

MAESTRÍA EN CIBERSEGURIDAD

DOCUMENTO FINAL DE PROYECTO DE INVESTIGACIÓN APLICADA 2

CREACIÓN DE UN SISTEMA DE DETECCIÓN DE PUNTOS DE ACCESO INALÁMBRICOS NO AUTORIZADOS UTILIZANDO TECNOLOGÍAS DE CÓDIGO ABIERTO Y UNA RASPBERRY PI.

RETANA ACOSTA JUAN DIEGO

VARELA MORALES BERNAL

ABRIL DEL 2018

Tabla de contenidos

Resumen ejecutivo 1
Palabras claves 2
Capítulo 1. Introducción 3
1.1 Generalidades 3
1.2 Antecedentes del Problema 3
1.3 Definición y Descripción del Problema 4
1.4 Justificación 4
1.5 Viabilidad 5
1.5.1 Punto de Vista Técnico 5
1.5.2 Punto de Vista Operativo 5
1.5.3 Punto de Vista Económico 6
1.6 Objetivos 6
1.6.1 Objetivo General 6
1.6.2 Objetivos Específicos 6
1.7 Alcances y Limitaciones 7
1.7.1 Alcance 7
1.7.2 Limitaciones 7
Capítulo 2. Marco teórico 9
2.1 Punto de acceso inalámbrico no autorizado 9
2.2 Punto de acceso inalámbrico no autorizado y seguridad de la información 11
2.3 Métodos para la detección de puntos de acceso inalámbricos. 13
2.3.1 Detección mediante técnicas estadísticas 13
2.3.2 Detección utilizando tiempos de respuesta 15
2.3.3 Análisis de clientes y señal 16
2.3.4 Análisis de señal mediante sensores 17
2.4 Sistemas de monitoreo utilizando sensores inalámbricos 18
2.5 Soluciones existentes. 25
2.5.1 Cisco Wireless Intrusion Prevention System / Cisco wIPS 26
2.5.2 HP Mobility Security IDS/IPS System series 28
2.5.3 AirMagnet Enterprise 30
Capítulo 3. Estado de la cuestión 34
3.1 Planificación de la revisión 34
3.1.1 Formulación de la pregunta 34
3.1.2 Foco de la pregunta 34
3.1.3 Amplitud y calidad de la pregunta 34

3.1.3.1 Problema 34
3.1.3.2 Pregunta de investigación 35
3.1.3.3 Palabras clave y sinónimos 35
3.1.3.4 Intervención 36
3.1.3.5 Control 36
3.1.3.6 Resultado 36
3.1.3.7 Diseño experimental 36
3.2 Selección de fuentes 37
3.2.1 Definición del criterio de selección de fuentes 37
3.2.2 Lenguaje de estudio 37
3.2.3 Identificación de fuentes 37
3.2.3.1 Método de selección de fuentes 37
3.2.3.2 Lista de fuentes 38
3.2.3.3 Cadenas de búsqueda 38
3.2.3.4 Selección de fuentes después de la evaluación 38
3.2.3.5 Comprobación de las fuentes 38
3.3 Selección de los estudios 39
3.3.1 Definición del criterio de inclusión y exclusión de estudios 39
3.3.2 Definición de tipos de estudio 39
3.3.3 Procedimiento para la selección de los estudios 39
3.4 Ejecución de la revisión 39
3.4.1 Ejecución de la selección en la fuente DBLP 40
3.4.1.1 Selección de estudios iniciales 40
3.4.1.2 Evaluación de la calidad de los estudios 41
3.4.1.3 Extracción de información 41
3.4.1.3.1 Definición del criterio de inclusión y exclusión de información 41
3.4.1.3.2 Formulario para la extracción de información 41
3.4.1.3.3 Extracción de resultados objetivos y subjetivos 42
3.5 Análisis de resultados 49
3.5.1 Fuentes analizadas 49
Capítulo 4. Marco metodológico 51
4.1 Tipo de Investigación 51
4.2 Enfoque 51
4.3 Diseño 52
4.4 Población y muestreo 52
4.5 Técnicas y herramientas de recolección de datos 53
4.5.1 Técnicas de recolección de datos 53

4.5.2 Herramientas de recolección de datos. 54
4.5.2.1 Tablas resumen 54
4.5.2.2 Lista de cotejo 54
4.5.2.3 Rúbricas 55
4.5.2.3.1 Rúbrica de evaluación para lenguajes de programación. 55
4.5.2.3.2 Rúbrica de evaluación para hardware de tarjetas inalámbricas. 56
4.5.2.3.3 Rúbrica de evaluación para repositorios de datos 57
4.5.2.3.4 Rúbrica de evaluación para herramientas de escaneo de señales inalámbricas 58
4.5.2.4 Diagramas 59
4.5.2.5 Casos de uso 59
4.6 Estrategia de desarrollo de la propuesta 59
Capítulo 5. Análisis de resultados 60
5.1 Elementos de hardware y software que conforman un sistema de monitoreo de puntos de acceso inalámbricos no autorizados 60
5.2 Tecnologías de código abierto existentes que pueden ser utilizadas en el sistema de monitoreo de puntos de acceso inalámbricos no autorizados. 64
5.2.1 Lenguaje de programación 64
5.2.2 Hardware tarjetas inalámbricas 67
5.2.3 Repositorio de datos 69
5.2.4 Herramienta de escaneo de señales inalámbricas 72
5.3 Requerimientos funcionales y no funcionales del sistema de monitoreo de puntos de acceso no autorizados 74
5.4 Casos de uso de los requerimientos funcionales y no funcionales 78
5.4.1 Caso de uso: WS-RPI- Configurar dispositivo. 78
5.4.2 Caso de uso: WS-RPI- Iniciar configuración. 80
5.4.3 Caso de uso: WS-RPI- Configuración de fábrica 81
5.4.4 Caso de uso: WS-RPI- Tomar inventario 82
5.4.5 Caso de uso: WS-RPI - Obtener estatus 84
5.4.6 Caso de uso: Módulo de comunicación - Envió de notificaciones. 85
5.4.7 Caso de uso: DAC-S - Agregar WS-RPI. 86
5.4.8 Caso de uso: DAC-S - Obtener información de inventario. 88
5.4.9 Caso de uso: DAC-S - Obtener estatus del WS-RPI. 91
5.4.10 Casos de uso: DAC-S - Clasificar señales de inventario. 93
5.4.11 Caso de uso: DAC-S - Procesar estatus de señales. 96
5.4.12 Caso de uso: DAC-S - Atender alertas pendientes de resolver. 98
5.4.13 Caso de uso: DAC-S - Graficar dispositivos en plano. 101

5.5 Diseñar la arquitectura del sistema. 102
5.5.1 Diagramas de base de datos 102
5.5.2 Arquitectura del WS-RPI 104
5.5.3 Diagrama eléctrico del botón resetear y luces indicadoras 105
5.5.4 Arquitectura del DAC-S 107
5.5.5 Diagrama general de la solución 108
5.6 Desarrollar el software e interfaz de gestión del dispositivo. 109
5.6.1 WS-RPI 109
5.6.2 DAC-S 115
5.7 Plan de pruebas del funcionamiento de la solución en un ambiente controlado. 122
5.7.1 Escenarios de observación y resultados 123
5.7.1.1 Escenario 1: Configurar dispositivo 123
5.7.1.2 Escenario 2: Iniciar configuración 123
5.7.1.3 Escenario 3: Reiniciar a fábrica 124
5.7.1.4 Escenario 4: Tomar inventario 125
5.7.1.5 Escenario 5: Obtener estatus 125
5.7.1.6 Escenario 6: Envío de notificaciones 126
5.7.1.7 Escenario 7: Agregar sensor inalámbrico 127
5.7.1.8 Escenario 8: Obtener información del inventario. 127
5.7.1.9 Escenario 9: Obtener estatus del sensor. 128
5.7.1.10 Escenario 10: Clasificar las señales del inventario. 129
5.7.1.11 Escenario 11: Procesar estatus de las señales. 130
5.7.1.12 Escenario 12: Atender alertas pendientes de resolver 131
5.7.1.13 Escenario 13: Graficar dispositivo en el plano. 132
5.8 Discusión de resultados 132
Capítulo 6. Conclusiones y recomendaciones 135
Capítulo 7. Trabajos futuros 138
Glosario de términos 139
Referencias bibliográficas 143
Capítulo 8. Anexos 146

Índice de tablas

Tabla 1: Escalas de medición para la calidad de la señal. 20
Tabla 2: Tabla de clasificación de puntos de acceso detectados con su respectiva descripción. 23
Tabla 3: Detalla de los elementos que conforman la solución Cisco wIPS con sus respectivas funciones. 26
Tabla 4: Detalle de los componentes que conforman la solución AirMagnet. 30
Tabla 5: Listado de palabras claves y respectivos sinónimos que serán utilizados para establecer las cadenas de búsqueda. 35
Tabla 6: Fuentes obtenidas como resultado de aplicar los criterios de búsqueda en el repositorio de datos DBLP. 40
Tabla 7: Cuadro resumen utilizado para extraer la información relevante de cada fuente obtenida. 41
Tabla 8: Cuadro resumen de la fuente 1 obtenido de la base de datos DBLP. 42
Tabla 9: Cuadro resumen de la fuente 2 obtenido de la base de datos DBLP. 43
Tabla 10: Cuadro resumen de la fuente 3 obtenido de la base de datos DBLP. 45
Tabla 11: Cuadro resumen de la fuente 4 obtenido de la base de datos DBLP. 47
Tabla 12: Cuadro resumen de la fuente 5 obtenido de la base de datos DBLP. 48
Tabla 13: Rubrica de evaluación para los lenguajes de programación. 55
Tabla 14: Rubrica de evaluación para seleccionar modelo tarjeta inalámbrica. 56
Tabla 15: Rubro de evaluación para seleccionar motor de base de datos. 57
Tabla 16: Rubro de evaluación para seleccionar herramienta de análisis de señal inalámbricas. 58
Tabla 17: Lista de cotejo que permite identificar los elementos en común que comparten las diferentes soluciones de monitoreo que existen en el mercado 60
Tabla 18: Cuadro de elementos que conforman un sistema de monitoreo de puntos de acceso inalámbricos no autorizados. 61
Tabla 19: Análisis de los criterios de evaluación para el lenguaje de programación Python. 65
Tabla 20: Análisis de los criterios de evaluación para el lenguaje de programación Java EE. 65
Tabla 21: Análisis de los criterios de evaluación para el lenguaje de programación Node JS. 66
Tabla 22: Rúbrica de evaluación para el modelo de tarjeta inalámbrica Panda PAU05. 67

Tabla 23: Rúbrica de evaluación para el modelo de tarjeta inalámbrica TP-LINK WN722N. 68
Tabla 24: Rúbrica de evaluación para el modelo de tarjeta inalámbrica Alfa AWUS036ACH..... 69
Tabla 25: Rúbrica de evaluación para el repositorio de datos MySql Database..... 70
Tabla 26: Rúbrica de evaluación para el repositorio de datos Mongo DB. 70
Tabla 27: Rúbrica de evaluación para el repositorio de datos Postgresql. 71
Tabla 28: Rúbrica de evaluación para la herramienta de escaneo de señales inalámbricas Linux Wireless Tool. 72
Tabla 29: Rúbrica de evaluación para la herramienta de escaneo de señales inalámbricas Aircrack-ng. 72
Tabla 30: Rúbrica de evaluación para la herramienta de escaneo de señales inalámbricas iwlist. 73
Tabla 31: Detalle de los requerimientos funcionales con los que debe cumplir el dispositivo WS-RPI. 75
Tabla 32: Detalle de los requerimientos funcionales con los que debe cumplir el módulo de comunicación..... 76
Tabla 33: Detalle de los requerimientos funcionales con los que debe cumplir el DAC-S. 76
Tabla 34: Flujo principal de eventos para el caso de uso. 79
Tabla 35: Flujo principal de eventos para el caso de uso. 80
Tabla 36: Flujo principal de eventos para el caso de uso. 81
Tabla 37: Flujo principal de eventos para el caso de uso. 82
Tabla 38: Flujo principal de eventos para el caso de uso. 84
Tabla 39: Flujo principal de eventos para el caso de uso. 86
Tabla 40: Flujo principal de eventos para el caso de uso agregar WS-RPI. 87
Tabla 41: Flujo principal de eventos para el caso de uso obtener información de inventario. 89
Tabla 42: Flujo principal de eventos para el caso de uso obtener estatus del WS-RPI. 92
Tabla 43: Flujo principal de eventos para el caso de uso clasificar señales de inventario. 93
Tabla 44: Flujo principal de eventos para el caso de uso procesar estatus de señales. 96

Tabla 45: Flujo principal de eventos para el caso de uso atender alertas pendientes de resolver. 98
Tabla 46: Flujo principal de eventos para el caso de uso graficar dispositivos en plano. 101
Tabla 47: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de configurar el sensor inalámbrico. 123
Tabla 48: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de iniciar configuración del sensor inalámbrico. 123
Tabla 49: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de reiniciar a fábrica el sensor inalámbrico. 124
Tabla 50: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de tomar inventario. 125
Tabla 51: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de obtener estatus del sensor inalámbrico. 125
Tabla 52: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de envío de correos mediante el módulo de notificaciones. 126
Tabla 53. Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de agregar sensor inalámbrico en el DAC-S. 127
Tabla 54: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de obtener inventario del sensor inalámbrico desde el DAC-S. 127
Tabla 55: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de obtener estatus del sensor inalámbrico desde el DAC-S. 128
Tabla 56: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de clasificar las señales del inventario desde el DAC-S. 129
Tabla 57: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de procesar señales inalámbricas obtenidas de los sensores. 130
Tabla 58: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad atender alertas generadas por el DAC-S en el procesamiento de señales inalámbricas. 131
Tabla 59: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de graficar dispositivos en el plano. 132

Índice de figuras

Figura 1: Arquitectura de red donde se ha instalado un punto de acceso inalámbrico no autorizado: 9
Figura 2: Representación gráfica de modos de operación de puntos de acceso con funciones de servicio de datos y monitoreo integrado o separado. 19
Figura 3: Caso práctico de como calcular el RSSI en base a los niveles de señal y ruido. 20
Figura 4: Escala de medición de la calidad de la señal según rango donde se ubique el RSSI. 21
Figura 5: Diagrama de flujo de arquitectura de comunicación donde se representa la aplicación de estandarización de datos y protocolo de comunicación. 22
Figura 6: Flujo de proceso para clasificar puntos de acceso detectados en la categoría que corresponde. 24
Figura 7: Diagrama de arquitectura de la solución de monitoreo Cisco wIPS. 27
Figura 8: Diagrama de funcionamiento de la solución AirMagnet. 31
Figura 9*:* Parámetros de búsqueda de la consulta en la base de datos de DBLP. 40
Figura 10: Diagrama de base de datos donde se almacena la información recolectada por las herramientas de escaneo dentro del WS-RPI. 103
Figura 11:Diagrama de la estructura de base de datos utilizada por el DAC-S para almacenar la información recibida por los WS-RPI. 103
Figura 12: Diagrama de los principales elementos que conforman el WS-RPI. 105
Figura 13: Diagrama de los componentes eléctricos con los que se implementó las luces indicadoras del sensor y el botón resetear. 106
Figura 14: Diagrama de arquitectura de la solución del DAC-S. 108
Figura 15: Diagrama de red de una posible implementación de la solución. 109
Figura 16: Detalle de la pantalla de inicio de sesión de la interfaz de gestión del sensor inalámbrico. 111
Figura 17: Pantalla con el detalle del estado de la configuración del sensor inalámbrico. 111
Figura 18: Pantalla donde se ingresan los parámetros de configuración del sensor inalámbrico. 112
Figura 19: Detalle de los datos recolectados por la herramienta de análisis de señales inalámbricas Airmong-ng. 112
Figura 20: Detalle de los métodos que se encargan de configurar la GPIO de la Raspberry PI, así como encender-apagar leds y leer la señal del botón. 113

Figura 21: Detalle del código fuente que se encarga de iniciar el Web Socket (módulo de comunicación) en la Raspberry PI. 113
Figura 22: Detalle del código fuente del método que se encarga de procesar los comandos que recibe la Raspberry desde el DACS en formato JSON. 114
Figura 23: Detalle del código fuente del método que se encarga de procesar los datos generados por la herramienta de análisis de señales y la transforma a una estructura estandarizada en formato JSON. 114
Figura 24: Detalle del código fuente del método que se ejecuta con una tarea programada del sistema operativo de la Raspberry, el cual se encarga de procesar los datos estandarizados generados por la herramienta de análisis de señales y la carga a la base de datos del dispositivo. 115
Figura 25: Pantalla del DAC-S donde se ingresa la configuración del sensor inalámbrico junto con mensaje de confirmación de configuración realizada con éxito. 116
Figura 26: Pantalla del DAC-S donde se muestra el listado de sensores configurados. 117
Figura 27: Pantalla del DAC-S donde se muestra la información de inventario obtenida por un sensor. 117
Figura 28: Pantalla del DAC-S donde se ingresa la clasificación de cada uno de los puntos de accesos detectados en el proceso de inventario del sensor inalámbrico. . 118
Figura 29: Pantalla del DAC-S donde se muestran las alertas generadas como el resultado de analizar del estatus de las señales enviadas por el sensor inalámbrico. 118
Figura 30: Pantalla del DAC-S donde se puede gestionar las alertas generadas como resultado del procesamiento de las señales inalámbricas detectadas por el sensor inalámbrico. 119
Figura 31: Código fuente de función desarrollada a nivel de base de datos, la cual permite determinar si un cliente que pertenece a un punto de acceso miembro se está conectado a un punto de acceso que no pertenece a esa categoría. 119
Figura 32: Código fuente de método desarrollado en Java con el que se puede verificar el estatus de los sensores, mediante este método se puede valorar si se genera una alerta por falta de conectividad o porque el sensor se encuentra desconfigurado..... 120
Figura 33: Detalle de código fuente de función de base de datos desarrollada para realizar la clasificación de los puntos de acceso una vez se haya cargado la información del inventario. 120

Figura 34: Detalle de código fuente de función de base de datos desarrollada para realizar la clasificación de los puntos de acceso una vez se haya cargado la información del inventario, segunda parte..... 121
Figura 35: Detalle del código fuente de función desarrollada a nivel de base de datos, la cual se encarga de analizar los datos del estatus del sensor y el inventario configurado y en caso de que detecte alguna anomalía genera las alertas y notificaciones correspondientes al administrador de la aplicación..... 121
Figura 36: Diagrama de la configuración de red que se va a utilizar para ejecutar los guiones de observación de las pruebas. 122

Resumen ejecutivo

Desde la creación de los primeros computadores y con el paso del tiempo el uso de las tecnologías de información se ha ido masificando hasta llegar al punto que actualmente se han convertido en una necesidad para poder realizar las tareas diarias de las personas. Actualmente se dispone con un rango de dispositivos muy amplio, los cuales se caracterizan por ser cada día más pequeños y potentes, tal es el caso de los computadores portátiles, tabletas, teléfonos y aparatos del internet de las cosas, además, se pueden resaltar otras características como la portabilidad y la autonomía energética.

Una de las problemáticas que se presenta con las características de los dispositivos mencionadas anteriormente, es que pueden ser utilizados para funciones que resultan un riesgo para la seguridad de la información de las empresas, al mismo tiempo que pueden pasar desapercibidos gracias a su tamaño y capacidad de procesamiento, tal es el caso de los puntos de acceso inalámbricos no autorizados que se pueden habilitar en las redes corporativas o sus alrededores.

Según los expertos los puntos de acceso inalámbricos no autorizados son una amenaza potencial para la seguridad de la información de las empresas, debido a que sirve como puerta de entrada a dispositivos no autorizados que pueden realizar tareas como análisis de tráfico de datos, robo de información, denegación de servicio, inyección de archivos maliciosos, virus, malware e inclusive infecciones sumamente peligrosas como Ransomware dentro de la red.

Otro problema que se presenta con este tipo de vulnerabilidad es que los administradores de red le restan mucha importancia, y quienes lo hacen se ven limitados debido a que las tecnologías capaces de prevenirlo requieren presupuestos muy elevados.

Con el presente trabajo de investigación se plantea desarrollar un sistema de detección de intrusos inalámbricos, conocidos como WIDS (Wireless Intrusion Detection Systems), el cual permita a los administradores de red detectar de una forma automatizada cuando un punto de acceso inalámbrico no autorizado se conectó en las redes de sus empresas. La idea es desarrollar el WIDS utilizando tecnologías de código abierto y un dispositivo Rasperry PI, lo que permitiría que sea una solución de bajo costo accesible para pequeñas y medianas empresas.

Palabras claves

Detección intrusos inalámbricos, Punto de acceso no autorizado, seguridad inalámbrica, sensor inalámbrico, sistema de monitoreo, Raspberry PI.

Capítulo 1. Introducción

1.1 Generalidades

El proyecto se presenta como una iniciativa personal de los miembros que conforman el grupo de investigación, especialmente porque es un tema que se puede explorar ampliamente aprovechando las características de escalabilidad que posee el hardware de un Raspberry PI junto con la capacidad de adaptarse a tecnologías de código abierto.

Basándose en la experiencia y conocimiento que posee el grupo de investigación en tecnologías de código abierto, seguridad de la información y desarrollo de software se tiene una idea general de cómo desarrollar el sistema de monitoreo. Sin embargo, el proceso de investigación es clave para poder generar la documentación y conocimiento de forma estructurada que permita garantizar el desarrollo y correcto funcionamiento del mismo.

