1. TEMA:
ETHICAL HACKING para la identificación de vulnerabilidades de seguridad en frecuencias inalámbricas de portones eléctricos mediante el uso de dispositivo analizadores de espectro.

2. REALIZADO POR:
Tandayamo Valencia Smith Francisco

3. REVISADO Y APROVADO POR:
Msc. Fabián Geovanny Cuzme Rodríguez

4. OBJETIVO:
Evaluar las vulnerabilidades presentes en el portón eléctrico de la marca LiftMaster (8587WL) en los diferentes ataques realizados y proponer una solución técnica para mejorar la seguridad de estos sistemas en caso de existir algún tipo de vulnerabilidad encontrada.

5. RESULTADOS DE LOS ATAQUES

Ataque 1: Uso de Flipper Zero

- **Dispositivo Utilizado:** Flipper Zero.
- **Objetivo del Ataque**: Vulnerar el portón eléctrico mediante el uso del Flipper Zero.

Descripción: Se utilizó el Flipper Zero para emular y analizar la señal de RF del mando de portón eléctrico.

Impacto: Posibilidad de abrir portones eléctricos sin autorización en la marca evaluada

Resultado: No se logró copiar y emular la señal del sistema del portón eléctrico.

Ataque 2: Uso de RTL-SDR y Software GQRX

- **Dispositivos Utilizados:** RTL-SDR, Software: GQRX y Audacity.
- **Objetivo del Ataque:** Interceptar y capturar señales de mandos inalámbricos de portones eléctricos.

Descripción: Configuración de RTL-SDR con GQRX para escuchar y guardar señales inalámbricas para identificar los datos enviados.

Impacto: Facilita la reproducción de señales de control, posibilitando la apertura no autorizada de portones.

Resultado: El ataque no permitió interceptar la señal RF del mando inalámbrico.

Ataque 3: Uso ADALM PLUTO

- **Dispositivos Utilizados:** ADALM-PLUTO, Software: MATLAB
- **Objetivo del Ataque:** Replicar y transmitir señales del mando inalámbrico capturado para abrir portones eléctricos.

Descripción: Uso de MATLAB y ADALM-Pluto para procesar y transmitir señales en diferentes modulaciones de operación

Impacto: Posibilidad de programar códigos que permitan abrir los portones eléctricos replicando señales legítimas de un mando original.

Resultado: El ataque no permitió replicar la señal RF del mando inalámbrico

- **Resultado General**

	Resultado
Ataque 1	NO
Ataque 2	NO
Ataque 3	NO

De acuerdo con los hallazgos encontrados por los diferentes ataques realizados para el motor de la marca LiftMaster, no se logró identificar que el sistema de comunicación inalámbrica puede ser objeto de diversos problemas de seguridad.

6. RECOMENDACIÓN

Se establece como recomendación la utilización del mando original, el cual es compatible con sistemas de seguridad Security+ 2.0. Esta compatibilidad implica que utiliza

tecnología de código cambiante para garantizar que la señal transmitida sea única y segura en cada uso.

Además, se recomienda el uso de la tecnología MyQ, desarrollada por LiftMaster, que permite la comunicación bidireccional entre el portón del garaje y varios accesorios compatibles. A través de la aplicación móvil MyQ, los usuarios pueden recibir alertas y controlar el portón desde cualquier lugar, incluyendo funciones como abrir, cerrar y monitorear el estado de la puerta del garaje.

Ing. Fabián Cuzme MSc
DIRECTOR

Tandayamo Smith

Jacome Logacho Jorge

7.3. ANEXO C: Solicitud y carta de aprobación de los dueños o encargados de los portones eléctricos.

7.3.1. ANEXO C.1

Cayambe 30 de abril del 2024

Sr. Estudiante

Tandayamo Valencia Smith

De mis consideraciones:

De acuerdo con la solicitud del estudiante Tandayamo Valencia Smith Francisco quien está desarrollando su tesis sobre "Ethical Hacking para la identificación de Vulnerabilidades de Seguridad en Frecuencias Inalámbricas de Portones Eléctricos mediante el Uso de Dispositivos Analizadores de Espectro", bajo la tutela del Msc. Fabián Geovanny Cuzme Rodríguez, se otorga la autorización correspondiente. Valoramos su interés en llevar a cabo esta investigación en nuestras instalaciones y estamos comprometidos a brindarle el apoyo necesario para facilitar su trabajo.

Por favor, tenga en cuenta que es importante respetar las reglas y regulaciones del lugar durante el desarrollo de su investigación. Le pedimos que coordine cualquier acceso necesario y que se comprometa a mantener la privacidad y la seguridad del lugar.

Le deseamos mucho éxito en su proyecto y esperamos ver los resultados de su investigación.

ATENTAMENTE

Pedro Terán

CI: 1212451141-5

Cayambe 30 de abril del 2024

Señor

Pedro Terán

De mis consideraciones:

Me dirijo a usted con respeto y consideración para solicitarte autorización para llevar a cabo pruebas de campo en el sector de Cayambe en la calles El camino al sol y El pajonal.

Como estudiante de la Universidad Técnica del Norte, me encuentro en el proceso de obtener mi título de Ingeniero en Telecomunicaciones. El tema de mi proyecto de grado se centra en "ETHICAL HACKING PARA LA IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN FRECUENCIAS INALÁMBRICAS DE PORTONES ELÉCTRICOS MEDIANTE EL USO DE DISPOSITIVOS ANALIZADORES DE ESPECTRO". En este contexto, es necesario realizar pruebas de campo en los portones eléctricos del sector mencionado, con el único propósito de evaluar sus comportamientos inalámbricos.