1.2 Antecedentes del Problema

El problema se presenta debido a la facilidad con la que se puede establecer un punto de acceso no autorizado utilizando un dispositivo portable en los diferentes tipos de redes(empresariales, corporativas, gubernamentales, educativas, entre otras), especialmente en aquellas organizaciones donde la información que se maneja es muy sensible y se desea tener un nivel de acceso restrictivo que evite que sus empleados ingresen o extraigan datos del conjunto de activos de información que poseen o resguardan.

Con las tecnologías actuales un punto de acceso inalámbrico no autorizado se puede crear de una forma muy fácil, como es el caso de compartir la red con computador portátil, o se puede realizar algo más complejo como conectar un enrutador inalámbrico en un puerto de red cableado de una estación de trabajo.

Además, la problemática se agrava por el hecho de que el punto de acceso puede ser temporal, por lo que se requiere monitorear permanentemente si se desea evitar este tipo de amenazas en las redes empresariales.

1.3 Definición y Descripción del Problema

Se puede definir el problema como la necesidad de los administradores de redes empresariales de poseer un sistema de monitoreo automatizado que les alerte cuando un punto de acceso no autorizado se ha activado en las instalaciones de sus compañías. Es importante mencionar que una de las tareas fundamentales para poder realizar una adecuada detección es elaborar el inventario de puntos de acceso autorizados o vecinos, tarea que puede resultar bastante tediosa y que debe ser considera como una de las funcionalidades del sistema al momento de desarrollarlo.

Otra característica del problema es que actualmente existen aplicaciones y dispositivos capaces de realizar esta tarea, sin embargo, no son accesibles para cualquier usuario/empresa debido a sus altos costos e incompatibilidad entre fabricantes, lo que los convierte en soluciones muy restrictivas y cerradas. Por mencionar un ejemplo, el implementar una solución de HP Mobility Security o Cisco wIPS en una organización con infraestructura mediana o pequeña puede tener un costo inicial que ronda aproximadamente entre los $10.000 y $15.000.

1.4 Justificación

La principal razón por lo que se busca desarrollar la solución es que se desea crear una medida alternativa con la que se pueda afrontar el problema de monitoreo de puntos de acceso inalámbricos no autorizados, sin la necesidad de utilizar las soluciones propietarias que requieren presupuestos muy elevados.

Adicionalmente se desea crear una solución basada en tecnologías de código abierto que permita ser escalable y se le puedan integrar nuevas funcionalidades según las necesidades del usuario.

Por último, se desea explotar los conocimientos y experiencias del grupo de investigación en áreas como desarrollo de software, tecnologías de código abierto y ciberseguridad, para crear una solución integral capaz de resolver el problema de investigación a un bajo costo y con una interfaz de gestión amigable para el usuario.

1.5 Viabilidad

1.5.1 Punto de Vista Técnico

Desde el punto de vista técnico, el proyecto es viable. Especialmente por la escalabilidad y nivel de procesamiento que presenta el hardware de Raspberry PI, en el cual se pueden ejecutar distribuciones de GNU/Linux como Kali, la cual posee gran cantidad de herramientas que permiten realizar análisis y captura de datos de redes inalámbricas. Otro aspecto importante es la amplia experiencia que posee el grupo de investigación en temas de seguridad de la información, desarrollo del software y tecnologías de código abierto.

1.5.2 Punto de Vista Operativo

El proyecto es viable desde el punto de vista operativo debido a que el hardware de la Raspberry PI es capaz de soportar el procesamiento necesario por las herramientas y lenguajes de programación requeridos para desarrollar la solución.

En momentos posteriores la solución se podría utilizar a gran escala, sin requerir mayor nivel de complejidad para poder integrarla con otros sistemas o arquitecturas existentes de las compañías.

1.5.3 Punto de Vista Económico

Desde el punto de vista económico el proyecto es viable, especialmente porque los costos que representan los elementos de hardware necesarios para desarrollar la investigación son muy bajos, aproximadamente $50 dólares por cada dispositivo Raspberry PI que se adquiera. Como se pretende desarrollar el sistema de monitoreo utilizando tecnologías de código abierto no se requiere ningún tipo de inversión adicional por rubros de licencias o derechos de uso de software. El monto total de la inversión requerida será cubierto por los integrantes que conforman el grupo de investigación.

1.6 Objetivos

1.6.1 Objetivo General

Crear de un sistema de detección de puntos de acceso inalámbricos no autorizados utilizando tecnologías de código abierto y una Raspberry PI.

1.6.2 Objetivos Específicos

- Identificar los elementos de hardware y software que conforman un sistema de monitoreo de puntos de acceso inalámbricos no autorizados.
- Analizar las tecnologías de código abierto existentes que pueden ser utilizadas en el sistema de monitoreo de puntos de acceso inalámbricos no autorizados.
- Definir los requerimientos funcionales y no funcionales que conforman un sistema de monitoreo de puntos de acceso no autorizados.
- Especificar los casos de uso de los requerimientos funcionales y no funcionales que conforman un sistema de monitoreo de puntos de acceso no autorizados.

- Diseñar la arquitectura del sistema de monitoreo de puntos de acceso no autorizados.
- Desarrollar el software e interfaz de gestión del sistema de monitoreo de puntos de acceso no autorizados.
- Ejecutar plan de pruebas del funcionamiento de la solución en un ambiente controlado.

1.7 Alcances y Limitaciones

1.7.1 Alcance

El alcance de la investigación se delimita a la creación del sistema de detección de puntos de acceso inalámbricos no autorizados capaz de funcionar en un ambiente de pruebas controlado (utilizando una cantidad de dispositivos de telecomunicaciones limitados). Estará compuesto por una primera fase de documentación, en la cual se recolectará información acerca definición de conceptos, soluciones existentes, elaboración de casos de uso, tecnologías y métodos que se pueden utilizar en esta clase de sistemas. Una segunda fase práctica está compuesta por el desarrollo de software, integración de herramientas, plan de pruebas y análisis de resultados. Adicionalmente se entregará una guía paso a paso de cómo instalar la solución desde cero, para que futuras personas que quieran explotar la investigación tengan los insumos necesarios para realizar la instalación y configuraciones necesarias para poner en funcionamiento el sistema de monitoreo.

1.7.2 Limitaciones

El proyecto de investigación se limita a crear un sistema de detección de puntos de acceso inalámbricos no autorizados con el cual se busca ejecutar los escenarios de pruebas que verifiquen su correcto funcionamiento en un ambiente

controlado; se considera que puede requerir mejoras estéticas y documentación adicional para que pueda ser comercializado a gran escala.

Debido a limitación de tiempo y recursos, el sistema desarrollado en la investigación solo realizará funciones de detección y monitoreo, y no será capaz de tomar algún tipo de acción correctiva en caso de que se detecte un punto de acceso inalámbrico no autorizado, como sí sucede con la mayoría de las soluciones propietarias disponibles en el mercado.

En el proceso que conforma el ciclo de vida de desarrollo de software solo se documentarán los casos de uso con sus respectivos flujos, entradas y salidas. El plan de pruebas se desarrollará en un ambiente controlado con una cantidad de dispositivos limitados, no se garantiza el correcto funcionamiento de la solución en todas las condiciones de conectividad a las que se puede enfrentar si se empieza a utilizar a gran escala. No se realizarán capacitaciones acerca del funcionamiento y configuración, no se brindará soporte en su implementación una vez concluida la investigación.

Capítulo 2. Marco teórico

2.1 Punto de acceso inalámbrico no autorizado

Según la definición de (Ganesh B., Vidya S., & Siddharth A., 2012) un punto de acceso inalámbrico no autorizado se puede definir como “punto de acceso inalámbrico que se ha instalado sin el consentimiento explícito del administrador local de la red”. Por otra parte, también le dan una segunda definición, la cual expresan de la siguiente forma: “Punto de acceso Wifi el cual es configurado por un atacante con el propósito de analizar el tráfico de red de las redes inalámbricas”.

En la figura 1 se muestra un típico ejemplo de la arquitectura de red donde se instala un punto de acceso no autorizado:

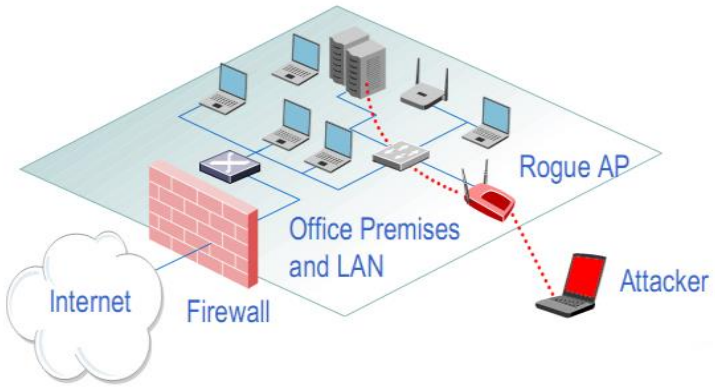


Figura 1: Arquitectura de red donde se ha instalado un punto de acceso inalámbrico no autorizado: Fuente: (Ganesh B., Vidya S., & Siddharth A., 2012).

Además, (Ganesh B., Vidya S., & Siddharth A., 2012) caracterizan este tipo de punto de acceso porque no cumple con las políticas de seguridad que poseen las redes donde se ha instalado, y comúnmente se puede clasificar en los siguientes tipos:

- **Punto de acceso de empleado:** El punto de acceso inalámbrico no autorizado es instalado dentro de la red por los empleados de la organización para obtener beneficios propios. La principal amenaza que representa se debe a que

usuarios o dispositivos no autorizados pueden acceder a la red de la organización. Es muy común que se presente en organizaciones donde no se tienen políticas de seguridad inalámbricas definidas y no se brinda capacitación a los colaboradores acerca de este tema.

- **Punto de acceso atacante externo:** En este caso el punto de acceso no se instala directamente en la red de la organización, consiste en que un usuario malicioso aprovecha las capacidades de transmisión y potencia de antenas e instala el punto de acceso fuera de la organización duplicando el SSID de los puntos de acceso legítimos, de esta forma trata de seducir a los empleados de la organización a que se conecten; de lograrlo podrá realizar el análisis de todo el tráfico de red que ellos trasmitan. Generalmente este ataque es conocido como ataque de hombre en el medio.
- **Punto de acceso atacante interno:** Este tipo de punto de acceso inalámbrico no autorizado se configura dentro de las instalaciones de la organización, y tiene acceso directo a la red de la misma, por lo cual el usuario atacante puede utilizarlo como una puerta de ingreso trasera para acceder cuando guste. Este tipo de amenaza tiene la restricción de que el usuario malicioso debe superar los controles de acceso físico a la organización, pero una vez logrado, se convierte en una brecha de seguridad sumamente peligrosa. Los autores hacen mención que generalmente este tipo de punto de acceso apaga la difusión del SSID para pasar desapercibido.
- **Punto de acceso inalámbrico vecino:** Según los autores este tipo de acceso inalámbrico son considerados por algunos administradores de red como no autorizados, consiste básicamente en las señales que tienen al alcance dentro de la organización y que son el resultado de puntos de acceso que instalan

organizaciones vecinas. Ante esta situación el administrador de red no puede realizar ninguna acción para deshabilitar estos puntos de acceso, pero una buena práctica para evitar amenazas asociadas a esta situación es educar a los empleados sobre los riesgos de seguridad de información que representa.

2.2 Punto de acceso inalámbrico no autorizado y seguridad de la información

Se ha definido que es un punto de acceso inalámbrico no autorizado, cuáles son sus características y cómo funcionan. No obstante, ahora se procede a describir cuáles son los problemas que representan para la seguridad de la información y el porqué es un tema que se debe manejar con mucha seriedad. Para el fabricante de equipos de seguridad y telecomunicaciones (Juniper Networks, 2016), las amenazas a la seguridad de la información que se pueden presentar como resultado de un punto de acceso inalámbrico no autorizado son:

- **Ataques de hombre en el medio:** Técnica en la cual un usuario mal intencionado intercepta la comunicación entre dos puntos o sistemas, como es el caso de cliente servidor en el protocolo HTTP, por decir un ejemplo. Para poder llevar acabo el ataque se debe separar la comunicación en dos partes, una entre el primer punto y el atacante y luego entre el atacante y el segundo punto. Si bien es cierto este tipo de ataque es más efectivo en protocolo donde los datos enviados no están cifrados, recientemente ataques elaborados han demostrado que protocolos seguros como HTTPS también pueden ser vulnerados. Los principios de la seguridad de información que se ven comprometidos con este tipo de ataque son la integridad y confidencialidad (Open Web Application Security Project(OWASP), 2015).
- **Ataques denegación de servicio:** Técnica con la cual uno o varios usuarios mal intencionados tratan o evitan que usuarios legítimos puedan ingresar a un

recurso específico de la red. Este tipo de ataques se pueden clasificar en dos tipos: 1- El atacante envía información de paquetes malformados a la víctima para que los protocolos y programas que esté utilizando se confundan y fallen. 2- Se basa en enviar un flujo de datos que produzca un sobre procesamiento en recursos como ancho de banda, enrutadores, conmutadores, servidores, entre otros; de tal forma que no puedan responder a peticiones de recursos que realizan usuarios legítimos. Este tipo de ataque se ve asociado a los puntos de acceso inalámbrico no autorizados debido a que sirve como puerta de entrada a dispositivos con los que se puede generar los flujos de paquetes mal intencionados. El principio de seguridad de la información que se ve afectado es la disponibilidad (Taghavi Zargar, Joshi, & Tipper, 2013).

- **Robo o pérdida de información:** Debido a que el punto de acceso inalámbrico no autorizado funciona como puerta de acceso trasera para usuarios o dispositivos no legítimos, los mismos pueden acceder a recursos internos de la organización que poseen información relevante, como servidores de datos compartidos, sistemas, servicios, correo electrónico, entre otros. Ante esta amenaza los principios de la seguridad de la información que se ven comprometidos son la integridad y confidencialidad (Dhiman, 2014).
- **Inyección de software malicioso:** Como el punto de acceso inalámbrico no autorizado no cumple con las políticas de seguridad de la organización, puede funcionar como puerta de entrada a componentes de software dañinos como es el caso del malware; el cual se define como cualquier software malicioso creado intencionalmente para que cause daños en computadores o recursos informáticos y que generalmente se instala sin el consentimiento y conocimiento del dueño.

Los gusanos son el tipo de malware que mejor explota la vulnerabilidad de los puntos de acceso inalámbricos no autorizados, pues una vez hace su ingreso en una red, realizan una búsqueda automatizada en todos los recursos disponibles con el fin de explotar otras vulnerabilidades que les permita propagarse. Ante esta amenaza, los principios de la seguridad de la información que se ven comprometidos son la disponibilidad, integridad y confidencialidad. (National Institute of Standards and Technology, 2006).

2.3 Métodos para la detección de puntos de acceso inalámbricos.

Para (Sachin R. , Sandeep P. , & Ajeet A. , 2013) existen diferentes metodologías o técnicas con las cuales se puede realizar la detección de puntos de acceso inalámbricos no autorizados, los cuales se describen a continuación con sus respectivos beneficios y desventajas:

2.3.1 Detección mediante técnicas estadísticas

Esta técnica consiste en instalar una herramienta o algoritmo de aprendizaje automatizado en un equipo centralizado por donde pase la información de la mayoría de los recursos de la red, como lo es la puerta de enlace predeterminada o el firewall de salida a internet, la cual sea capaz de analizar las propiedades de los paquetes asociados a los puntos de acceso inalámbricos legítimos y mediante la creación de una base de conocimiento se puede determinar cuándo un paquete posee un comportamiento anómalo. Debido a que el algoritmo de aprendizaje se basa en técnicas estadísticas debe ser capaz de tener una tolerancia o margen de error ante variantes que pueden tener las propiedades de los paquetes como resultado de factores de ruido. Generalmente este tipo de solución está conformada por dos elementos, el primero es un modelo de aprendizaje, con el que se evalúan parámetros como el tiempo de respuesta de los paquetes. El segundo es un

algoritmo probabilístico que determina la cantidad de saltos que debería dar un paquete. Según (Ganesh B., Vidya S., & Siddharth A., 2012) una de las limitaciones que presenta este tipo de metodología, es que no es capaz de detectar los puntos de acceso no autorizados generados por dispositivos externos y vecinos, los cuales son instalados, pero no tienen acceso directo a la red de la organización, por lo que el equipo centralizado nunca va a detectar el comportamiento anómalo de los paquetes.

Entre las ventajas que presenta esta metodología se tienen las siguientes:

- El algoritmo de análisis es liviano y no requiere exceso de recursos para poder procesar las tareas asignadas.
- Utiliza un algoritmo de aprendizaje y de probabilidades que trabajan en conjunto, lo cual lo convierte en una herramienta eficiente y eficaz.
- Es de más bajo costo que soluciones que requiere elementos de hardware dedicados.

Desventajas:

- Aunque resulta muy difícil de lograr, teóricamente el atacante podría ser capaz de modificar los paquetes para tratar de engañar el sistema, aunque requiere que se conozcan los parámetros que se están evaluando y las propiedades creadas por el modelo de aprendizaje.
- Si un punto de acceso legítimo posee mucha carga de red, se puede presentar variantes en la propiedad de los paquetes debido al nivel de procedimiento, provocando que las diferencias de paquetes enviados desde puntos de acceso legítimos y no autorizados sean poco distinguibles.
- Factores externos de la señal inalámbrica, como ruido, intensidad de la señal o condiciones ambientales pueden provocar falsos positivos.

- Es modelo teóricamente complejo difícil de entender e implementar.

2.3.2 Detección utilizando tiempos de respuesta

Método que se basa en el hecho de que un punto de acceso inalámbrico no autorizado que busca realizar un ataque de hombre en el medio generalmente posee dos tarjetas inalámbricas, una con la cual establece la red falsa con la que busca seducir al usuario para que se conecte y una segunda con la cual brinda salida a internet o se conecta al punto de acceso autentico.

El esquema de detección es orientado al lado del cliente y su principal objetivo es alertar al usuario cuando se está conectado a un punto de acceso no seguro, para esto ejecuta internamente herramientas como el traceroute hacia sitios previamente analizados y documentados, de esta manera se puede detectar inconsistencias en la cantidad de saltos que realiza un paquete para poder llegar a una dirección específica como lo es un servidor DNS.

Adicional a la cantidad de saltos se puede medir el tiempo de viaje (ida y vuelta) de paquetes ACK generados por herramientas como el ping, si el paquete es trasmitido por un equipo que posee dos tarjetas de red inalámbricas sufrirá un atraso en el tiempo de respuesta significativo.

Entre los principales beneficios que representa esta técnica están:

- Es un método práctico que cuyo principal objetivo es evitar que los usuarios se conecten a puntos de acceso inalámbricos no autorizados que buscan robar la identidad de puntos de acceso legítimos clonando el SSID y el BSSID.
- Es compatible con cualquier tipo de protocolo inalámbrico 802.11, sin importar si trabaja en la frecuencia 2.4Ghz y 5.8Ghz.
- Las desventajas que presenta son:

- Factores como saturación en el tráfico de red, ruido e intensidad de la señal puede generar resultados erróneos.
- No es fácil de implementar y requiere datos de referencia para realizar el análisis.
- Puede presentar limitaciones y problemas de compatibilidad en los equipos donde se necesite instalar.
- No es una solución práctica para todos los tipos de puntos de acceso inalámbricos no autorizados.

2.3.3 Análisis de clientes y señal

Esta técnica es muy similar a la anterior, consiste en instalar un cliente o aplicación en los equipos de los funcionarios, la cual se encargará de recolectar datos de las señales inalámbricas que detecta, y las enviará a un servidor centralizado que se encargará de procesar la información y detectar si existe algún comportamiento anómalo. Según (Sachin R. , Sandeep P. , & Ajeet A. , 2013) con el mecanismo se puede recolectar otros datos que pueden ser valiosos para el analizador de datos, como lo es la dirección IP y la ruta de salida que el punto de acceso entrega a los clientes, por decir un ejemplo, si dos puntos de acceso se llaman de forma idéntica, ambos asignan un mismo segmento de red y el seguimiento de rutas revela caminos diferentes, es un indicador que un punto de acceso es falso.

Por otra parte, también se indica que es una solución sumamente efectiva para los puntos de acceso inalámbricos no autorizados que buscan realizar un ataque de hombre en el medio mediante clonación de puntos legítimos. Entre las ventajas que presenta están las siguientes:

- Sumamente efectivo para la detección de cualquiera de los tipos de puntos de acceso inalámbricos no autorizados.
- No se requiere modificar la arquitectura de red pues la aplicación se ejecuta del lado del cliente.
- No se necesitan elementos de hardware especializados para recolectar los datos.
- Entre las principales desventajas se tiene:
- La aplicación puede presentar problemas de compatibilidad con dispositivos como teléfonos, tabletas o sistemas operativos poco comunes.
- Para el caso de dispositivos móviles que salen de la organización, requieren mecanismos para que no confundan redes inalámbricas de otros lugares con puntos de acceso inalámbricos no autorizados.

2.3.4 Análisis de señal mediante sensores

Este método se basa en la utilización de dos componentes, uno que funciona como cliente y otro como servidor. Para esto se colocan equipos o elementos de hardware que fungen como sensores de señales inalámbricas, los cuales se encargan de recolectar información de radio frecuencias que tiene a su alcance, les aplica un método de normalización de información y por último termina enviándola a un servidor o equipo capaz de analizar dichos datos. Entre la principal función que realiza el equipo de análisis es la clasificación de los puntos de acceso detectados, donde se debe determinar si un punto de acceso es confiable, es vecino o es desconocido (Indicador de que se trata de un punto de acceso inalámbrico no autorizado).

Entre las ventajas que presenta esta metodología se tienen:

- Está diseñado para que sea una solución liviana que no consume recursos de los clientes.
- Es capaz de detectar cualquier tipo de puntos de acceso inalámbrico no autorizados.
- Según la capacidad del sensor inalámbrico, el mismos puede ser utilizado como herramienta de defensa y anulación del punto de acceso inalámbrico no autorizado.
- Entre las principales desventajas se tienen:
- Requiere equipo de hardware adicional que realiza la función de monitoreo.
- Los equipos que se utilizan como sensor inalámbrico deben soportar el modo monitor.
- Se puede tener limitaciones en lugares donde se utilice diferente radio frecuencias en los equipos de comunicación inalámbricos.

2.4 Sistemas de monitoreo utilizando sensores inalámbricos

Debido a que el enfoque de la investigación se basa en la utilización de una Raspberry PI, se realizara énfasis en la creación de un modelo de monitoreo de puntos de acceso no autorizados utilizando el método de análisis de señal con sensores inalámbricos, en la cual la Raspberry se encargará de analizar los datos de radio frecuencias a su alcance y las enviará a un equipo que realice el análisis de los datos.

Según (Sachin R. , Sandeep P. , & Ajeet A. , 2013) un sistema de monitoreo de este tipo está conformado por 3 etapas, las cuales se describen a continuación:

- **Recolección de señales recibidas:** Esta función la realiza el sensor de señales inalámbricas, se puede destinar un equipo dedicado o un punto de acceso que cada cierto periodo cambie a modo monitor y recolecte los datos, no obstante,

de la segunda forma se pueden presentar problemas de rendimiento y compatibilidad.

El análisis puede ser realizado por el equipo de forma activa (envía un mensaje de prueba a los puntos de acceso que detecta y espera la respuesta) o pasiva (escucha las tramas de información de los puntos de acceso cercados entre 10 y 100 veces por segundo). El esquema de operación de estos dispositivos se podría representar como se muestra en la figura 2:

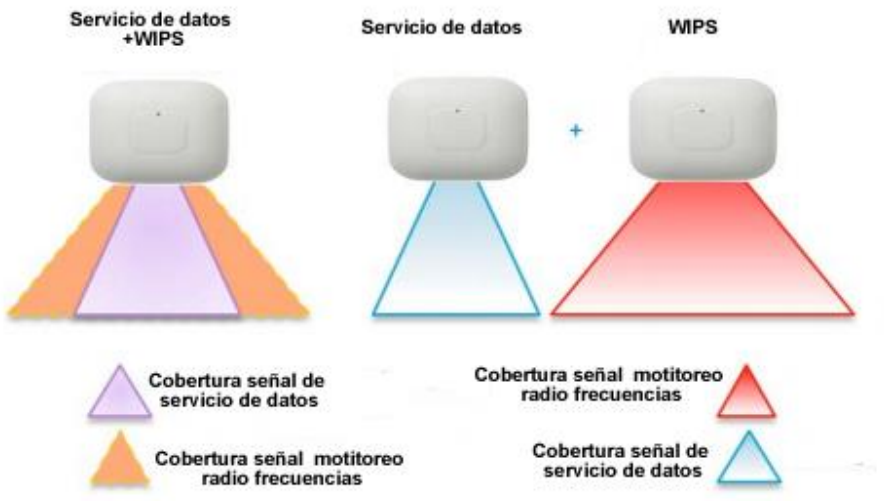


Figura 2: Representación gráfica de modos de operación de puntos de acceso con funciones de servicio de datos y monitoreo integrado o separado.

Fuente: (Cisco Systems, 2014).

Por otra parte, según (Cisco Systems, 2014) entre los principales parámetros que se deberían recolectar en esta etapa están la dirección MAC(BSSID) de los puntos de acceso, clientes conectados, SSID, indicadores de la potencia de señal RSSI (intensidad de la señal y nivel de ruido) y parámetros físicos como la frecuencia de operación, canal de frecuencia y fabricante.

- **Normalización de la información de las señales:** (Sachin R. , Sandeep P. , & Ajeet A. , 2013) mencionan que después de recolectar los datos por parte de los sensores de señal inalámbrica, se debe pasar por una etapa de normalización, en la

cual una primera tarea consiste en descartar señales que pueden producir falsos positivos, especialmente porque son de puntos de acceso generados por vecinos, y que son detectados con RSSI muy bajos o que son detectados de forma intermitente por los sensores. Según (NetSpot Community, s.f.) el RSSI es un parámetro que permite determinar la calidad de una señal inalámbrica, el cual se obtiene al aplicar una relación directa entre la intensidad de la señal y el ruido de la misma, las cuales son medidas en decibelio-milivatio(dbm). Para poder obtener el nivel del RSSI se debe medir la magnitud de ambos parámetros y aplicar la siguiente formula:

Margen SNR = señal (dBm) - ruido (dBm)

Se muestra un ejemplo práctico de como calcular el RSSI según la figura 3:

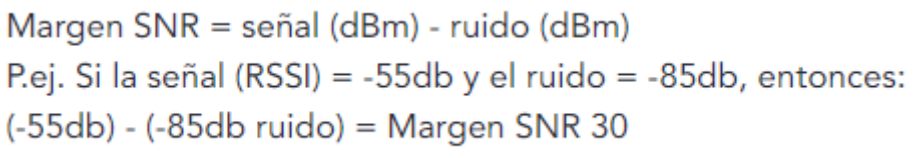


Figura 3: Caso práctico de como calcular el RSSI en base a los niveles de señal y ruido.
Fuente: (NetSpot Community, s.f.).

Para (NetSpot Community, s.f.) generalmente el nivel del RSSI se considera de buena calidad cuando tiene un valor mayor o igual a los -50dBm, mientras que si es menor o igual a -100dBm la calidad de la señal es nula, por lo que se considera inservible. Con base a las características brindadas por el autor, se establece la siguiente escala de medición para el nivel de calidad de las señales inalámbricas, como se muestra en la tabla1:

Tabla 1: Escalas de medición para la calidad de la señal.

Escala de calidad	Nivel RSSI
Alta	90% ~ = -55db
Media	50% ~ = -75db

Baja	30% ~ = -85db
Inutilizable	8% ~ = -96db

Fuente: (NetSpot Community, s.f.).

Escalas que también pueden ser representadas según el rango de dBm que presente el RSSI, como se muestra en la figura 4:

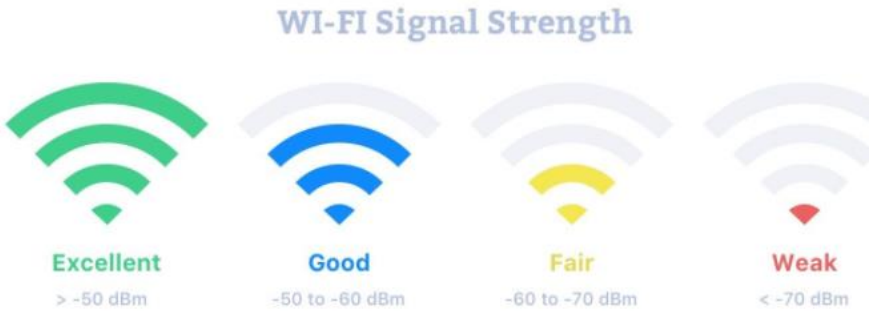


Figura 4: Escala de medición de la calidad de la señal según rango donde se ubique el RSSI.

Fuente: (NetSpot Community, s.f.).

Para (Cisco Systems, 2014), una vez que el análisis de las señales se ha realizado y se han descartado las que no se deben tomar en cuenta, se deben transforma los datos en un formato estandarizado con el cual se pueda enviar la información al equipo centralizado encargado de procesarla y generar las alarmas. El estándar utilizado por Cisco es SOAP/XML el cual viaja en un canal de comunicación bidireccional de forma segura.

En la figura 5 se muestra un posible diagrama de arquitectura de los datos estandarizados y protocolo de comunicación según (Telelink Company, 2013):

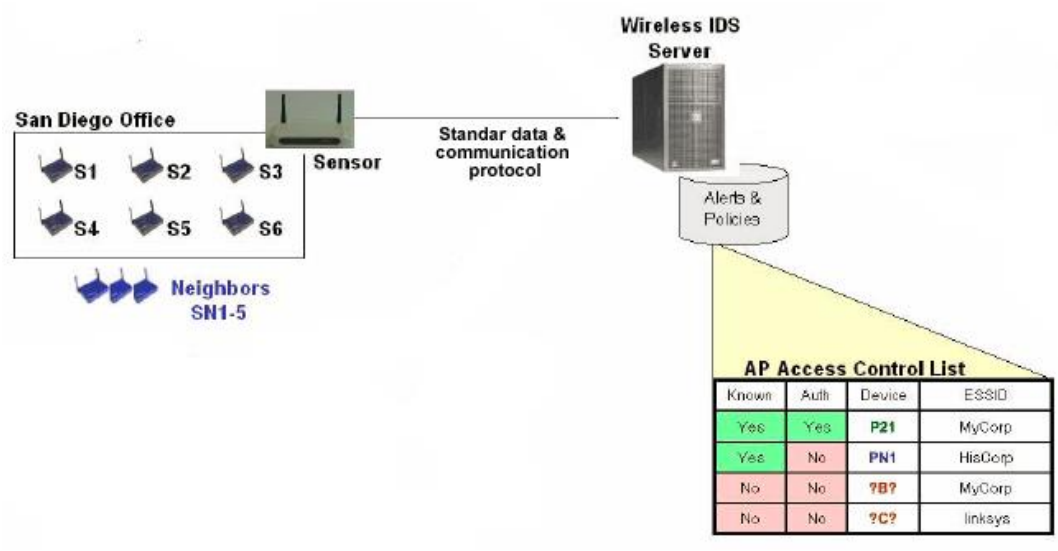


Figura 5: Diagrama de flujo de arquitectura de comunicación donde se representa la aplicación de estandarización de datos y protocolo de comunicación.

Fuente: (Telelink Company, 2013).

- **Clasificación de los puntos de acceso:** Esta etapa consiste en tomar la información recolectada por los sensores de señales inalámbricas y determinar con los datos obtenidos si el punto de acceso inalámbrico es autorizado o no. Para algunos autores como (Sachin R. , Sandeep P. , & Ajeet A. , 2013) esta tarea podría realizarse con base a la intensidad RSSI detectada por varios sensores y aplicando un algoritmo de triangulación para determinar si el emisor de la señal se encuentra dentro de las instalaciones de organización o no. Por otra parte, fabricantes de equipos de telecomunicaciones como (Juniper Networks, 2016) y (Cisco Systems, 2014) han optado por desarrollar soluciones donde un equipo centralizado posee una base de datos que maneja información asociada a los puntos de acceso autorizados, parámetros, puntos de acceso detectados e información de dispositivos clientes conocidos. Para (Juniper Networks, 2016) los puntos de acceso detectados por el sistema de monitoreo deberían recibir alguna de las clasificaciones que se muestran en la tabla 2:

Tabla 2: Tabla de clasificación de puntos de acceso detectados con su respectiva descripción.

Clasificación	Descripción
Miembro	Punto de acceso que se encuentra en el dominio de la organización, con la información recolectada se puede identificar como un punto de acceso autorizado.
Vecino	Dispositivo que no se encuentra del domino de la organización, sin embargo, está catalogado como confiable porque se detectó su SSID al momento de habilitar el sistema de monitoreo.
Sospechoso	Punto de acceso que con la información que se posee no se puede determinar si es confiable o no está autorizado, requiere participación de administrador de red para que le asigne alguna categoría.
No autorizado	Punto de acceso no autorizado en el aire, el cual ha sido clasificado en esa categoría por información comprobada o evidencias claras de ser un punto de acceso malicioso.

Fuente: (Juniper Networks, 2016).

Para (Juniper Networks, 2016) cuando se analiza cada uno de los puntos de acceso detectados por los sensores, se puede seguir el siguiente flujo para asignarles su respectiva clasificación, como se muestra en la figura 6:

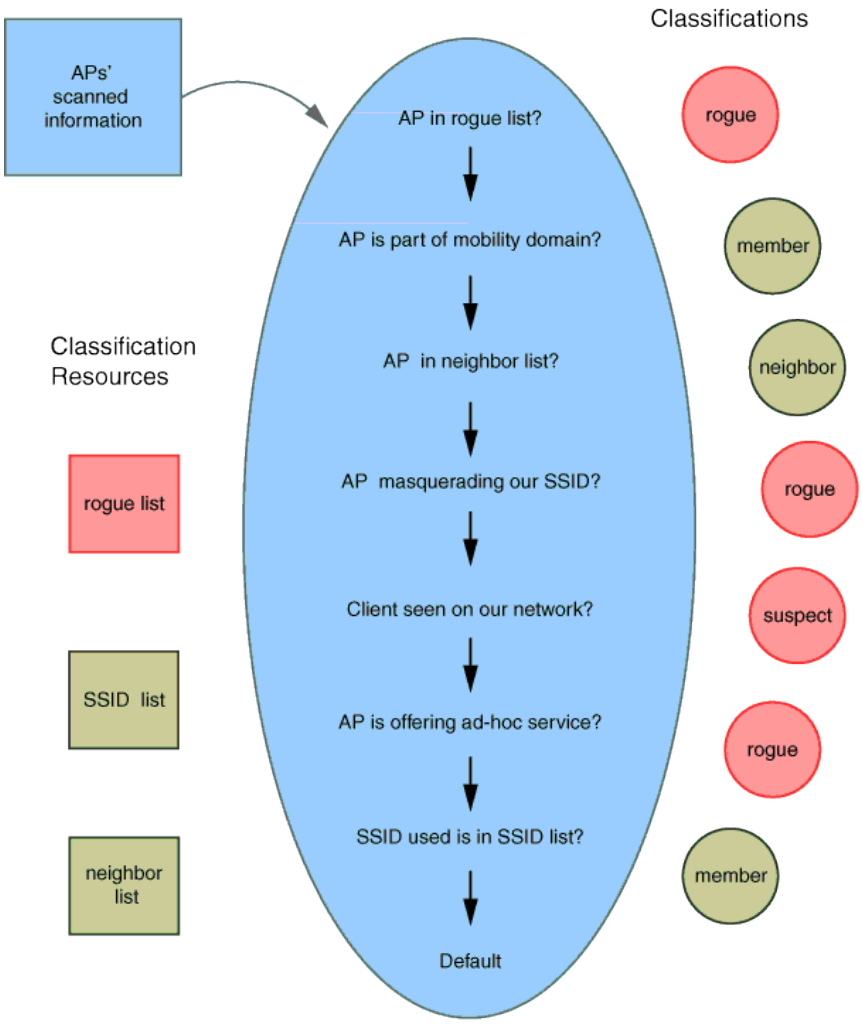


Figura 6: Flujo de proceso para clasificar puntos de acceso detectados en la categoría que corresponde.
Fuente: (Juniper Networks, 2016).

Como se puede ver en el proceso, para cada punto de acceso detectado se debe realizar un conjunto de validaciones hasta que los datos calcen en alguna de las condiciones, la primera condición consiste en verificar que el punto de acceso no se encuentre registrado en el repositorio de datos como no autorizado, la segunda y tercera verificación es tratar de identificarlo como miembro o vecino con base en la información recolectada en el repositorio de datos. Una cuarta validación es verificar si está clonando el BSSID de un punto de acceso clasificado como miembro, en este caso es un comportamiento malicioso y se clasifica directamente como un punto de acceso no autorizado. La siguiente evaluación es verificar que el punto de

acceso tenga conectado alguno de los dispositivos marcados como conocidos dentro de la organización, se clasifica como sospechoso. La penúltima condición es verificar si el punto de acceso esté operando en modo Ad-hoc, de ser así se clasifica como punto de acceso no autorizado, y por último se verifica si el SSID que está emitiendo se encuentra dentro de un listado de SSID reconocidos, los cuales tuvieron que ser identificados por el administrador de red cuando instaló el sistema de monitoreo. En caso de que el punto de acceso no cumpla con ninguno de los criterios mencionados anteriormente se deberá asignarle un estado por defecto que el administrador de red defina en los parámetros de configuración de la aplicación.

Un aspecto importante en la clasificación de puntos de acceso inalámbricos, es que por razones como ubicación física o condiciones ambientales existen dispositivos vecinos que pueden ser detectados de forma poco frecuente, pero que si no se les da el tratamiento necesario pueden generar falsos positivos; por esta razón el grupo de investigación consideró agregar una categoría adicional denominada “omitido”, para la cual la solución de monitoreo se debe entender como una señal que se conoce que existe pero que no debe ser procesada por el sistema para evitar que se generen alertas innecesarias.

2.5 Soluciones existentes.

Hasta este punto se ha definido cuáles son los principales mecanismos con los que se puede detectar los puntos de acceso inalámbricos no autorizados, así como las dificultades que representa para el administrador de red el poder detectarlos.

En esta sección se hará un resumen de 3 herramientas disponibles en el mercado que pueden ser utilizadas para tratar este tipo de amenazas, mencionando cuáles son sus principales características, ventas y desventajas, como se muestra a continuación.

2.5.1 Cisco Wireless Intrusion Prevention System / Cisco wIPS

Es una solución desarrollada por el fabricante de equipos de telecomunicaciones CISCO, la cual es una suite completa de seguridad inalámbrica que permite brindar acceso unificado a equipos dentro de la red, al mismo tiempo que realiza funciones de detección, localización, mitigación y contención de puntos de acceso no autorizados (cableados e inalámbricos) a nivel de capa de red 1 y 3. Las funciones de monitoreo las realiza mediante la metodología de uso de sensores de señales inalámbricas, donde los puntos de acceso que sirven los datos a los clientes también realizan funciones de monitoreo con el fin de recolectar datos de las señales inalámbricas que tienen a su alcance (Cisco Systems, 2014).

Entre los elementos que conforman la solución se tiene los que se detalla en la tabla 3:

Tabla 3: Detalla de los elementos que conforman la solución Cisco wIPS con sus respectivas funciones.

Componente	Características
Punto de acceso	Puntos de acceso con equipamiento de la tecnología CleanAir, que permite detectar a nivel de capa 1 amenazas y ataques que vienen de dispositivos que no utilizan el protocolo 802.11, como los son cámaras e interruptores de radio frecuencia. También permite realizar análisis de las potencias de señal RSSI y almacenar información de direcciones MAC de clientes y posibles atacantes en caso de que se detecte un comportamiento anómalo.
Punto de acceso con módulo de seguridad inalámbrico.	Puntos de acceso que posee el módulo de seguridad Cisco Aironet, el cual es capaz de escanear todos los canales de radio frecuencia 2.4Ghz y 5.8GHz, al mismo tiempo que puede ofrecer los datos a dispositivos clientes sin tener ningún tipo de afectación en el rendimiento.
Controlador	Es un módulo encargado de enviar tramas al sistema de

inalámbrico LAN(WLC).	administración de red cuando un evento de seguridad se reporta, como la detección de un punto de acceso no autorizado o un ataque de denegación de servicio. Adicionalmente trata de mitigar dichas amenazas con base en la política de seguridad que se le haya configurado.
Motor de servicio móvil cisco (MSE)	Componente que recibe la información de los controladores, puntos de acceso y sus respectivas localizaciones y las grafica en un mapa de ubicación donde despliega información en tiempo real de direcciones MAC detectadas, sellos de tiempo, señales RSSI e identificadores de ataques. Se caracteriza porque puede analizar la información de diferentes eventos y remueve eventos duplicados generados por una misma amenaza, lo que permite un mejor enfoque por parte del personal encargado de tomar las acciones necesarias.
Infraestructura Cisco Prime(WCS)	Recibe datos desde el módulo MSE y genera paneles de monitoreo, configuración, reportes, localización en el mapa de puntos de acceso no autorizados, clientes válidos y no autorizados, sistemas de alarmas, eventos de seguridad y herramientas de captura de datos forenses.

Fuente: (Cisco Systems, 2014).

Según la figura 7, se muestra el diagrama de arquitectura de la solución Cisco wIPS:

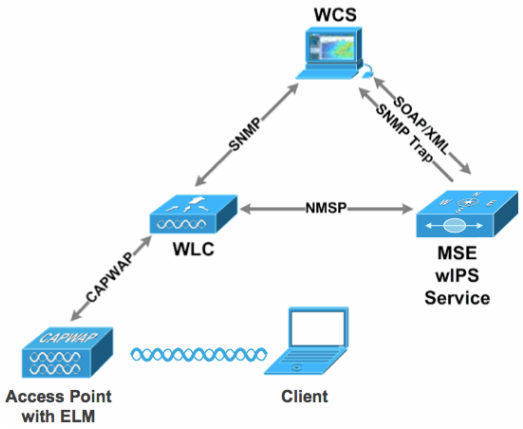


Figura 7: Diagrama de arquitectura de la solución de monitoreo Cisco wIPS.

Fuente: (Cisco Systems, 2014).