Agradezco de antemano su atención a esta solicitud y quedo a disposición para proporcionar cualquier información adicional que pueda necesitar. Asimismo, me comprometo a cumplir con todas las normativas y regulaciones pertinentes durante la realización de estas pruebas.

Quedo a la espera de su respuesta y agradezco de antemano su colaboración en este proceso académico.

ATENTAMENTE

Sr. Tandayamo Smith

ESTUDIANTE UTN

CI:1753015609

Ing. Fabián Cuzme MSc

DIRECTOR

7.3.2. ANEXO C.2

Cayambe 11 de mayo del 2024

Sr. Estudiante

Tandayamo Valencia Smith

De mis consideraciones:

De acuerdo con la solicitud del estudiante Tandayamo Valencia Smith Francisco quien está desarrollando su tesis sobre "Ethical Hacking para la Identificación de Vulnerabilidades de Seguridad en Frecuencias Inalámbricas de Portones Eléctricos mediante el Uso de Dispositivos Analizadores de Espectro", bajo la tutela del Msc. Fabián Geovanny Cuzme Rodríguez, se otorga la autorización correspondiente. Valoramos su interés en llevar a cabo esta investigación en nuestras instalaciones y estamos comprometidos a brindarle el apoyo necesario para facilitar su trabajo.

Por favor, tenga en cuenta que es importante respetar las reglas y regulaciones del lugar durante el desarrollo de su investigación. Le pedimos que coordine cualquier acceso necesario y que se comprometa a mantener la privacidad y la seguridad del lugar.

Le deseamos mucho éxito en su proyecto y esperamos ver los resultados de su investigación.

ATENTAMENTE

Vivar Eduardo

CI:

Cayambe 11 de mayo del 2024

Señor

Eduardo Vivar

De mis consideraciones:

Me dirijo a usted con respeto y consideración para solicitarle autorización para llevar a cabo pruebas de campo en el sector de Cayambe en el conjunto Ciudad del Sol

Como estudiante de la Universidad Técnica del Norte, me encuentro en el proceso de obtener mi título de Ingeniero en Telecomunicaciones. El tema de mi proyecto de grado se centra en "ETHICAL HACKING PARA LA IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN FRECUENCIAS INALÁMBRICAS DE PORTONES ELÉCTRICOS MEDIANTE EL USO DE DISPOSITIVOS ANALIZADORES DE ESPECTRO". En este contexto, es necesario realizar pruebas de campo en los portones eléctricos del sector mencionado, con el único propósito de evaluar sus comportamientos inalámbricos.

Agradezco de antemano su atención a esta solicitud y quedo a disposición para proporcionar cualquier información adicional que pueda necesitar. Asimismo, me comprometo a cumplir con todas las normativas y regulaciones pertinentes durante la realización de estas pruebas.

Quedo a la espera de su respuesta y agradezco de antemano su colaboración en este proceso académico.

ATENTAMENTE

Sr. Tandayamo Smith

ESTUDIANTE UTN

CI:1753015609

Msc. Fabian Geovanny Cuema Rodriguez

Directo de Tesis

7.3.2. ANEXO C.3

Cayambe 19 de abril del 2024

Sr. Estudiante

Tandayamo Valencia Smith

De mis consideraciones:

De acuerdo con la solicitud del estudiante Tandayamo Valencia Smith Francisco quien está desarrollando su tesis sobre "Ethical Hacking para la Identificación de Vulnerabilidades de Seguridad en Frecuencias Inalámbricas de Portones Eléctricos mediante el Uso de Dispositivos Analizadores de Espectro", bajo la tutela del Msc. Fabián Geovanny Cuzme Rodríguez, se otorga la autorización correspondiente. Valoramos su interés en llevar a cabo esta investigación en nuestras instalaciones y estamos comprometidos a brindarle el apoyo necesario para facilitar su trabajo.

Por favor, tenga en cuenta que es importante respetar las reglas y regulaciones del lugar durante el desarrollo de su investigación. Le pedimos que coordine cualquier acceso necesario y que se comprometa a mantener la privacidad y la seguridad del lugar.

Le deseamos mucho éxito en su proyecto y esperamos ver los resultados de su investigación.

ATENTAMENTE

Jacome Lagacho Jorge

CI:1714889753

JACOME
INDUSTRIA MECANICA
R.U.C. 1714889753001

Cayambe 19 de abril del 2024

Señor

Jorge Jacome Logacho

De mis consideraciones:

Me dirijo a usted con respeto y consideración para solicitarle autorización para llevar a cabo pruebas de campo en el sector de Cayambe en el conjunto Ciudad del Sol

Como estudiante de la Universidad Técnica del Norte, me encuentro en el proceso de obtener mi título de Ingeniero en Telecomunicaciones. El tema de mi proyecto de grado se centra en "ETHICAL HACKING PARA LA IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN FRECUENCIAS INALÁMBRICAS DE PORTONES ELÉCTRICOS MEDIANTE EL USO DE DISPOSITIVOS ANALIZADORES DE ESPECTRO". En este contexto, es necesario realizar pruebas de campo en los portones eléctricos del sector mencionado, con el único propósito de evaluar sus comportamientos inalámbricos.

Agradezco de antemano su atención a esta solicitud y quedo a disposición para proporcionar cualquier información adicional que pueda necesitar. Asimismo, me comprometo a cumplir con todas las normativas y regulaciones pertinentes durante la realización de estas pruebas.

Quedo a la espera de su respuesta y agradezco de antemano su colaboración en este proceso académico.

ATENTAMENTE

Sr. Tandayamo Smith

ESTUDIANTE UTN

CI:1753015609

Mgs. Adrián Geovanny Cuzme Rodríguez

Directo de Tesis