Según (Cisco Systems, 2014) las principales ventajas que presenta la solución son las siguientes:

- Es capaz de realizar análisis de las señales inalámbricas y tráfico de red, lo cual lo convierte en una solución integral que permite realizar monitoreo de los dispositivos en tiempo real de una forma más precisa y completa.
- Debido a que es una solución inmersa dentro de la arquitectura de red es capaz de realizar acciones correctivas que permitan una rápida respuesta ante la detección de un incidente de seguridad.
- Entre las desventajas se puede listar:
- No todos los modelos de puntos de acceso inalámbricos Cisco tienen soporte para los WIPS.
- Al ser una solución propietaria es poco compatible con dispositivos de otras marcas y fabricantes.
- Requiere el uso e instalación de 5 componentes para su correcto funcionamiento.
- Es una solución pensada para infraestructuras grandes, donde el costo del Cisco Prime, MSE, EML y WLC puede rondar los $15000, más un costo adicional que ronda entre los $500 y $800 que representa el valor de cada punto de acceso que se requiera instalar.

2.5.2 HP Mobility Security IDS/IPS System series

Sistema de detección de puntos de acceso no autorizados desarrollado por el fabricante de equipos de cómputo Hewlett-Packard Company, el cual se caracteriza por estar conformado por dos componentes principales que ejecutan la funcionalidad de monitoreo: controlador de radio frecuencia y dispositivos que se

instalan como sensores de señales inalámbricas, el cual se encarga de recolectar datos y enviarlos al controlador (Hewlett-Packard, 2013).

Entre las principales ventajas que brinda esta solución se tienen:

- Sistema integrado que permite la detección y prevención automatizada de incidentes de seguridad, como puntos de acceso inalámbricos no autorizados, ataques de denegación de servicio y ataques de rompimiento de seguridad WEP.
- El sistema utiliza un algoritmo patentizado que permite eliminar los falsos positivos utilizando mecanismos de clasificación y mitigación que permiten bloquear el tráfico inalámbrico no autorizado sin afectar el rendimiento de los puntos de acceso legítimos.
- Los sensores son capaces de realizar escaneos de forma continua en las diferentes variables de redes inalámbricas que utilizan el protocolo 802.11, como los tipos a, b, g y n.
- Posee herramienta de reportes simplificada y comprensiva, la cual puede ser utilizada para emitir informes de auditoría.
- Estimación de posicionamiento físico donde se presenta el ataque o amenaza.
- Detecta y localiza interferencia inalámbrica no Wifi e interruptores de radio frecuencia.
- Los sensores son capaces de recolectar información y enviarla posteriormente en caso de que se produzca un fallo en la comunicación con el controlador.

Según las características del producto que menciona (Hewlett-Packard, 2013), se pueden deducir algunos datos que pueden ser considerados como desventajas del producto, los cuales se mencionan a continuación:

- El controlador de radio frecuencias es una solución de alto costo que requiere un equipo de hardware especializado, el precio base para un aplicativo con soporte para 50 sensores puede rondar los $9500. Adicionalmente el costo de cada sensor ronda los $50.
- Es un producto cuya vida útil está llegando a su fin y actualmente está siendo remplazado por una nueva línea de producto de la empresa, la cual se denomina Aruba RFProtect, la cual está enfocada en la protección de dispositivos de internet de las cosas.

2.5.3 AirMagnet Enterprise

Aplicación para la detección y protección de puntos de acceso inalámbricos falsos y no autorizados que fue desarrollada por el fabricante Fluke Networks, las principales funcionalidades que permite realizar son detectar, bloquear, trazar y localizar amenazas de seguridad de la información relacionadas con la tecnología Wifi, se caracteriza porque está compuesta por dos módulos de operación principales, los cuales son un conjunto de sensores que recolectan datos de la radio frecuencias que tienen a su alcance y un servidor centralizado donde se ejecuta un aplicativo que se encarga de realizar tareas de análisis, reportes y alertas (Fluke Networks, 2012).

Se describe las principales características de cada uno de los componentes que conforman la solución, según se muestra en el detalle de la tabla 4:

Tabla 4: Detalle de los componentes que conforman la solución AirMagnet.

Componente	Características
AirMagnet Enterprise Console	Solución centralizada donde se recibe toda la información recolectada por los sensores y es procesada, entre las funciones que realiza están las siguientes: alerta de eventos, análisis, contención y descarte de amenazas detectadas, escalamiento de

	casos, solución de problemas de forma remota, análisis forense, análisis de la salud de la red, verificación de cumplimiento de políticas y generación de reportes.
AirMagnet Software Sensor Agent	Componente de hardware que realiza monitoreo del estado de la radio frecuencias de forma constante, se caracteriza porque tiene soporte para las dos frecuencias (2.4Ghz y 5.8Ghz) que pueden ser utilizadas en Wifi, aparte que tiene capacidad para analizar las radio frecuencias utilizadas en tecnología celular. Una característica destacable es que el sensor se puede conectar vía inalámbrica, por lo que se disminuye y simplifica la arquitectura de instalación, al requerir menos cables de red.

Fuente: (Fluke Networks, 2012)

En la figura 8 se muestra un ejemplo del funcionamiento de la arquitectura de la solución AirMagnet:

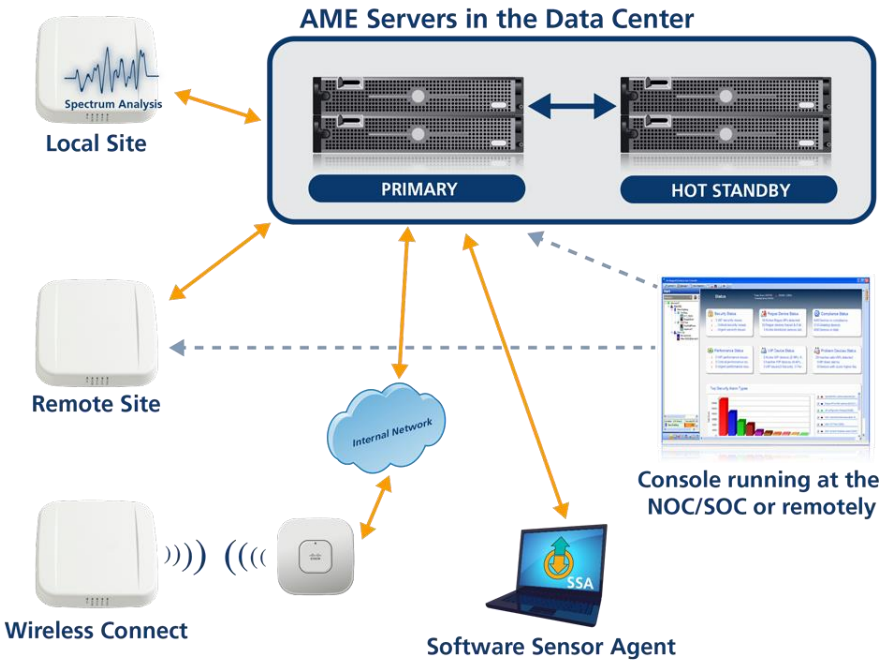


Figura 8: Diagrama de funcionamiento de la solución AirMagnet.

Fuente: (NetScoup Solutions).

Según (Fluke Networks, 2012) las principales ventajas que presenta esta solución son las siguientes:

- Es una solución sumamente escalable en la cual se puede llegar a integrar hasta 1000 sensores y no se requiere mayor consumo de ancho de banda.
- Capacidad de correlacionar eventos de información obtenida de diferentes sensores, lo cual permite realizar un mejor análisis, evitar duplicación de alarmas y falsos positivos.
- Permite generar reportes de análisis del estado de la red, radio frecuencias, eventos de seguridad e interferencia que cumplen con el formato de varios estándares internacionales como el ISO 27001.
- Interfaz gráfica amigable que permite solucionar problemas remotamente en tiempo real.
- Permite realizar clasificación automatizada de los dispositivos.
- La consola administrativa se puede adquirir como una solución completa que incluye el hardware o se puede instalar en un servidor de otro fabricante que cumpla con el requisito de poseer una instancia del sistema operativo Microsoft Windows Server 2012 o superior.
- Soporte de notificaciones en diferentes formatos como correo electrónico, SMS, logs del sistema, SMNP, sonidos, entre otros.
- Entre las desventajas que se encontraron de la aplicación se tienen:
- La consola administrativa como una solución completa (incluye él hardware) tiene un costo elevado, el precio inicial puede superar los $11.000.
- Si se instala la consola administrativa en un servidor de otro fabricante se debe pagar una licencia por usuario, la cual tiene un costo aproximado de $4000.

Adicional a estos costos se debe sumar licencias de sistema operativo y base de datos.

- El valor de cada sensor que se implemente es aproximadamente $100.
- No es una solución tan comercializada como la de Cisco y HP, por lo que puede ser difícil encontrar un distribuidor autorizado en regiones fuera de los Estados Unidos de América.

Capítulo 3. Estado de la cuestión

3.1 Planificación de la revisión

3.1.1 Formulación de la pregunta

Ante el eminente riesgo que puede representar un punto de acceso inalámbrico no autorizado y lo difícil que puede ser monitorear y detectar esta amenaza en las redes de las organizaciones, surge la siguiente interrogante: ¿Es posible crear un sistema de detección de intrusos inalámbricos utilizando una Raspberry PI y tecnologías de código abierto?

3.1.2 Foco de la pregunta

Con base en la revisión sistemática se pretende identificar trabajos de investigación asociados con el tema de sistemas de detección de intrusos inalámbricos(WIDS), así como temas asociados a soluciones de código abierto que puedan ser utilizadas en conjunto con una Raspberry Pi para solucionar el problema descrito en la sección introductoria.

3.1.3 Amplitud y calidad de la pregunta

En esta sección se define un conjunto de secciones y apartados en los que se puede analizar aspectos relacionados con el problema por tratar, se define la pregunta de investigación y el conjunto de palabras claves que permitan definir la amplitud y calidad de la pregunta.

3.1.3.1 Problema

Tal y como se indicó en los apartados del problema y la justificación de la sección introductoria, la problemática se presenta debido a que la detección de puntos de acceso inalámbricos no autorizados puede ser una tarea difícil de resolver para los administradores de red, especialmente porque requiere monitoreo

constante, al mismo tiempo que las soluciones existentes son exclusivas hacia empresas que manejan enormes presupuestos para el área de la seguridad de la información, además, dichas soluciones no son compatibles con todas las marcas de equipos de telecomunicaciones. De esta manera el trabajo de investigación se centra en el estudio de los principales mecanismos para la detección y monitoreo de puntos de acceso inalámbricos y los métodos que permitan aminorar el impacto de los riesgos asociados.

3.1.3.2 Pregunta de investigación

Basándose en la definición del problema se puede establecer la pregunta de investigación de la siguiente manera: “¿Cuáles trabajos de investigación aplicada en la detección y monitoreo de puntos de acceso inalámbricos no autorizados se han llevado a cabo utilizando una Raspberry PI y tecnologías de código abierto?”.

3.1.3.3 Palabras clave y sinónimos

A continuación, se define el conjunto de palabras claves asociadas a la pregunta de investigación, así como los correspondientes sinónimos que serán utilizados para formular las cadenas de búsqueda que permitan identificar los trabajos de investigación asociados con el tema en las diferentes bases de datos que serán utilizadas.

Según la tabla 5 se describe el listado de palabras claves y sus respectivos sinónimos:

Tabla 5: Listado de palabras claves y respectivos sinónimos que serán utilizados para establecer las cadenas de búsqueda.

Palabra clave	Sinónimo	Área asociada
Detección intrusos inalámbricos.	WIPS	Monitoreo y detección.
Punto de acceso no	Rogue Access	Redes inalámbricas.

autorizado.	point	información.
seguridad inalámbrica.	Wireless security, wireless risk.	Seguridad de la información. Redes inalámbricas.
Sensor inalámbrico	Wireless sensor	Monitoreo y detección.
Raspberry PI.		Telecomunicaciones y seguridad de la información.

Fuente: Elaboración propia.

3.1.3.4 Intervención

Se busca encontrar fuentes que posean la mayor cantidad de palabras claves para posteriormente analizarlas. Para esto se realizará una revisión sistemática de fuentes existentes cuyo tema de investigación esté asociado a sistemas de monitoreo y detección de intrusos inalámbricos.

3.1.3.5 Control

Las fuentes seleccionadas serán las que se obtengan del proceso de búsqueda y análisis en las diferentes bases de datos. En el conjunto de resultados no se utiliza ningún trabajo inicial que pueda ser considerado como la fuente primaria de investigación.

3.1.3.6 Resultado

Con los resultados de la búsqueda se pretende identificar fuentes asociadas al tema de monitoreo y detección de intrusos inalámbricos utilizando tecnologías de código abierto y Raspberry PI, el cual permita obtener una base de conocimiento de referencia que permite crear una solución integral capaz de solventar la problemática descrita en el trabajo de investigación.

3.1.3.7 Diseño experimental

El meta análisis de la revisión se enfoca en analizar y extraer los aportes principales de las fuentes en el área de monitoreo y detección de intrusos

inalámbricos, así como métodos y tecnologías de código abierto existentes que se puedan unificar junto a las características que brinda el hardware de una Raspberry PI en una solución integral.

3.2 Selección de fuentes

3.2.1 Definición del criterio de selección de fuentes

La selección de fuentes se desarrolla en dos etapas, en la primera se realiza la búsqueda e identificación de fuentes en las bases de datos seleccionadas utilizando los criterios establecidos. En la segunda, el grupo de investigación determinará cuáles fuentes son relevantes y cuáles serán excluidas con base en la experiencia y conocimiento técnico del área de investigación.

3.2.2 Lenguaje de estudio

El lenguaje de estudio será el inglés, debido a que es el idioma en el que generalmente se escribe los procedimientos, definiciones y estándares asociados a tecnologías de información, esto con el fin de facilitar las tareas de búsqueda y análisis de fuentes asociadas con el tema de investigación.

3.2.3 Identificación de fuentes

3.2.3.1 Método de selección de fuentes

La metodología utilizada para seleccionar las fuentes se basa en extraer un listado de repositorios obtenidos como resultado de aplicar los criterios de búsqueda en las bases de datos seleccionadas, para posteriormente clasificarlas como relevantes o no, con base en la experiencia profesional de los miembros que conforman el grupo de investigación.

3.2.3.2 Lista de fuentes

El repositorio de datos que se utilizará en la revisión sistemática es el siguiente:

- DBLP

Otros repositorios fueron descartados debido a que las fuentes que tienen disponibles no están enfocadas en el área de las tecnologías de información, no son de libre acceso o se debe pagar pada poder consultarlas.

3.2.3.3 Cadenas de búsqueda

Basándose en el conjunto de palabras claves definidas previamente y en los operadores de lógica booleana AND o OR, se define las siguientes cadenas de búsqueda que serán utilizadas en el repositorio de datos:

- (((wireless intrusion detection) AND rogue access point) AND risk OR security).
- ((raspberry pi) AND wireless sensor)

3.2.3.4 Selección de fuentes después de la evaluación

En la sección de fuentes será incluida cualquiera que cumpla con los criterios de búsqueda establecidos en secciones anteriores, y que se encuentre disponible dentro del repositorio de datos elegido.

3.2.3.5 Comprobación de las fuentes

La comprobación de fuentes se realiza ejecutando las cadenas de búsqueda en el repositorio de datos seleccionado. Se asume que este repositorio es suficiente para desarrollar este apartado de la investigación, por lo que no serán incluidos más repositorios después de la primera revisión.

3.3 Selección de los estudios

3.3.1 Definición del criterio de inclusión y exclusión de estudios

Los criterios de inclusión y exclusión de fuentes están basados en una primera selección donde se extraen las fuentes que posean palabras claves utilizadas en la búsqueda. En una segunda fase el grupo de investigación determina las fuentes relevantes con base en el conocimiento y experiencia profesional en el área de investigación.

3.3.2 Definición de tipos de estudio

Se utiliza cualquier tipo de estudio que cumpla con los criterios de búsqueda, y no se hará énfasis en ningún específico.

3.3.3 Procedimiento para la selección de los estudios

El procedimiento para la selección de estudios estará conformado por el siguiente flujo:

- Definición de criterios de búsqueda.
- Definición de los repositorios de búsquedas.
- Ejecución de la búsqueda.
- Aplicar criterios de inclusión y exclusión.
- Extraer información de estudios relevantes (superaron los criterios de inclusión).

3.4 Ejecución de la revisión

En esta sección se elabora una descripción detallada del proceso de búsqueda en la base de dato selecciona.

3.4.1 Ejecución de la selección en la fuente DBLP

3.4.1.1 Selección de estudios iniciales

La búsqueda se realiza utilizando la opción “Semantic Scholar Search”, la cual nos brinda la facilidad de ingresar la consulta en formato booleano definido en las secciones anteriores, tal como se muestra en la Figura 9.

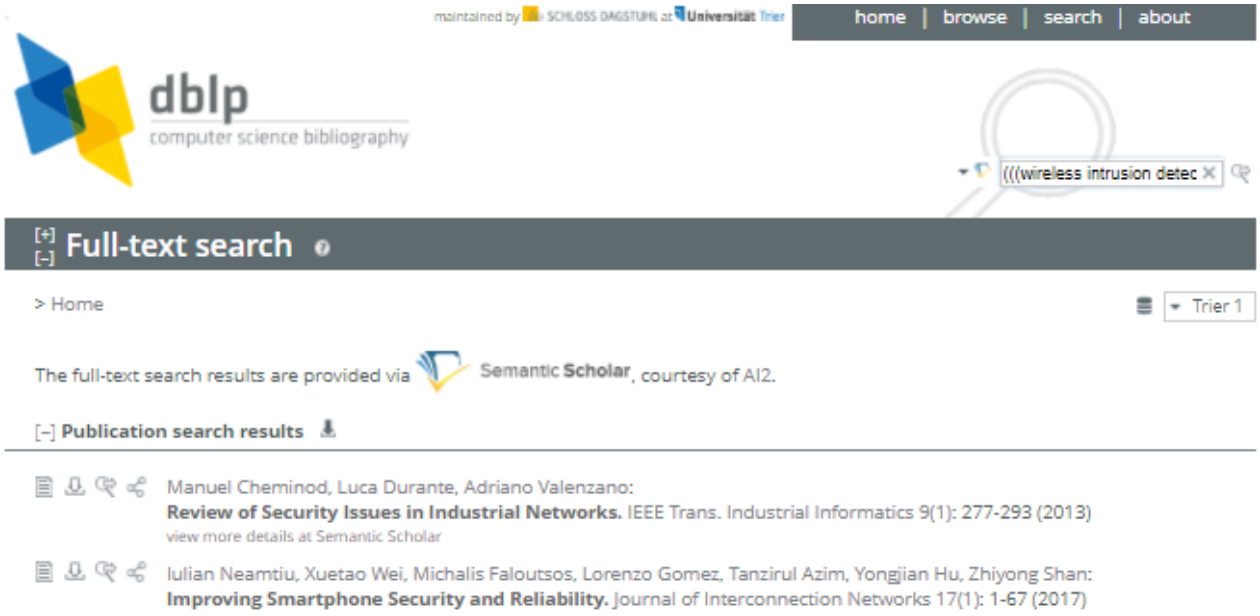


Figura 9*:* Parámetros de búsqueda de la consulta en la base de datos de DBLP.

Fuente: http://dblp.uni-trier.de/search/

Como resultado de la ejecución de la búsqueda se obtuvo 116 resultados, de los cuales al aplicar los parámetros de inclusión y exclusión se seleccionaron las fuentes que se muestran en la tabla 6.

Tabla 6: Fuentes obtenidas como resultado de aplicar los criterios de búsqueda en el repositorio de datos DBLP.

1	Rogue Access Point Detection System in Wireless LAN
2	A Review of Online Rogue Access Point Detection
3	Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN
4	Unauthorized Access Point Detection in Wireless Lan
5	Received signal strength indication (RSSI) code assessment for wireless sensors network (WSN) deployed Raspberry-Pi

Fuente: elaboración propia.

3.4.1.2 Evaluación de la calidad de los estudios

Debido a que las fuentes se obtuvieron de una base de datos reconocida, se asume que superaron los filtros y evaluaciones necesarias para ser consideradas como confiables.

3.4.1.3 Extracción de información

3.4.1.3.1 Definición del criterio de inclusión y exclusión de información

Para identificar las fuentes consideradas como relevantes, se realizó un análisis del contenido de las mismas, y se eligió las que tenían aportes significativos en las siguientes áreas:

- Riesgos en las redes inalámbricas.
- Detección de intrusos inalámbricos.
- Puntos de acceso no autorizados.
- Sensores Wireless y Raspberry PI.

3.4.1.3.2 Formulario para la extracción de información

Se muestra la tabla 7 la cual es utilizada como una plantilla resumen que permite extraer la información más relevante de cada una de las fuentes seleccionadas:

Tabla 7: Cuadro resumen utilizado para extraer la información relevante de cada fuente obtenida.

Título	
Publicación	
Autores	
Dirección de referencia	
Área	

Aspectos relevantes:

Fuente: elaboración propia.

3.4.1.3.3 Extracción de resultados objetivos y subjetivos

Se detalla el contenido de las tablas de la 8 al 13 donde se visualiza la información resumen de cada una de las fuentes incluidas en el resultado de la búsqueda de la base de datos DBLP.

Tabla 8: Cuadro resumen de la fuente 1 obtenido de la base de datos DBLP.

Título	Rogue Access Point Detection System in Wireless LAN.
Publicación	International Journal of Computer Technology and Electronics Engineering 2012.
Autores	Ganesh B. Bandal, Vidya S. Dhamdhere, Siddharth A. Pardeshi.
Dirección de referencia	https://www.semanticscholar.org/paper/Rogue-Access-Point-Detection-System-in-Wireless-LA-Bandal-Dhamdhere/41a44df312f08ce3551a932335310d6e542e2fa7
Área	Wireless communication, communication system security.

Aspectos relevantes: El autor hace una breve explicación en lo que consiste un punto de acceso no autorizado y los riesgos potenciales que puede representar para la seguridad de la información de las compañías. Adicionalmente hace mención que la mayoría de las soluciones para este tipo de problemas son muy costosas, especialmente porque requieren equipos especializados que estén monitoreando el estatus de las radio frecuencias, o que exista personal de TI dedicado a estar realizando escaneos manuales dentro de las instalaciones de la empresa, solución poco eficiente debido a que el punto de acceso no autorizado puede ser apagado por el usuario que lo instaló cuando detecte que un monitoreo se esté llevando a cabo, adicionalmente indica que con el incremento en el uso de la frecuencia de 5.8Mhz ha venido a complicar más aun las tareas de monitoreo.

Él propone un algoritmo para identificación de puntos de acceso no

autorizados utilizando la arquitectura de red local inalámbrica que permita solucionar el problema a un bajo costo, para esto indica que se debe utilizar puntos de acceso inalámbricos capaces de operar en modo normal y escáner, y se deben tener conmutadores capaces de habilitar y deshabilitar puertos remotamente utilizando el protocolo SNMP.

El algoritmo básicamente consiste en estar cambiando los puntos de acceso autorizados cada cierto periodo de modo normal a monitoreo, y recolectar información del estatus de la radio frecuencias en un formato normalizado, donde se puede recolectar información como el SSID y la dirección Mac de cada punto de acceso detectado, información que será enviada a un sistema centralizado que analice si es un punto de acceso es desconocido o confiable. Si el punto de acceso es desconocido y se logra determinar que brinda acceso a la red de la compañía, el sistema centralizado deberá apagar el puerto del conmutador donde se conectó el punto de acceso, utilizando el protocolo de gestión SNMP.

Fuente: elaboración propia.

Tabla 9: Cuadro resumen de la fuente 2 obtenido de la base de datos DBLP.

Título	A Review of Online Rogue Access Point Detection.
Publicación	International Journal of Computer Technology and Electronics Engineering 2013.
Autores	K Tejaswi, Syed Umar, K Bhavana.
Dirección de referencia	https://www.semanticscholar.org/paper/A-Review-of-Online-Rogue-Access-Point-Detection-Tejaswi-Umar/d0ed1b76a7acad87e8bb816c84444e4cf6a64b7c
Área	Wireless communication, communication system security.

Aspectos relevantes: El autor hace una introducción describiendo en qué consiste un punto de acceso no autorizado, indica que en muchas ocasiones son instalados por los propios usuarios de la empresa para obtener beneficios propios o

con la intención de ayudar a un usuario malicioso a que realice un ataque de hombre en el medio. Según la fuente los puntos de acceso no autorizados pueden ser detectados de formas efectivas, la primera es monitoreando permanentemente las ondas de radiofrecuencia, en búsqueda de cambios en la información que se obtiene frecuentemente, también indica que esta tarea depende del apoyo de equipos como enrutadores y conmutadores. El segundo método es mediante el análisis de paquetes en un equipo centralizado, como puede ser el caso de la puerta de enlace predeterminada, en la cual se observa si un host está conectado a una red cableada o inalámbrica, y si se encuentra en el inventario de dispositivos autorizados a estar conectados en la red. Si se detecta que el host está conectado mediante un medio no autorizado (inalámbrico cuando el registro es cableado, por ejemplo), o si se detecta un equipo que no está registrado dentro del inventario de dispositivos conocidos, es un claro indicador que un punto de acceso no autorizado se ha instalado en la red de la empresa. Según el artículo el primer método puede presentar problemas como compatibilidad, escalabilidad y costos, mientras que el segundo requiere poco esfuerzo y tiene un nivel de integración muy alto, no obstante, puede ser que resulte menos eficaz porque tiende a producir más falsos positivos.

La investigación desarrolla toda una metodología de detección de puntos de acceso inalámbricos no autorizados utilizando el segundo método, en el cual se propone un algoritmo que analiza los paquetes que pasan por la puerta de enlace determinada a nivel de capa 2 y 3. Adicionalmente se complementa con un algoritmo que utiliza un set de datos iniciales de entrenamiento que permite determinar el comportamiento de los paquetes ACK de las redes cableadas e inalámbricas y con base a patrones se puede identificar si un dispositivo que

debería tener comportamiento de red cableada se asemeja al de una red inalámbrica y viceversa.

Fuente: elaboración propia.

Tabla 10: Cuadro resumen de la fuente 3 obtenido de la base de datos DBLP.

Título	Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN.
Publicación	International Journal of Advanced Research in Computer Science and Software Engineering 2013.
Autores	Sachin R. Sonawane, Sandeep P. Chavan, Ajeet A. Ghodeswar.
Dirección de referencia	https://www.semanticscholar.org/paper/Study-of-Different-Rogue-Access-Point-Detection-an-Sonawane-Chavan/fdd576255ac26cccc6f427ddb5e88c1268ff6b94
Área	Wireless communication, communication system security.

Aspectos relevantes: El autor hace una breve reseña de la evolución que la tecnología Wireless ha tenido, y todas las ventajas en eficiencia y productividad que ha traído a las empresas. Después de esto define qué es un punto de acceso no autorizado, los riesgos que puede representar para la seguridad de la información, e inclusive lo define como una de las principales amenazas asociadas a la tecnología WIFI. Según el artículo, uno de los principales métodos para la detección de puntos de acceso no autorizados o falsos, es analizar el tráfico inalámbrico con dispositivos adicionales a los puntos de accesos legítimos. En la investigación se detalla algunas de las principales técnicas que pueden ser utilizadas para detectar puntos de acceso no autorizados:

- Esquema de detección utilizando estadísticas: Este mecanismo se utiliza generalmente para detectar los puntos de acceso no autorizado que se han instalado con el fin de realizar un ataque de hombre en el medio. Se basa en el uso de algoritmos que analicen el tráfico que pasa por un equipo centralizado (puerta de

enlace determinada), donde se puede estimar las variaciones de las propiedades de los paquetes asociados a las redes inalámbricas y mediante técnicas estadísticas y métodos de inteligencia artificial qué permite determinar que tanto se alejan las características de un equipo en específico del comportamiento de un punto de acceso autorizado.

- Entre las ventajas que presentan es que son algoritmos livianos que no requieren mucho procesamiento, las desventajas es que los atacantes pueden tratar de esquivar el mecanismo mediante la manipulación de los paquetes.
- Esquema de detección utilizando tiempo de respuesta: Esta técnica también es utilizada para detectar puntos de acceso cuyo fin es realizar un ataque de hombre en el medio. Se basa en que un punto de acceso no autorizado requiere tener dos tarjetas inalámbricas para realizar este tipo de ataque, una con la que se conecta al punto de acceso válido que obtiene internet, y la segunda con la que se activa el punto de acceso al que se deben conectar las víctimas. Tomando parámetros como la cantidad de saltos que debe realizar un paquete para llegar a un equipo determinado o teniendo estadísticas del tiempo que requiere un paquete ACK generado por la herramienta ping para moverse de un lado a otro, variaciones en esos parámetros son indicadores que se ha detectado un punto de acceso no autorizado. Entre las principales ventajas que presenta es que es una técnica compatible con el protocolo 802.11 y que hace énfasis en los ataques de hombre en el medio, los cuales pueden ser considerados de los más peligrosos en este tipo de vulnerabilidad. Como desventaja se tiene que algunas condiciones del ambiente o la red puede provocar fluctuaciones en el tiempo de respuesta, por lo que puede generar falsos positivos.
- Esquema de detección utilizando los niveles de señal recibidos: Consiste en

recolectar información asociada a las radiofrecuencias detectadas por los puntos de accesos autorizados, en los cuales se estandariza para obtener información como el SSID, la dirección MAC, nivel de la señal, ruido e interferencia. Una vez que se obtiene la información se puede calcular un índice de correlación empírico que permita identificar la probabilidad de que una señal sea catalogada como un punto de acceso no autorizado. Entre los beneficios que presenta es que se puede realizar mediante dispositivos de monitoreo dedicados o mediante una solución que se ejecute del lado del cliente. Las desventajas serían que para garantizar la movilidad del cliente se requiere activar el sistema de monitoreo en plataformas y lugares específicos.

Fuente: elaboración propia.

Tabla 11: Cuadro resumen de la fuente 4 obtenido de la base de datos DBLP.

Título	Unauthorized Access Point Detection in Wireless Lan.
Publicación	Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on.
Autores	Sandeep B. Vanjale, P. B. Mane, Sandip V. Patil.
Dirección de referencia	https://www.semanticscholar.org/paper/Wireless-LAN-Intrusion-Detection-and-Prevention-sy-Vanjale-Mane/0d551e09d3dd3b887f3d59fcc333e8cb12f2ee06
Área	Wireless communication, communication system security.

Aspectos relevantes: El autor hace una introducción explicando en qué consiste un punto de acceso no autorizado, y los peligros que se corren si los mismos no se descubren a tiempo. Indica que este tipo de acceso puede representar amenazas como degradación de la red o pérdida de información sensible. Menciona que la mayoría de las soluciones para el monitoreo y detección de este tipo de vulnerabilidad son poco automatizadas y dependen de tecnologías específicas que las hacen poco accesibles y eficientes. Además, explica que, para

desarrollar un sistema de detección de puntos de acceso inalámbricos no autorizados, se deben manejar dos fases, en la primera se identifica la presencia de puntos de acceso inalámbricos, mientras que en la segunda se debe determinar cuáles son falsos o no. En la fuente se propone la creación de un algoritmo de que sea capaz de analizar las huellas digitales de cada uno de los puntos de acceso asociados a las señales detectadas, y de esta manera poder identificar si un punto de acceso es falso o no.

Para esto se deben utilizar clientes que trabajan como monitores, que se encargan de tomar información como características de la señal y transmisión de datos, para posteriormente enviarlos a un servidor que analiza los datos y determina si el punto de acceso es falso o no.

Fuente: elaboración propia.

Tabla 12: Cuadro resumen de la fuente 5 obtenido de la base de datos DBLP.

Título	Received signal strength indication (RSSI) code assessment for wireless sensors network (WSN) deployed Raspberry-Pi
Publicación	Robotics, Automation and Sciences (ICORAS), International Conference on
Autores	M. I. Jais, T. Sabapathy, M. Jusoh, P. Ehkan, L. Murukesan, I. Ismail, R. B. Ahmad
Dirección de referencia	https://www.semanticscholar.org/paper/Received-signal-strength-indication-RSSI-code-asse-Jais-Sabapathy/04c7c83fbaa4ed2ac3460db3b0a759c51631908e
Área	wireless sensor networks, RSSI

Aspectos relevantes: En la fuente los autores explican el concepto de sensores de redes inalámbricas, los cuales son conocidos como WSN de su acrónimo en inglés. También explica los usos comunes que se le dan a ese tipo de dispositivo, como lo pueden ser aplicaciones de localización. Además, explican un poco de técnicas de análisis de la potencia de señales inalámbricas y sus

indicadores, los cuales son conocidos como RSSI dentro de la perspectiva de sensores de redes inalámbricas. En el detalle de la investigación se hace una propuesta de cómo crear WSN utilizando una Raspberry PI aplicando métodos que permitan establecer métricas RSSI. Entre las características que resaltan del dispositivo, es la capacidad de procesamiento que al mismo tiempo posee un tamaño aceptable para ser considerado como un sensor, adicionalmente que es una plataforma perfecta debido a que es capaz de interactuar con una amplia variedad de dispositivos periféricos.

Por último, hace un análisis de algunas herramientas que han sido liberadas para la plataforma Raspberry con el propósito de realizar análisis de potencias e indicadores de señal inalámbricas, donde se hace una breve comparación de los principales elementos que los conforman y sus desempeños con base a los sensores de redes inalámbricas que se tenían disponibles en el mercado al momento del estudio.

Fuente: elaboración propia.

3.5 Análisis de resultados

Una vez obtenidas las fuentes del repositorio de datos, se realiza un análisis más profundo para obtener información relevante que pueda ser utiliza en el marco teórico y análisis de resultados de la investigación.

3.5.1 Fuentes analizadas

Después de aplicar las consultas de búsquedas en la base de datos se obtuvo 116 resultados para el repositorio DBLP, de los cuales 5 fueron seleccionados después de aplicar los criterios de inclusión y exclusión definidos en secciones anteriores.

De las fuentes incluidas tenemos 4 que están asociadas al área de puntos de acceso no autorizados, 4 detección de intrusos inalámbricos y 1 asociada a sensores inalámbricos y Raspberry PI.

Capítulo 4. Marco metodológico

4.1 Tipo de Investigación

El tipo de investigación puede ser considerada como evaluativa, en la cual se busca medir el resultado de un programa que está siendo aplicado dentro de un contexto determinado. Para esto se analiza los efectos del programa con respecto a las metas que se planteó lograr en los objetivos específicos de la investigación. Por otra parte, una vez finalizada la evaluación se pueden tomar nuevas decisiones que permitan mejorar ejecuciones futuras (Tecnología Educativa Unefa, 2012).

Además, en la investigación se utiliza conocimiento generado en investigaciones similares relacionadas con seguridad de la información, redes inalámbricas y tecnologías de código abierto, con las cuales se trata de crear una solución que permita solventar la pregunta de investigación, para finalmente valorar la eficacia del sistema de monitoreo de puntos de acceso inalámbricos no autorizados en un ambiente de pruebas controlado.

4.2 Enfoque

La investigación se desarrolla utilizando un enfoque alternativo, el cual supone que no se puede desarrollar una investigación utilizando los enfoques cualitativos y cuantitativos de forma separada; al no existir esta separación tampoco puede existir un enfoque mixto pues no se puede mezclar algo que nunca ha estado desligado (Naranjo Zeledón, 2017).

Por esta razón se estarán utilizando técnicas e instrumentos en la investigación que se basan en principios de enfoques cualitativos y cuantitativos.

Ante el fenómeno investigativo el grupo de investigación utiliza la postura de involucrados, debido a que se requiere realizar pruebas de campo y laboratorios donde se puede verificar el correcto funcionamiento de la solución propuesta, al

mismo tiempo que se recolectan y analizan datos que serán utilizados en etapas posteriores de la investigación.

4.3 Diseño

Este apartado permite definir la estrategia del grupo de investigación para responder al problema o pregunta de investigación planteado. Para el caso particular de esta investigación se estarán utilizando dos tipos de diseños:

- **Diseño documental:** Este tipo de diseño se basa en la obtención y análisis de datos provenientes de materiales impresos u otros tipos de documentos. Será utilizado para lograr objetivos asociados con la identificación de los elementos que conforman un sistema de monitoreo de puntos de acceso inalámbricos no autorizados, identificar las tecnologías de código abierto que pueden ser utilizadas, definición de requerimientos funcionales y no funcionales, especificación de los casos de uso del sistema y definir la arquitectura del sistema (Tecnología Educativa Unefa, 2012).
- **Diseño de laboratorio:** Es utilizado para recolectar información en ambientes artificiales o creados. En la investigación será utilizado para obtener los resultados de los objetivos asociados al desarrollo del software que conforma el sistema y la ejecución de las pruebas para verificar el correcto funcionamiento (Tecnología Educativa Unefa, 2012).

4.4 Población y muestreo

Debido a que la cantidad de escenarios de conectividad a los que se puede enfrentar la solución son muy variados y difíciles de determinar, se opta por utilizar una población de tipo casual o accidental, donde la muestra es seleccionada por el grupo de investigación con base en sus características y no al porcentaje de población que representan. Además, de poder determinar todos los posibles

elementos que conforman la muestra, por cuestiones de tiempo y presupuesto sería imposible analizarlos (Naranjo Zeledon , 2017).

Los resultados serán evaluados con una muestra de toda la población, la cual estará conformada por un equipo de gestión centralizado, un sensor de señal inalámbrica, un punto de acceso miembro, un punto de acceso vecino y un punto de acceso sospecho o no autorizado.

4.5 Técnicas y herramientas de recolección de datos

4.5.1 Técnicas de recolección de datos

El análisis de documentación y la observación directa serán utilizados como técnicas de recolección de datos, la primera tendrá mayor protagonismo en las etapas de análisis de resultados donde se busca alcanzar los objetivos planteados y que se encuentran asociados al diseño documental, mientras que la segunda será de mayor uso en la recolección de datos con los que se busca alcanzar objetivos asociados al diseño experimental.

A continuación, se describe cómo será utilizada cada una de las técnicas de recolección de datos mencionadas anteriormente:

- **Análisis de documentación:** A partir de fuentes de información obtenidas y descritas en el marco metodológico, estado de la cuestión y estudio de las principales características de las soluciones existentes en el mercado, se realiza una comparación y evaluación de las mismas para cumplir con los objetivos propuestos. A partir de este análisis se generan tablas, diagramas, listas de cotejo y rúbricas con los aspectos más importantes por considerar.
- **Observación:** Se diseña y configura un ambiente de pruebas controlado en el cual se puedan aplicar escenarios de observación del comportamiento de la solución de monitoreo desarrollada. El grupo de investigación evalúa si el

funcionamiento es correcto observando y documentando en tablas resumen cómo se comporta ante diferentes estímulos y cambios que se presentan en el entorno de operación del objeto de estudio.

4.5.2 Herramientas de recolección de datos.

Se describe las diferentes herramientas de recolección de datos que serán utilizadas en conjunto con las técnicas establecidas en la metodología de investigación.

4.5.2.1 Tablas resumen

Es una herramienta de autoría propia, en la cual se pretende realizar análisis de las fuentes bibliográficas de la investigación y generar cuadros o tablas de resumen de los elementos más importantes por considerar y en los cuales se puede agregar información de referencia como descripciones o funciones.

En la etapa de análisis de resultados esta herramienta será utilizada principalmente en la identificación de los elementos de hardware y software que conforman un sistema de monitoreo de puntos de acceso inalámbricos no autorizados y la definición de requerimientos funcionales y no funcionales del sistema.

4.5.2.2 Lista de cotejo

La lista de cotejo es una herramienta estructurada con la cual se puede registrar la ausencia o presencia de rasgos, conductas o acciones determinadas, además se caracteriza por ser dicotómica, por lo que solo acepta dos alternativas de respuesta, como lo puede ser sí o no, cumple o no cumple, por mencionar un ejemplo (Servicio Nacional de Capacitación y Empleo de Chile).

En la etapa de análisis de resultados esta herramienta será utilizada para definir los elementos de software y hardware que conforman un sistema de monitoreo de puntos de acceso no autorizado, así como la selección de tecnologías de código abierto que pueden ser utilizadas para crear el sistema.

4.5.2.3 Rúbricas

La rúbrica es una herramienta que permite crear una evaluación acerca del nivel o calidad de una tarea, proceso u objeto. Se caracteriza porque previo a ejecutarla se deben establecer los criterios utilizados para evaluar, así como los rangos de puntación (Servicio Nacional de Capacitación y Empleo de Chile).

Esta herramienta será utilizada en la etapa de análisis de resultados para seleccionar las tecnologías de código abiertas existentes que pueden ser utilizadas para desarrollar el sistema de monitoreo.

Se describe detalladamente los criterios de evaluación para cada uno de los elementos que deberían conformar un sistema de monitoreo de puntos de acceso inalámbrico no autorizados, los cuales fueron establecidos por el grupo de investigación con base en su experiencia y criterio profesional.

4.5.2.3.1 Rúbrica de evaluación para lenguajes de programación.

En la tabla 13 se muestra los rubros que serán evaluados para seleccionar los lenguajes de programación utilizados en la solución:

Tabla 13: Rubrica de evaluación para los lenguajes de programación.

Criterio de evaluación	Valor	Opciones
1. Multiplataforma.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
2. Soporte para hardware con 512MB o 1GB de memoria RAM.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.

3. Soporte para Raspbian SO.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
4. Soporte para Web Sockets	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
5. Capacidad de invocar comandos del SO.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
6. Soporte para Web Services.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
7. Soporte GUI Web	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
8. Código abierto	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
9. Soporte para realizar conexiones a bases de datos relacionales.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.

Fuente: Elaboración propia.

- **Aspectos importantes:** Para que un lenguaje de programación sea considerado viable de utilizar debe obtener al menos 6 puntos en la rúbrica de evaluación, se excluye los que no cumplan con los puntos 2, 3 y 8.

4.5.2.3.2 Rúbrica de evaluación para hardware de tarjetas inalámbricas.

En la tabla 14 se muestran la rúbrica utilizada para seleccionar el hardware de tarjeta inalámbrica idónea para implementar la solución:

Tabla 14: Rubrica de evaluación para seleccionar modelo tarjeta inalámbrica.

Criterio de evaluación	Valor	Opciones
1. Interfaz de conexión USB.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
2. Soporte para frecuencias de operación 5Mhz	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
3. Soporte para frecuencias de operación 2.4Mhz	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.

4. Soporte para trabajar en modo monitor.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
5. Soporte y driver para distribuciones de SO GNU/Linux.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.

Fuente: Elaboración propia.

- **Aspectos importantes:** Para que una tarjeta de red inalámbrica sea considerada viable de utilizar debe obtener al menos 4 puntos en la rúbrica de evaluación, se excluyen las opciones que no cumplan con los puntos 1, 4 y 5.

4.5.2.3.3 Rúbrica de evaluación para repositorios de datos

En la tabla 15 se muestran los rubros utilizados para seleccionar el repositorio de datos por utilizar en la solución.

Tabla 15: Rubro de evaluación para seleccionar motor de base de datos.

Criterio de evaluación	Valor	Opciones
1. Posee estructura de datos relacionales.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
2. Tecnología de código abierto.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
3. Soporte para almacenar datos en formato JSON y XML,	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
4. Soporte para múltiples plataformas de sistemas operativos.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.

Fuente: Elaboración propia.

- **Aspectos importantes:** Serán viables todas las tecnologías de repositorio de datos que tengan una calificación de 4 puntos con base en la rúbrica descrita en la tabla 15, lo cual significa que debe cumplir con todos los criterios de evaluación.

4.5.2.3.4 Rúbrica de evaluación para herramientas de escaneo de señales inalámbricas

En la tabla 16 se muestran la rúbrica utilizada para seleccionar las herramientas de escaneo de señales inalámbricas idóneas para implementar la solución.

Tabla 16: Rubro de evaluación para seleccionar herramienta de análisis de señal inalámbricas.

Rubro	Valor	Opciones
1. BSSID del AP	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
2. BSSID clientes.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
3. SSID	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
4. Intensidad de la señal	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
5. Nivel de ruido	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
6. Frecuencia de operación	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
7. Canal	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.
8. Fabricante.	1 punto.	Cumple = 1 punto. No cumple = 0 puntos.

Fuente: Elaboración propia.

- **Aspectos importantes:** Serán seleccionadas las herramientas que sean capaz de analizar o capturar todos los parámetros de configuración mencionados en la rúbrica de la tabla 16, no obstante, en caso de no encontrar una herramienta que obtenga la calificación perfecta, se optaría por utilizar varias herramientas de forma combinada.

4.5.2.4 Diagramas

Los diagramas son una herramienta que permite organizar y comprender ideas de manera significativa y es un proceso activo de aprendizaje donde se debe prestar atención a la relación entre los conceptos (Naranjo Zeledon , 2017).

Esta herramienta será utilizada especialmente en la etapa de análisis de resultados, especificación de los casos de uso de los requerimientos y el diseño de la arquitectura del sistema.

4.5.2.5 Casos de uso

Es una técnica en el proceso de vida del desarrollo de software con la cual se puede especificar el comportamiento de un sistema con base en una función o tarea que debe realizar. También permite determinar otros aspectos importantes, como datos de entrada, datos de salida, actores y pre-requisitos (Ceria, 2001).

Durante el análisis de resultados serán utilizados en la etapa de especificación y desarrollo de las funcionalidades que conforman la solución, pues permitirá establecer de forma clara y precisa cuál es el comportamiento que debe tener el sistema ante cada requerimiento establecido.

4.6 Estrategia de desarrollo de la propuesta

La estrategia para desarrollar la propuesta es ir elaborando el análisis de resultados por cada uno de los objetivos planteados en la sección introductoria de la investigación, se aplicará cada una de las técnicas de análisis y recolección de datos según corresponda con el objetivo que se busque desarrollar.

Capítulo 5. Análisis de resultados

5.1 Elementos de hardware y software que conforman un sistema de monitoreo de puntos de acceso inalámbricos no autorizados

Debido a que el enfoque de la investigación es crear una solución de monitoreo utilizando sensores inalámbricos, en la sección 2.4 del marco metodológico se describen las 3 funciones principales de este tipo de solución, las cuales son descritas por (Sachin R. , Sandeep P. , & Ajeet A. , 2013):

- Recolección de datos de las señales inalámbricas.
- Normalización de la información recolectada en un formato estandarizado.
- Clasificación y análisis de los datos recolectados.

En la tabla 17 se procede a crear una lista de cotejo de los elementos y funcionalidades principales que conforman las diferentes soluciones de monitoreo que existen en el mercado, y los cuales serán tomados como punto de referencia para determinar las características que debería tener la solución de monitoreo:

Tabla 17: Lista de cotejo que permite identificar los elementos en común que comparten las diferentes soluciones de monitoreo que existen en el mercado

Elemento	Cisco wIPS	HP Mobility Security IDS/IPS	AirMagnet Enterprise
Punto de acceso con seguridad	Sí	No	No
Sensor inalámbrico	Sí	Sí	Sí
Hardware especializado con funciones centralizadas de control.	Sí	Sí	Sí
Software especializado con funciones centralizadas de control.	Sí	Sí	Sí
Algoritmo especializado de procesamiento de información de los AP	Sí	Sí	Sí

Módulo de alertas y notificaciones	Sí	Sí	Sí
Escaneo de señales en frecuencias 2.4Ghz	Sí	Sí	Sí
Escaneo de señales en frecuencias 5.8Ghz	Sí	Sí	Sí
Contención de eventos	Sí	Sí	No
Análisis forense	No	Si	No
Reportes	Requiere modulo adicional	Si	Si
Motor de servicio móvil	Si	No	No

Fuente: Elaboración propia.

Una vez analizado la lista de cotejo y con base en el conocimiento y experiencia del grupo de investigación en el tema, se define la siguiente tabla resumen de los principales elementos de software y hardware que deberían conformar la solución, así como sus principales funciones y características:

Tabla 18: Cuadro de elementos que conforman un sistema de monitoreo de puntos de acceso inalámbricos no autorizados.

Elemento	Tipo	Descripción
Sensor inalámbrico	Hardware	Elemento de hardware que se instala en los diferentes puntos del espacio físico que se desea monitorear. Se caracteriza por poseer las características físicas necesarias para poder recolectar la información de las señales inalámbricas que tiene a su alcance. Debido que parte del objetivo de la investigación es utilizar una Raspberry PI, este elemento de hardware realizará la función del sensor dentro del sistema de monitoreo y el grupo de investigación decide llamarlo WS-RPI (Wireless sensor Raspberry PI).

Tarjeta inalámbrica	Hardware	Es el dispositivo de hardware que conforma parte fundamental del sensor inalámbrico. Si bien es cierto todas las soluciones analizadas traen la tarjeta inalámbrica integrada en el sensor inalámbrico, en la solución se optó por utilizar una tarjeta inalámbrica auxiliar con la Raspberry PI, con la intención de suplir la necesidad de tener una tarjeta dedicada a escaneo y una encargada de brindar conectividad hacia el resto de los equipos, Adicionalmente con la tarjeta auxiliar se podría dar soporte de hardware para escanear señales que operan tanto en la frecuencia 2.4GHz y 5.8GHz.
Sistema operativo sensor	Software	Sistema operativo capaz de ejecutarse en el hardware seleccionado para ser utilizado con el sensor inalámbrico, el cual debe ser capaz de reconocer las tarjetas inalámbricas conectadas al dispositivo (soporte para los drivers), ejecutar elementos de software que puedan obtener información de las señales inalámbricas detectadas por las tarjetas, estandarizar los datos recolectados y enviar la información al controlador complementándose con el módulo de comunicación. Para efectos de la investigación se tratará de ajustar el Rasbian OS (sistema operativo que posee la Raspberry por defecto) para que cumpla con los requerimientos del sistema de monitoreo.
Controlador HW	Hardware	Elemento de hardware que se encuentra presente en todas las arquitecturas estudiadas. En todas las soluciones analizadas, es un equipo con hardware y software especializado, no obstante, para efectos de la investigación se opta por utilizar un CPU de arquitectura x86 el cual es capaz de ejecutar un

		sistema operativo de uso común como Windows o Linux y donde se puede ejecutar los códigos fuentes desarrollados para crear los elementos de software que requiera el controlador.
Controlador SF		Elemento que está presente en todas las arquitecturas estudiadas y el cual se encarga de recibir los datos de las señales capturadas por los sensores inalámbricos, con base a esto realiza diferentes funciones como gestión de otros equipos, manejo de inventario de señales, ejecución de algoritmos de análisis y emisión de alertas y notificaciones. Este elemento de software debe ser capaz de procesar los datos según los requerimientos establecidos para el sistema de monitoreo y para razones de la investigación el grupo de trabajo decidió llamarlo DAC-S (data analysis and controller software).
Módulo de comunicación y notificaciones.	Software	Este es un elemento de software que debe estar presente tanto en los sensores como en el controlador, el cual permita compartir información entre ambos dispositivos de forma bidireccional. Con base en lo analizado en los apartados del marco teórico se ha demostrado que estructuras de datos en formatos JSON y XML tienen buen rendimiento para este tipo de comunicación. Por otra parte, también debe brindar soporte para los elementos de notificaciones del sistema, por lo que debe soportar protocolos de comunicación como SMTP.
Módulo de almacenamiento	Software	Si bien es cierto este elemento no está explícito en las soluciones estudiadas, se deduce que existe y no se muestra porque es un componente integrado

	con los equipos especializados que ofrecen los diferentes fabricantes para cumplir la función del controlador. Para efectos de la investigación se busca que sea un motor de base de datos capaz de almacenar de forma local los parámetros de configuración necesarios para el correcto funcionamiento del controlador.

Fuente: Elaboración propia.

5.2 Tecnologías de código abierto existentes que pueden ser utilizadas en el sistema de monitoreo de puntos de acceso inalámbricos no autorizados.

Una vez definidos los principales elementos que deberían conformar la solución, se procede a analizar las tecnologías de código abierto existentes que pueden ser utilizadas en el sistema de monitoreo, y que deberían ser la basa fundamental para realizar la función o crear los elementos definidos en la sección 5.1 de la investigación.

A continuación, se detalla el resultado del análisis obtenido de aplicar las rúbricas de evaluación definidas para cada una de las tecnologías de código abierto definidas por el grupo de investigación, mismas que fueron seleccionadas con base en el conocimiento y experiencia profesional.

5.2.1 Lenguaje de programación

Se muestra el detalle de aplicar la rúbrica de evaluación a los lenguajes de programación Python, Java Enterprise Edition y Node JS, según corresponde en las tablas 19, 20 y 21.

Tabla 19: Análisis de los criterios de evaluación para el lenguaje de programación Python.

Cuadro evaluativo lenguaje de programación		
Lenguaje	**Python**	
Factor de evaluación	**Cumple**	**Calificación**
Multiplataforma.	Sí	1 punto.
Soporte para hardware con 512MB o 1GB de memoria.	Sí	1 punto.
Soporte para Raspbian SO.	Sí	1 punto.
Soporte para Web Sockets.	Sí	1 punto.
Capacidad de invocar comandos del sistema operativo.	Sí	1 punto.
Soporte para Web Services.	Sí	1 punto.
Soporte GUI Web.	Sí	1 punto.
Código abierto.	Sí	1 punto.
Soporte para realizar conexiones a bases de datos relacionales.	Sí	1 punto.
Puntaje total obtenido	**9 puntos.**	
Solución es viable	**Sí(X)** No( )	

- Observaciones: Lenguaje de programación con gran capacidad de adaptación que se puede instalar en Rasbian OS desde el repositorio oficial de software, se caracteriza porque utiliza pocos recursos de hardware y puede ser utilizado para crear aplicaciones GUI y comunicarse de forma directa con el Hardware (Python Software Foundation, s.f.).

Fuente: Elaboración propia.

Tabla 20: Análisis de los criterios de evaluación para el lenguaje de programación Java EE.

Cuadro evaluativo lenguaje de programación		
Lenguaje	**Java Enterprice Edition**	
Factor de evaluación	**Cumple**	**Calificación**
Multiplataforma.	Sí	1 punto.
Soporte para hardware con 512MB o 1GB de memoria.	Sí	1 punto.
Soporte para Raspbian SO.	Sí	1 punto.

Soporte para Web Sockets.	Sí	1 punto.
Capacidad de invocar comandos del sistema operativo.	Sí	1 punto.
Soporte para Web Services.	Sí	1 punto.
Soporte GUI Web.	Sí	1 punto.
Código abierto.	Sí	1 punto.
Soporte para realizar conexiones a bases de datos relacionales.	Sí	1 punto.
Puntaje total obtenido	**9 puntos.**	
Solución es viable	**Sí(X)** No( )	

- **Observaciones:** Lenguaje de programación multiplataforma, debido a que requiere una máquina virtual con la cual se ejecuta el código fuente compilado requiere mayor cantidad de recursos de hardware, para el caso de Rasbian OS se requiere realizar configuraciones complejas en el sistema operativo, y la máquina virtual que se debe utilizar es SE Embedded. Puede realizar llamados al sistema operativo, no obstante, no es tan nativo como el caso de Python (Oracle, s.f.).

Fuente: elaboración propia.

Tabla 21: Análisis de los criterios de evaluación para el lenguaje de programación Node JS.

Cuadro evaluativo lenguaje de programación		
Lenguaje		**Node JS**
Factor de evaluación	**Cumple**	**Calificación**
Multiplataforma.	Sí	1 punto
Soporte para hardware con 512MB o 1GB de memoria.	Sí	1 punto
Soporte para Raspbian SO.	Sí	1 punto
Soporte para Web Sockets	Sí	1 punto
Capacidad de invocar comandos del sistema operativo.	Sí	1 punto
Soporte para Web Services.	Sí	1 punto
Soporte GUI Web.	Sí	1 punto
Código abierto.	Sí	1 punto
Soporte para realizar conexiones a bases de datos	Sí	1 punto

relacionales.

Puntaje total obtenido	**9 puntos.**
Solución es viable	**Sí(X)** No( )

- **Observaciones:** Lenguaje de programación con entorno de ejecución de JavaScript orientado a eventos asíncronos, es multiplataforma y se caracteriza por consumir muy pocos recursos de hardware, los cuales inclusive son parametrizables. Por defecto se encuentra incluido en Rasbian OS, se caracteriza porque puede ser utilizado para crear aplicaciones GUI como llamados de bajo nivel (ejecutar comandos del sistema operativo (Node JS Foundation, s.f.).

Fuente: elaboración propia.

5.2.2 Hardware tarjetas inalámbricas

Según el sitio especializado en asuntos de tecnología (Wonder How To, s.f.), se seleccionan 3 de los modelos de tarjetas inalámbricas disponibles en el mercado, que cumplen con las características de hardware necesarias para obtener un buen rendimiento en funciones de análisis de señales inalámbricas, donde los modelos escogidos son los siguientes: Panda PAU05, TP-LINK WN722N y Alfa AWUS036ACH.

Se procede aplicar las rubricas de evaluación definidas para el hardware de tarjetas inalámbricas a cada una de las opciones seleccionadas, como se muestra en las tablas 22, 23 y 24.

Tabla 22: Rúbrica de evaluación para el modelo de tarjeta inalámbrica Panda PAU05.

Cuadro evaluativo hardware de tarjetas inalámbricas		
Modelo	Panda PAU05	
Criterio de evaluación	**Cumple**	**Calificación**
Interfaz de conexión USB.	Sí	1 punto.
Soporte para frecuencias de operación 5Mhz	No	0 puntos.
Soporte para frecuencias de operación 2.4Mhz	Sí	1 punto.

Soporte para trabajar en modo monitor.	Sí	1 punto.
Soporte y driver para distribuciones de SO GNU/Linux.	Sí	1 punto.
Puntaje total obtenido	**4 puntos.**	
Solución es viable	Sí( ) No**(X)**	

- **Observaciones:** Tarjeta inalámbrica con capacidad de trabajar en modo monitor y realizar escaneo de frecuencias que operan bajo el protocolo 802.11b/g. Posee la ventaja ser muy compacta por lo que puede pasar desapercibida. Entre las desventajas que presenta es que no tiene soporte para realizar inyección de paquetes y no puede escanear señales inalámbricas que operan en la frecuencia 5.8Ghz, debido a esta última limitante deja de ser viable según se definió en la metodología (Wonder How To, s.f.).

Fuente: Elaboración propia.

Tabla 23: Rúbrica de evaluación para el modelo de tarjeta inalámbrica TP-LINK WN722N.

Cuadro evaluativo hardware de tarjetas inalámbricas		
Modelo	TP-LINK WN722N	
Criterio de evaluación	**Cumple**	**Calificación**
Interfaz de conexión USB.	Sí	1 punto.
Soporte para frecuencias de operación 5Mhz	No	0 puntos.
Soporte para frecuencias de operación 2.4Mhz	Sí	1 punto.
Soporte para trabajar en modo monitor.	Sí	1 punto.
Soporte y driver para distribuciones de SO GNU/Linux.	Sí	1 punto.
Puntaje total obtenido	**4 puntos.**	
Solución es viable	Sí( ) No**(X)**	

- **Observaciones:** Tarjeta inalámbrica con capacidad de trabajar en modo monitor y realizar escaneo de frecuencias que operan bajo el protocolo 802.11b/g/n. Entre las ventajas que presenta es que el costo es inferior a la mayoría de las soluciones y por tener antena externa tiene mayor alcance. Como desventaja

presenta que es poco compacta y carece de soporte para escanear señales inalámbricas que operan en la frecuencia 5.8Ghz, razón por la cual deja de ser viable según se estableció en la metodología (Wonder How To, s.f.).

Fuente: Elaboración propia.

Tabla 24: Rúbrica de evaluación para el modelo de tarjeta inalámbrica Alfa AWUS036ACH.

Cuadro evaluativo hardware de tarjetas inalámbricas		
Modelo	Alfa AWUS036ACH	
Criterio de evaluación	**Cumple**	**Calificación**
Interfaz de conexión USB.	Sí	1 punto.
Soporte para frecuencias de operación 5Mhz	Sí	1 punto.
Soporte para frecuencias de operación 2.4Mhz	Sí	1 punto.
Soporte para trabajar en modo monitor.	Sí	1 punto.
Soporte y driver para distribuciones de SO GNU/Linux.	Sí	1 punto.
Puntaje total obtenido	**5 puntos**	
Solución es viable	**Sí(X)** No( )	

- **Observaciones:** Tarjeta inalámbrica con capacidad de trabajar en modo monitor y realizar escaneo de frecuencias que operan bajo el protocolo 802.11a/b/g/n. Entre las ventajas que presenta es que tiene dos antenas externas que le permiten tener mayor alcance. Como desventaja es que es poco compacta. Debido a que tiene capacidad de analizar señales inalámbricas que operan tanto en la frecuencia de 2.4Ghz y 5.8Ghz se considerada como viable, según se estableció en la metodología (Wonder How To, s.f.).

Fuente: Elaboración propia.

5.2.3 Repositorio de datos

Se muestra el detalle de aplicar la rúbrica de evaluación a las bases de datos MySql, Mongo y Postgresql, según corresponde en las tablas 25, 26 y 27.

Tabla 25: Rúbrica de evaluación para el repositorio de datos MySql Database.

Cuadro evaluativo repositorio de datos		
Repositorio	MySql Database	
Criterio de evaluación	**Cumple**	**Calificación**
Posee estructura de datos relacionales.	Sí	1 punto.
Tecnología de código abierto.	Sí	1 punto.
Soporte para almacenar datos en formato JSON y XML.	Sí	1 punto.
Soporte para múltiples plataformas de sistemas operativos.	Sí	1 punto.
Puntaje total obtenido	**4 puntos**	
Solución es viable	**Sí(X)** No( )	

- **Observaciones:** Base de datos relacional de libre uso y de mayor popularidad en el mercado, se caracteriza porque ha sido utilizada para desarrollar aplicaciones Web. Posee múltiples adaptadores que le permite integrarse con lenguajes de programación como Java, Python, PHP, Perl y Node Js. Además, tiene capacidad para ser instalada en diferentes instancias de sistemas operativos como Windows, Linux y Mac OS. Entre las desventajas que presenta es que fue adquirida por Oracle, por lo que la participación de la comunidad ha disminuido considerablemente (Oracle Corporation, s.f.).

Fuente: Elaboración propia.

Tabla 26: Rúbrica de evaluación para el repositorio de datos Mongo DB.

Cuadro evaluativo repositorio de datos		
Repositorio	Mongo DB	
Criterio de evaluación	**Cumple**	**Calificación**
Posee estructura de datos relacionales.	No	0 puntos.
Tecnología de código abierto.	Sí	1 punto.
Soporte para almacenar datos en formato JSON y XML.	Sí	1 punto.
Soporte para múltiples plataformas de sistemas	Sí	1 punto.

operativos.

Puntaje total obtenido	**3 puntos**
Solución es viable	Sí( ) No(X)

- **Observaciones:** Base de datos no SQL orientada al uso de documentos, por esta razón la información no se almacena en tablas sino en estructura de documentos tipo JSON. Se caracteriza porque es de código abierto y posee soporte para múltiples plataformas de sistemas operativos, como Linux, Windows, Mac Os y Solaris. Debido a que no posee estructuras de datos relacionales se considera no viable según se estableció en la metodología (Mongo DB, s.f.).

Fuente: Elaboración propia.

Tabla 27: Rúbrica de evaluación para el repositorio de datos Postgresql.

Cuadro evaluativo repositorio de datos		
Repositorio	Postgresql	
Criterio de evaluación	**Cumple**	**Calificación**
Posee estructura de datos relacionales.	Sí	1 punto.
Tecnología de código abierto.	Sí	1 punto.
Soporte para almacenar datos en formato JSON y XML.	Sí	1 punto.
Soporte para múltiples plataformas de sistemas operativos.	Sí	1 punto.
Puntaje total obtenido	**4 puntos**	
Solución es viable	**Sí(X)** No( )	

- **Observaciones**: Base de datos no relacional y orientada a objetos, se caracteriza porque no es manejada por una empresa, sino, por una comunidad de miembros que realizan mejoras de forma gratuita. Posee soporte para distintos lenguajes de programación, como C, C++, Python, Perl, Java, PHP y Rubi. Además, tiene capacidad de ser instalado en instancias de sistemas operativos como Windows, Linux y Mac OS (PostgreSQL Global Development Group, s.f.).

Fuente: Elaboración propia.

5.2.4 Herramienta de escaneo de señales inalámbricas

Se detalla el resultado de aplicar las rúbricas de evaluación a las herramientas de escaneo de señales inalámbricas Linux Wireless Tools, Aircrack-ng y iwspy, las cuales han sido destacadas por (Offensive Security, s.f.).

A continuación, se muestra en las tablas 28, 29 y 30 los resultados de la rúbrica para cada una de las herramientas seleccionadas:

Tabla 28: Rúbrica de evaluación para la herramienta de escaneo de señales inalámbricas Linux Wireless Tool.

Cuadro evaluativo herramienta escaneo señales inalámbricas		
Herramienta	Linux Wireless Tools	
Criterio de evaluación	**Cumple**	**Calificación**
BSSID del AP.	Sí	1 punto.
BSSID clientes.	No	0 puntos.
SSID.	Sí	1 punto.
Intensidad de la señal.	Sí	1 punto.
Nivel de ruido.	Sí	1 punto.
Frecuencia de operación.	Sí	1 punto.
Canal.	Sí	1 punto.
Fabricante.	No	0 puntos.
Puntaje total obtenido	**6 puntos**	
Solución es viable	**Sí(X)** No( )	

- **Observaciones:** Herramienta que generalmente se encuentra instalada de forma nativa en los sistemas operativos Linux, posee un set de comandos con los cuales se puede opera las tarjetas inalámbricas en diferentes modos, lo que permite que puedan operar como cliente, master o monitor siempre y cuando el hardware lo soporte. Como limitante tiene que en las funciones de escaneo no permite obtener información de los clientes que se encuentran conectados al punto de acceso que se está escaneando (Tourrilhes, 2008).

Fuente: Elaboración propia.

Tabla 29: Rúbrica de evaluación para la herramienta de escaneo de señales inalámbricas Aircrack-ng.

Cuadro evaluativo herramienta escaneo señales inalámbricas		
Herramienta	Aircrack-ng	
Criterio de evaluación	**Cumple**	**Calificación**
BSSID del AP.	Sí	1 punto.
BSSID clientes.	No	0 puntos.
SSID.	Sí	1 punto.
Intensidad de la señal.	Sí	1 punto.
Nivel de ruido.	No	0 puntos.
Frecuencia de operación.	Sí	1 punto.
Canal.	Sí	1 punto.
Fabricante.	Sí	1 punto.
Intensidad de la señal.	Sí	1 punto.
Puntaje total obtenido	**7 puntos**	
Solución es viable	**Sí(X)** No( )	

- **Observaciones :** Es una herramienta con la que se puede evaluar el nivel de seguridad de las redes inalámbricas, entre las principales funciones que posee es monitoreo y captura de paquetes, los cuales pueden ser exportados en archivos de texto para que sean analizados posteriormente por herramientas de terceros, ataques, verificación de capacidad de controladores y tarjetas inalámbricas y rompimiento de protocolos de seguridad como WEP, WPA1 y WPA2 (Aircrack-ng, s.f.).

Fuente: Elaboración propia.

Tabla 30: Rúbrica de evaluación para la herramienta de escaneo de señales inalámbricas iwlist.

Cuadro evaluativo herramienta escaneo señales inalámbricas		
Herramienta	iwlist	
Criterio de evaluación	**Cumple**	**Calificación**
BSSID del AP	Sí	1 punto.
BSSID clientes.	No	0 puntos.
SSID	Sí	1 punto.
Intensidad de la señal	Sí	1 punto.

Nivel de ruido	Sí	1 punto.
Frecuencia de operación	Sí	1 punto.
Canal	Sí	1 punto.
Fabricante.	No	0 puntos.
Intensidad de la señal	Sí	1 punto.
Puntaje total obtenido	**7 puntos**	
Solución es viable	**Sí(X)** No( )	

- **Observaciones:** Herramienta de línea de comando que conforma parte de los complementos del Kernel de Linux, con la cual se puede escanear la información de los puntos de acceso disponibles y que sirve como referencia para generar los archivos de configuración de entornos no gráficos que se deben conectar a redes inalámbricas. La información que se puede obtener con esta herramienta depende del soporte que brinde la tarjeta inalámbrica con la que se realiza el escaneo (The official Linux Wireless wiki, s.f.).

Fuente: Elaboración propia.

5.3 Requerimientos funcionales y no funcionales del sistema de monitoreo de puntos de acceso no autorizados

Con base en las especificaciones de las soluciones analizadas en el capítulo del marco teórico y las funcionalidades que debe realizar un sistema de monitoreo de puntos de acceso inalámbricos no autorizados, se define la siguiente tabla resumen con el listado de requerimientos funcionales y no funcionales que debe cumplir cada uno de los elementos que conforma el sistema, como se muestra en las tablas 31, 32 y 33.

Tabla 31: Detalle de los requerimientos funcionales con los que debe cumplir el dispositivo WS-RPI.

Componente	Requerimiento	Caso de uso	Descripción
Dispositivo WS-RPI	Gestionar WS-RPI.	Configurar WS-RPI.	Módulo grafico que permite al usuario configurar los parámetros de red como dirección IP, máscara de red, puerta de enlace predeterminada, dirección de red del DAC-S, usuario, contraseña, entre otros.
		Iniciar configuración.	Funcionalidad que permite que el dispositivo recupere la última configuración guardada en caso de que el hardware se reinicie o apague.
		Configuración de fábrica.	Funcionalidad que permite configurar el dispositivo con los parámetros de fábrica mediante una señal de hardware.
	Escaneo.	Tomar inventario.	Funcionalidad que se activa mediante una señal del DAC-S y que permite realizar una captura de los parámetros de las señales inalámbricas por un periodo determinado, posteriormente los datos serán enviados al DAC-S.
		Obtener estatus.	Funcionalidad que se activa mediante una señal del DAC-S y que permite obtener el estado de las señales inalámbricas y sus parámetros, así como el estado general del dispositivo.

Fuente: Elaboración propia.

Tabla 32: Detalle de los requerimientos funcionales con los que debe cumplir el módulo de comunicación.

Componente	Requerimiento	Caso de uso	Descripción
Módulo de comunicación.	Transferencia de datos.	Envió de comandos.	Funcionalidad que permite establecer comunicación entre el DAC-S y los dispositivos WS-RPI, mediante el cual se pueden enviar comandos para obtener información de configuración, recepción de inventario, estatus del dispositivo entre otros.
		Envió de notificaciones	Funcionalidad mediante la cual el DAC-S se conecta a un servidor de correos y envía notificaciones a los usuarios correspondientes.

Fuente: Elaboración propia.

Tabla 33: Detalle de los requerimientos funcionales con los que debe cumplir el DAC-S.

Componente	Requerimiento	Caso de uso	Descripción
DAC-S	Gestión de la aplicación.	Configurar sistema de gestión.	Funcionalidad gráfica que permite configurar parámetros de sistema de gestión como usuario, contraseña, puerto de administración, puertos de comunicación, parámetros de red, servidores de notificaciones, certificados de seguridad, entre otros.
		Configurar WS-RPI	Funcionalidad gráfica que permite al usuario ingresar, modificar o eliminar la información del WS-RPI con el cual se pueden leer los parámetros de las señales

		inalámbricas.
Monitoreo	Obtener inventario	Funcionalidad que permite enviar un comando a un WS-RPI específico para que recolecte por un periodo las señales inalámbricas y clientes conectados que están dentro del rango de su alcance, para que posteriormente puedan ser analizados por el DAC-S.
	Obtener estatus del WS-RPI.	Funcionalidad que permite enviar un comando cada cierto periodo a un WS-RPI especifico, para obtener información del estatus del mismo y de las señales que percibe. Esta funcionalidad se debe realizar de forma automatizada o puede ser forzada por el usuario de forma manual desde la GUI del DAC-S.
	Procesar estatus de señales.	Funcionalidad que permite procesar la información recolectada del estatus del WS-RPI e identificar si alguna de las señales detectadas es un punto de acceso no autorizado. Lo lógica de esta funcionalidad se basa en el diagrama de flujo establecido en la figura 6 del capítulo del marco teórico.
	Graficar dispositivos en plano.	Funcionalidad gráfica que permite desplegar en una pantalla el plano de la infraestructura física donde se instaló el sistema junto con el

	estatus y posición de los dispositivos de monitoreo.

Fuente: Elaboración propia.

Por otra parte, como requerimientos no funcionales del sistema de monitoreo se definen las siguientes necesidades:

- La estructura de datos debe ser relacional y cumplir con reglas de normalización.
- Información sensible como contraseñas se debe almacenar de forma cifrada.
- Los dispositivos WS-RPI y el DAC-S deben ser capaces de recuperar su último estado de configuración guardado en caso de que se reinicien.

5.4 Casos de uso de los requerimientos funcionales y no funcionales

La solución se encuentra segmentada en diferentes módulos y funcionalidades, se realiza una descripción de los principales actores del sistema, los cuales interactúan en los diferentes flujos de los casos de uso:

- **Administrador del DAC-S:** Usuario con privilegios para instalar y configurar los diferentes parámetros de funcionamiento del DAC-S de monitoreo, también tiene permisos para agregar nuevos WS-RPI y recolectar información del inventario.
- **Administrador WS-RPI:** Usuario con privilegios para acceder a la interface de gestión de los sensores inalámbricos, puede modificar los parámetros de configuración del dispositivo.

Ahora se procede a definir los casos de uso con los que se pretende desarrollar cada una de las funcionalidades establecidas para el sistema de monitoreo, como se muestra en las tablas 34 a la 46.

5.4.1 Caso de uso: WS-RPI- Configurar dispositivo.

Precondiciones:

- El sensor se encuentra con la configuración inicial de fábrica.

Flujo principal de eventos:

Tabla 34: Flujo principal de eventos para el caso de uso.

Paso	Actor	Detalle
1	Administrador WS-RPI.	Instala el WS-RPI en una red local en el segmento de red 192.168.1.0/24, junto con un equipo que tenga un navegador Web y que no posea la dirección de red 192.168.1.10.
2	Administrador WS-RPI	Ingresa en el navegador del equipo el siguiente enlace: https://192.168.1.10:3000/
3	WS-RPI	Despliega pantalla donde se ingresa credenciales de acceso al dispositivo.
4	Administrador WS-RPI	Ingresa las siguientes credenciales de acceso: Usuario: admin Contraseña: defaultAdmin
5	WS-RPI	Muestra pantalla principal de la interfaz de gestión, en la cual se muestra información del estatus del dispositivo, como espacio en las particiones, direcciones IP, interfaces de red, información del DAC-S, nombre, tiempo encendido y botón “Configuración”.
6	Administrador WS-RPI	Oprime botón “Configuración”.
7	WS-RPI	Despliega pantalla denominada “Configuración del dispositivo”, en la cual se muestran los siguientes campos: • Usuario: Campo de texto de tamaño máximo de 20 caracteres y obligatorio • Contraseña: Campo de texto de tamaño máximo de 20 caracteres, tipo password y obligatorio • Puerto de gestión: Campo numérico donde se

		especifica el puerto de gestión por el que se debe conectar el DAC-S. • Configuración de red: ○ Sección de viñetas donde se puede ingresar la configuración de red, como dirección IP, máscara de red, puerta de enlace predeterminada, si utiliza DHCP y para el caso de la tarjeta inalámbrica los parámetros de la red inalámbrica a la que se debe conectar como el BSSID y la contraseña. • Botón “Guardar”.
8	Administrador WS-RPI	Ingresa la información de los parámetros de configuración y oprime el botón “Guardar”.
9	WS-RPI	Crea un archivo con los parámetros de configuración denominado config.ini en el directorio /Cenfotec/config/, y reinicia el dispositivo.

Fuente: Elaboración propia.

5.4.2 Caso de uso: WS-RPI- Iniciar configuración.

Precondiciones:

- La configuración del dispositivo fue creada previamente.

Flujo principal de eventos:

Tabla 35: Flujo principal de eventos para el caso de uso.

Paso	Actor	Detalle
1	WS-RPI	Inicia todos los módulos del sistema operativo hasta que ingresa en el modo de operación multi-usuario.
2	WS-RPI	Cargar el contenido del archivo /Cenfotec/config/config.ini y ejecuta los comandos necesarios para que cargue la configuración establecida en los parámetros del archivo.
3	WS-RPI	Enciende luz led de color verde como indicador que la configuración fue cargada exitosamente.

Fuente: Elaboración propia.

- **Nota:** Se recomienda que la configuración de la aplicación se inicie en el script rc.local del sistema operativo Rasbian OS, lo cual garantice que todos los módulos del sistema operativo se encuentran cargados al 100% al momento de aplicar la configuración.

5.4.3 Caso de uso: WS-RPI- Configuración de fábrica

Precondiciones:

- La configuración del dispositivo fue creada previamente.

Flujo principal de eventos:

Tabla 36: Flujo principal de eventos para el caso de uso.

Paso	Actor	Detalle
1	Administrador WS-RPI	Oprime el botón “Reset” que se encuentra ubicado en parte exterior del dispositivo por 5 segundos.
2	WS-RPI	Restablece el contenido del archivo /Cenfotec/config/config.ini y asigna los valores a los siguientes parámetros: *[admin]* *user = admin* *password = defaultAdmin* *token = 00000* *sensor_name = Sensor* *admin_port = 9001* *[controler]* *controler_ip =* *controler_port =* *config = N* *[network]* *eth0_ip = 192.168.1.10* *eth0_enable = Y* *eth0_dhcp = N* *eth0_mask = 255.255.255.0* *eth0_gw =* *wlan0_enable = N* *wlan0_dhcp = Y* *wlan0_ip =*

		wlan0_mask = *wlan0_gw =* *wlan0_wl_nm =* *wlan0_wl_pass =*
3	WS-RPI	Reinicia el sistema operativo y carga la configuración por defecto del dispositivo.

Fuente: Elaboración propia.

5.4.4 Caso de uso: WS-RPI- Tomar inventario

Precondiciones:

- El sensor fue asociado previamente con el DAC-S según el caso de uso “Agregar WS-RPI”.

Flujo principal de eventos:

Tabla 37: Flujo principal de eventos para el caso de uso.

Paso	Actor	Detalle
1	DAC-S.	Establece comunicación con el WS-RPIy envía el comando para recolección de inventario, el cual tiene la siguiente estructura: *{"CMD":"STOCK", "ID":"XXXX", "USER":"XXXXX", "PASS":"XXXXXX", "TOKEN":"XXXXXX", "TIME":"XX"}* Donde CMD es el comando de solicitud de inventario, ID el identificador de la petición de inventario, USER y PASS usuario y contraseña de acceso al WS-RPI, TOKEN es el código de seguridad que se le ingresó al WS-RPI cuando se configuró desde el DAC-S y TIME es el periodo en minutos que el WS-RPI debe recolectar información del inventario.
2	Sensor inalámbrico.	Mediante el uso de herramientas de análisis de señales inalámbricas y frameworks de seguridad de la información inicia la recolección de información de las señales que tiene a su alcance. En el directorio /Cenfotec/data/ crea un archivo denominado airdump-XXXXXx.csv con los datos de cada

		punto de acceso detectado con la siguiente estructura: *{"AP":* *{"BSSID":"XXXXX", "SSID":"XXXXX", "SL":"XXXXX", "NOISE":"XXXXX", "FREQ":"XXXX", "CHANNEL":"XXXXX", "VENDOR":"XXXX"* *"REABI":"XXX",* *"C-BSSID"["MAC":"XXXXXX", "MAC":"XXXXXX", "MACN":"XXXXXX" }]* *}*
3	WS-RPI.	Continúa recolectando la información de las señales por el periodo que se haya especificado en la solicitud de inventario del DAC-S y elimina información de registros duplicados.
4	WS-RPI.	Una vez haya terminado el periodo de recolección de información toma el contenido del archivo de datos y mediante el módulo de comunicación envía un comando al DAC-S con la siguiente estructura de datos: *{"CMD":"RESPONSE", "ID":"XXXX", "CODE":"XX", "DESCRIPTION":"XXXXX"* *"AP":{"BSSID":"XXXXX", "SSID":"XXXXX", "SL":"XXXXX", "NOISE":"XXXXX", "FREQ":"XXXX", "CHANNEL":"XXXXX", "VENDOR":"XXXX"* *"REABI":"XXX", "C-BSSID"{"MAC1":"XXXXXX", "MAC2":"XXXXXX", "MACN":"XXXXXX" }* *}* *}* Donde CMD es la instrucción que se está enviando, el ID es el identificador de la petición que generó la respuesta, CODE el código de la respuesta(0 sin error, 1 error), DESCRIPTION descripción de la causa que generó el error, AP registro por cada uno de los punto de acceso inalámbrico detectados y que en su interior está

	conformado por información de los parámetros de la señal como el BSSID, SSID, nivel de señal, ruido, frecuencia, canal y fabricante, en el campo C-BSSID se adjunta todas las direcciones MAC de los clientes que están conectados al punto de acceso.

Fuente: Elaboración propia.

5.4.5 Caso de uso: WS-RPI - Obtener estatus

Precondiciones:

- El WS-RPI fue asociado previamente al DAC-S según el caso de uso "Agregar WS-RPI".

Flujo principal de eventos:

Tabla 38: Flujo principal de eventos para el caso de uso.

Paso	Actor	Detalle
1	DAC-S	Establece comunicación con el WS-RPI y envía un comando con la siguiente estructura: *{"CMD":"STATUS", "ID":"XXXX", "USER":"XXXXX", "PASS":"XXXXX", "TOKEN":"XXXXX"}* Donde CMD es el comando con la instrucción, ID el identificador de la petición, USER y PASS las credenciales de autenticación del WS-RPI y TOKEN el identificador de seguridad.
2	WS-RPI.	Mediante el uso de herramientas de análisis de señales inalámbricas y frameworks de seguridad de la información, inicia la recolección de las señales inalámbricas que tiene a su alcance. Para esto en el directorio /Cenfotec/data/ crea un archivo denominado airdump-XXXXXx.csv con los datos de cada punto de acceso.
3	WS-RPI.	Una vez haya terminado el periodo de recolección de información toma el contenido del archivo de datos y mediante el módulo de comunicación envía un comando

	al DAC-S con la siguiente estructura de datos: *{"AP":* *{"BSSID":"XXXXX", "SSID":"XXXXX", "SL":"XXXXX", "NOISE":"XXXXX", "FREQ":"XXXX", "CHANNEL":"XXXXX", "VENDOR":"XXXX"* *"REABI":"XXX",* *"C-BSSID"["MAC":"XXXXXX", "MAC":"XXXXXX", "MACN":"XXXXXX" }]* *}* Donde CMD es la instrucción que se está enviando, ID es el identificador de la petición que generó la respuesta, CODE el código de la respuesta(0 sin error, 1 error), DESCRIPTION descripción de la causa que generó el error, AP es un registro por cada punto de acceso inalámbrico detectado que en su interior está conformado por información de los parámetros de la señal como el BSSID, SSID, nivel de señal, ruido, frecuencia, canal y fabricante, en el campo C-BSSID se adjunta las direcciones MAC de los clientes que se encuentran conectados al punto de acceso.

Fuente: Elaboración propia.

5.4.6 Caso de uso: Módulo de comunicación - Envió de notificaciones.

Precondiciones:

- El DAC-S se encuentra configurado previamente.
- El equipo donde se encuentra instalado el DAC-S tiene salida a internet.
- La red donde se encuentra instalado, el equipo DAC-S no tiene bloqueado los puertos que utiliza el protocolo SMTP.
- En el servidor de correo posee las configuraciones necesarias para poder enviar notificaciones desde un cliente remoto.
- El flujo de eventos se repite por cada persona que se debe notificar.

Flujo principal de eventos:

Tabla 39: Flujo principal de eventos para el caso de uso.

Paso	Actor	Detalle
1	DAC-S	Envía al módulo de comunicación una instrucción indicando que debe enviar una notificación, la cual posee la siguiente estructura de datos: *{"CMD":"SMTP", "ID":"XXXXX" "EMAIL":"XXXXXXX", "CONT":"XXXXX"}* Donde CMD es el comando con la instrucción, el ID es el identificador de la notificación, EMAIL correo electrónico de la persona que se debe notificar y CONT el contenido de la notificación.
2	Módulo de comunicación.	Toma la información de configuración del servidor SMTP creada en el caso de uso “Configurar sistema de gestión” y envía la notificación mediante el protocolo de comunicación SMTP.
3	Módulo de comunicación.	Devuelve al DAC-S un mensaje de confirmación indicando si la notificación se envió de forma exitosa o no.
4	DAC-S	Almacena la información de la notificación enviada en el repositorio de datos.

Fuente: Elaboración propia.

5.4.7 Caso de uso: DAC-S - Agregar WS-RPI.

Precondiciones:

- El software del DAC-S fue instalado previamente.
- La configuración inicial del DAC-S fue creada.

- El usuario denominado “Administrador del DAC-S” ha realizado inicio de sesión en la aplicación.

Flujo principal de eventos:

Tabla 40: Flujo principal de eventos para el caso de uso agregar WS-RPI.

Paso	Actor	Detalle
1	Administrador del DAC-S	Entra en el menú denominado “Agregar WS-RPI”.
2	DAC-S	Despliega una pantalla denominada “Agregar WS-RPI”, la cual despliega los siguientes campos: • Nombre: Campo de texto de tamaño máximo de 20 caracteres obligatorio. • Usuario: Campo de texto de tamaño máximo de 20 caracteres obligatorio. • Contraseña: Campo de texto de tamaño máximo de 20 caracteres obligatorio y de tipo Password. • Dirección IP: Campo de texto, obligatorio con el siguiente formato de máscara: XXX.XXX.XXX.XXX • Puerto: Campo numérico de máximo 5 dígitos obligatorio. Adicionalmente un botón denominado “Agregar”.
3	Administrador del DAC-S	Ingresa los datos correspondientes en la pantalla y oprime el botón “Agregar”.
4	DAC-S	Verifica que la información del nombre del WS-RPI y dirección IP no se encuentren repetidas (si ya existen debe desplegar un mensaje de error). Si la información no existe, la almacena en el repositorio de datos y envía un mensaje de configuración mediante el módulo de comunicación al WS-RPI, con la siguiente estructura de datos:

		{"CMD":"CONFIG", "ID":"XXXX", "IP":"XXX.XXX.XXX.XXX", "PORT":"XXXX", "USER":"XXXXX", "PASS":"XXXXX", "TOKEN":"XXXXXX", "SENSOR_NAME":"XXXXX"} Donde CMD es la instrucción que se le está enviando al WS-RPI, ID identificador de la transacción, IP y PORT es la dirección red y el puerto de gestión del DAC-S, USER y PASS usuario y contraseña con el que se puede acceder al WS-RPI, SENSOR_NAME el nombre que se le asignó al WS-RPI y TOKEN es un identificador con el que el WS-RPI verificar su identidad.
5	DAC-S	Verifica que se puede comunicar con el WS-RPI inalámbrico y espera la respuesta de confirmación con la siguiente estructura: *{"CMD":"RESPONSE", "ID":"XXXX", "CODE":"XX", "DESCRIPTION":"XXXXX"}* Donde CMD es la instrucción que está recibiendo el DAC-S, ID el identificador de la petición que generó la respuesta, CODE el resultado del procesamiento (0 = Sin error, 1 = Error) y DESCRIPTION es la descripción del origen del error en caso de que se haya producido.
6	DAC-S	Despliega un mensaje indicando que el WS-RPI inalámbrico se guardó correctamente.
7	DAC-S	Direcciona la pantalla del usuario al mapa de dispositivos WS-RPI y actualiza la gráfica.

Fuente: Elaboración propia.

- **Nota:** En el flujo de registro de WS-RPI se debe habilitar una funcionalidad que permita modificar la información de un WS-RPI previamente registrado.

5.4.8 Caso de uso: DAC-S - Obtener información de inventario.

Precondiciones:

- El software del DAC-S fue instalado previamente.
- La configuración inicial del DAC-S fue creada.
- El usuario denominado “Administrador del DAC-S” ha realizado inicio de sesión en la aplicación.
- El WS-RPI fue registrador con éxito previamente en el sistema.

Flujo principal de eventos:

Tabla 41: Flujo principal de eventos para el caso de uso obtener información de inventario.

Paso	Actor	Detalle
1	Administrador del DAC-S	Ingresa en el menú denominado “Listado WS-RPI”.
2	DAC-S	Muestra la pantalla denominada “Listado de los WS-RPI”, la cual despliega un listado con los siguientes campos: • Nombre del WS-RPI. • Dirección IP. • Fecha de última conexión. • Botón “Inventario”. • Botón “Clasificar AP”. • Botón “Eliminar WS-RPI”.
3	Administrador del DAC-S	Oprime el botón “Inventario”.
4	DAC-S	Despliega una pantalla denominada “Obtener información de inventario”, con los siguientes campos: • Tiempo procesamiento: Lista con la que indica el tiempo que el WS-RPI debe recolectar la información, tiene los siguientes valores: 1, 10, 15, 20, 30, 60, 120 minutos. • Margen de error: Lista donde se selecciona el

		margen de error con el cual se excluyen señales inalámbricas que se perciben muy débiles o en muy pocas ocasiones, los valores son 0%, 5%, 10%, 20%, 30% y 40%. Botón “Obtener inventario”.
5	Administrador del DAC-S	Selecciona los parámetros para la toma del inventario y oprime el botón “Obtener inventario”.
6	DAC-S	Establece comunicación con el WS-RPI y envía el comando para recolección de inventario, el cual tiene la siguiente estructura: *{"CMD":"STOCK", "ID":"XXXXX", "USER":"XXXXX", "PASS":"XXXXX", "TOKEN":"XXXXXXXX", “TIME”:” XXX”}* Donde CMD es el comando de solicitud de inventario, ID el identificador de la petición de inventario, USER y PASS el usuario y la contraseña de acceso al WS-RPI, TOKEN el código de seguridad que se le ingresó al WS-RPI cuando se configuró desde el DAC-S y TIME el periodo de tiempo en minutos que el WS-RPI debe recolectar información del inventario.
7	DAC-S	Queda a la espera de que el WS-RPI procese la información de las señales capturadas y envíe la respuesta en el tiempo establecido en la recolección del inventario.
8	WS-RPI	Recolecta la información de las señales inalámbricas que están dentro de su alcance y que serán utilizadas para crear el inventario, las envía al controlador con una estructura de datos como la siguiente: *{"AP”:* *{"BSSID":"XXXXX", "SSID":"XXXXX", "SL":"XXXXX", "NOISE":"XXXXX", "FREQ":"XXXX",*

		"CHANNEL":"XXXXX", "VENDOR":"XXXX" *"REABI":"XXX",* *"C-BSSID"["MAC":"XXXXXX", "MAC":"XXXXXX",* *"MACN":"XXXXXX" }]* *}* Donde CMD es la instrucción que se está enviando, el ID es el identificador de la petición que generó la respuesta, CODE el código de la respuesta(0 sin error, 1 error), DESCRIPTION descripción de la causa que generó el error, AP es un registro por cada punto de acceso inalámbrico detectado que en su interior está conformado por información de los parámetros de la señal como el BSSID, SSID, nivel de señal, ruido, frecuencia, canal y fabricante, en el campo C-BSSID se adjunta todas las direcciones MAC de los clientes que se encuentran conectados a ese punto de acceso.
9	DAC-S	Toma la información de los puntos de acceso detectados por el WS-RPI y los guarda en el repositorio de datos, para que posteriormente sean clasificados por el usuario “Administrador del DAC-S”.

Fuente: Elaboración propia.

5.4.9 Caso de uso: DAC-S - Obtener estatus del WS-RPI.

Precondiciones:

- El software del DAC-S fue instalado previamente.
- La configuración inicial del DAC-S fue creada.
- El usuario denominado “Administrador del DAC-S” ha realizado inicio de sesión en la aplicación.
- El WS-RPI fue registrado con éxito previamente en el DAC-S.

Flujo principal de eventos:

Tabla 42: Flujo principal de eventos para el caso de uso obtener estatus del WS-RPI.

Paso	Actor	Detalle
1	DAC-S	Realiza comunicación de forma periódica (cada 2 minutos) con el WS-RPI, envía un comando mediante el módulo de comunicación con la siguiente estructura: *{"CMD":"STATUS", "ID":"XXXXX", "USER":"XXXXX", "PASS":"XXXXX", "TOKEN":"XXXXXXXX"}* Donde CMD es el comando con la instrucción, ID el identificador de la petición, USER y PASS las credenciales de autenticación del WS-RPI y TOKEN el identificador de seguridad.
2	DAC-S	Queda a la espera del procesamiento del WS-RPI.
3	WS-RPI	Recolecta la información de las señales inalámbricas que están dentro de su alcance, las envía al controlador mediante el módulo de comunicación con una estructura de datos como la siguiente: *{"CMD":"RESPONSE", "ID":"XXXX", "CODE":"XX", "DESCRIPTION":"XXXXX", "AP":* *{"BSSID":"XXXXX", "SSID":"XXXXX", "SL":"XXXXX", "NOISE":"XXXXX", "FREQ":"XXXX", "CHANNEL":"XXXXX", "VENDOR":"XXXX"* *"C-BSSID":{"MAC1":"XXXXXX", "MAC2":"XXXXXX", "MACN":"XXXXXX" }* *}* *}* Donde CMD es la instrucción que se está enviando, ID el identificador de la petición que generó la respuesta, CODE el código de la respuesta(0 sin error, 1 error),

		DESCRIPTION descripción de la causa que generó el error, AP registro por cada punto de acceso inalámbrico detectado y que en su interior está conformado por información de los parámetros de la señal como el BSSID, SSID, nivel de señal, ruido, frecuencia, canal y fabricante, en el campo C-BSSID se adjunta todas las direcciones MAC de los clientes que están conectados al punto de acceso.
4	DAC-S	Toma la información de los puntos de acceso detectados por el WS-RPI y los guarda en el repositorio de datos, para que posteriormente sean procesados por el algoritmo de procesamiento de datos.

Fuente: Elaboración propia.

- **Nota:** Debe existir una funcionalidad desde el módulo gráfico que muestra los WS-RPI en el mapa que permita al usuario solicitar y consultar el estado del WS-RPI.

5.4.10 Casos de uso: DAC-S - Clasificar señales de inventario.

Precondiciones:

- El software del DAC-S fue instalado previamente.
- La configuración inicial del DAC-S fue creada.
- El WS-RPI fue registrado con éxito previamente en el DAC-S.
- Un proceso de análisis de inventario se ha completado previamente de forma exitosa.

Flujo principal de eventos:

Tabla 43: Flujo principal de eventos para el caso de uso clasificar señales de inventario.

Paso	Actor	Detalle
1	Administrador del DAC-S	Ingresa en el menú denominado “Listado de WS-RPI”.

2	DAC-S	Muestra la pantalla denominada “Listado de WS-RPI”, la cual despliega un listado con los siguientes campos: • Nombre del WS-RPI. • Dirección IP. • Fecha de ultima conexión. • Botón “Inventario” (Solo se muestra cuando al WS-RPI no se le ha generado el inventario). • Botón “Generar nuevo inventario” (Se muestra cuando el WS-RPI ya posee el inventario configurado, y se desea que se borre y se genere nuevamente). • Botón “Clasificar AP”. • Botón “Eliminar WS-RPI”.
3	Administrador del DAC-S	Oprime sobre el botón “Clasificar AP”.
4	DAC-S	Muestra la pantalla denominada “Inventario de puntos de acceso”, en la cual se despliega un listado con los puntos de acceso detectados por el WS-RPI cuando se realizó el proceso de recolección de señales de inventario, entre la información que se muestra esta: • BSSID: Nombre del punto de acceso. • Confiabilidad: Porcentaje de veces que apareció la señal al momento de realizar el escaneo, se obtiene al dividir 100 entre la cantidad de escaneos que realizo el WS-RPI multiplicado por la cantidad de veces que se detectó la señal inalámbrica del punto de acceso. • SSID: Dirección física de la tarjeta inalámbrica que está utilizando el punto de acceso.

- SL: Nivel de la señal.
- Ruido: Nivel de ruido que presenta el punto de acceso inalámbrico.
- Frecuencia: Frecuencia de operación del punto de acceso inalámbrico, puede ser 2.4Ghz o 5.8Ghz.
- Canal: Canal de frecuencia en el cual está operando el punto de acceso inalámbrico.
- Fabricante: Fabricante de la tarjeta inalámbrica que está utilizando el punto de acceso inalámbrico.
- Seguridad: Algoritmo de seguridad que tiene habilitado el punto de acceso inalámbrico.
- Clientes: Enlace que muestra ventana con la información de las direcciones físicas de los clientes que están conectados al punto de acceso inalámbrico.
- Clasificación: Listado donde se le puede asignar una clasificación a los puntos de acceso inalámbricos, los posibles valores son “No Clasificado”, “Miembro”, “Vecino”, “Sospechoso”, “No autorizado” y “Omitido”.

Guardar: Botón que se encuentra en la parte inferior de la pantalla y que permite guardar las clasificaciones asignadas por el administrador del DAC-S a cada punto de acceso inalámbrico que conforma el inventario.

El listado de los puntos de acceso se deberán mostrar ordenados descendentemente con base en el valor del campo “Confiabilidad”, los que tenga un nivel de confiabilidad menor al definido en el parámetro que se ingresó cuando se ejecutó el caso de uso “Obtener

		información del inventario” se deberá mostrar en un color diferente y con opción de ser descartado por el usuario; sin embargo, deberá ser manejado en el repositorio de datos para que en momentos posteriores no genere falsos positivos de puntos de acceso no autorizados.
9	Administrador del DAC-S	Selecciona una categoría para cada uno de los puntos de acceso inalámbricos desplegados y remueve los puntos de acceso con niveles de señal poco confiables. Oprime el botón guardar.
10	DAC-S	Muestra un mensaje de confirmación que las categorías de los puntos de acceso inalámbricos fueron almacenadas correctamente.

Fuente: Elaboración propia.

5.4.11 Caso de uso: DAC-S - Procesar estatus de señales.

Precondiciones:

- El software del DAC-S fue instalado previamente.
- La configuración inicial del DAC-S fue creada.
- El WS-RPI fue registrador con éxito previamente en el DAC-S.
- Un proceso de análisis de inventario se ha completado previamente de forma exitosa.
- Las señales del inventario fueron clasificadas previamente por el administrador del DAC-S.
- El caso de uso se ejecuta por cada uno de los WS-RPI configurados en el DAC-S.

Flujo principal de eventos:

Tabla 44: Flujo principal de eventos para el caso de uso procesar estatus de señales.

Paso	Actor	Detalle
1	DAC-S	Toma la información del estatus del WS-RPI recolectada previamente en el caso de uso “Obtener estatus del WS-

		RPI” y aplica algoritmo que permite categorizar las señales detectadas.
2	DAC-S	Utilizando la información de clasificación que se le asignó a cada punto de acceso inalámbrico detectado por el WS-RPI en el caso de uso “Clasificar señales del inventario” (se denominara AP_I), se realiza el siguiente procesamiento a cada uno de los puntos de acceso detectados (se denominara AP_D) en el paso 1 (Si el punto de acceso cumple con alguna de las condiciones se da por finalizado el flujo): 1. AP_D está clasificado como “no autorizado” en AP_I, se le asigna categoría “No autorizado” (Se verifica el SSID, BSSID, frecuencia y fabricante). 2. AP_D está clasificado como “Miembro” en AP_I, se le asigna categoría “Miembro” (Se verifica el SSID, BSSID y frecuencia). 3. AP_D está clasificado como “Vecino” en AP_I, se le asigna categoría “Vecino” (Se verifica el SSID, BSSID y frecuencia). 4. AP_D está clasificado como “Omitido” en AP_I, se le asigna categoría “Omitido” (Se verifica el SSID, BSSID y frecuencia). 5. AP_D está clonando otro punto de acceso, se le asigna categoría “No autorizado” (El SSID está registrado en AP_I, pero el BSSI y/o frecuencia son diferentes). 6. Un cliente de AP_D estuvo conectado a un AP_I miembro, se le asigna categoría “Sospechoso” (Se validan los BSSID_D entre los BSSID_I miembros). 7. AP_D está operando en modo “Ad_Hoc”, se le asigna categoría “No autorizado”. 8. Si no calza en ninguna de las otras categorías se le asigna un valor por defecto, en que este caso se optó

		por clasificarlo como “Sospechoso”.
3	DAC-S	En caso de que el AP_D sea catalogado como “miembro” o “vecino” no toma ningún tipo de acción y se termina el flujo del proceso.
4	DAC-S	Si el AP_D se le asigna la categoría “sospecho” o “no autorizado”, el DAC-S envía una notificación al usuario “Administrador del DAC-S” vía correo electrónico e ingresa la información del AP_D en el repositorio de datos para que sea procesada como alertas pendientes de resolver.
10	DAC-S	Queda a la espera que el administrador del DAC-S tome una acción en el sistema.

Fuente: Elaboración propia.

- **Nota:** El procesamiento de los puntos de acceso detectados se debe realizar de forma automatizada cada vez que el DAC-S solicite el estatus de las señales a los WS-RPI.

5.4.12 Caso de uso: DAC-S - Atender alertas pendientes de resolver.

Precondiciones:

- El software del DAC-S fue instalado previamente.
- La configuración inicial del DAC-S fue creada.
- El WS-RPI fue registrado con éxito previamente en el DAC-S.
- Un proceso de análisis de inventario se ha completado previamente de forma exitosa.
- Las señales del inventario fueron clasificadas previamente por el administrador del DAC-S.
- El proceso de análisis de señales generó algún tipo de alerta.

Flujo principal de eventos:

Tabla 45: Flujo principal de eventos para el caso de uso atender alertas pendientes de resolver.

Paso	Actor	Detalle
1	Administrador del DAC-S.	Ingresa a la interfaz de gestión del DAC-S y oprime el menú “Gestión de alertas”.
2	DAC-S	Muestra la pantalla denominada “Listado de alertas”, la cual despliega un listado de todas las alertas que ha generado el DAC-S (ordenadas descendentemente según la fecha de registro) con los siguientes campos: • Fecha: Fecha en la que se generó la alerta. • ID: Identificador de la alerta. • WS-RPI: Nombre del WS-RPI donde se generó la alerta. • IP: Dirección IP del WS-RPI donde se generó la alerta. • BSSID: Enlace que muestra la dirección física de la tarjeta inalámbrica del punto de acceso que está generando la alerta • SSID: Enlace que muestra el nombre del punto de acceso que está generando la alerta • Clasificación: Clasificación que se le asignó al punto de acceso, puede tener los valores “No autorizado” o “Sospechoso”. • Estado: Estado que posee la alerta, puede tener los valores “Pendiente de tramitar”, “En espera”, “Tramitada”. • Gestionar: Botón que permite gestionar la alerta para asignarle un nuevo estado.

		Nota: El campo BSSID y SSID son enlaces que al oprimirlos permiten consultar el detalle completo de la información del punto de acceso, como fabricante, frecuencia, ruido, cliente conectados, entre otros.
3	Administrador del DAC-S	Oprime el botón “Gestionar” sobre la alerta que desea gestionar.
4	DAC-S	Muestra una ventana denominada “Gestión de alertas”, en la cual se muestra los siguientes campos. • Fecha: Fecha en la que se generó la alerta. • ID: Identificador de la alerta. • WS-RPI: Nombre del WS-RPI donde se generó la alerta. • SSID: Enlace que muestra el nombre del punto de acceso que está generando la alerta • Acción: Listado de posibles acciones que pueden ser realizadas por el usuario, entre los posibles valores se tienen: “Mover al inventario como autorizado”, “Mover al inventario como vecino”, “Mover al inventario como no autorizado”, “Alerta en espera” y “Descartar alerta”. • Descripción: Campo de texto de tamaño de 1000 caracteres donde el administrador del DAC-S puede ingresar cualquier comentario asociado a la gestión que se realizó en la alerta. • Guardar: Botón que permite almacenar el estado asignado a la alerta.
10	Administrador del DAC-S	Ingresa la información asociada a la alerta y oprime el botón “Guardar”.

11	DAC-S	Con base en la información ingresada por el administrador del DAC-S realiza las siguientes acciones: • Si la acción es “Mover al inventario como autorizado, vecino o no autorizado”, guarda la información del AP_D que generó la alerta en el inventario del WS-RPI con la clasificación correspondiente y le asigna el estado “Tramitada”. • Si la acción es “Alerta en espera”, la alerta cambia al estado “En espera”. Se despliega un mensaje indicando que la información se guardó correctamente.

Fuente: Elaboración propia.

5.4.13 Caso de uso: DAC-S - Graficar dispositivos en plano.

Precondiciones:

- El software del DAC-S fue instalado previamente.
- La configuración inicial del DAC-S fue creada.
- Existe al menos un WS-RPI registrado.
- El usuario con el rol “Administrador del DAC-S” inició sesión en la aplicación.

Flujo principal de eventos:

Tabla 46: Flujo principal de eventos para el caso de uso graficar dispositivos en plano.

Paso	Actor	Detalle
1	Administrador del DAC-S	Ingresa a la página principal de la interfaz de gestión del DAC-S.
2	DAC-S	Despliega de forma gráfica en una figura cuadrada o rectangular todos los WS-RPI que posee configurados el DAC-S, por defecto se muestra la siguiente información: • Nombre: Nombre que se le asignó al WS-RPI

		cuando se registró en el sistema. • IP: Dirección IP que se le asignó al WS-RPI cuando se registró en el sistema. • Última conexión: Fecha y hora de la última vez que se tuvo comunicación con el WS-RPI. Por defecto el icono del WS-RPI se deberá mostrarse en color verde, pero si tiene una alerta pendiente de tramitar se debe mostrar en color rojo, mientras que si posee algún problema de configuración se debe mostrar de color amarillo, si no existe comunicación se despliega de color gris.
3	Administrador del DAC-S	Coloca del cursor del mouse sobre el icono del WS-RPI.
4	DAC-S	Despliega un menú con las opciones “Información detallada”, “Consulta inventario” y “Consulta de alertas”.
5	Administrador del DAC-S	Selecciona alguna opción del menú que se desplegó en el paso anterior.
6	DAC-S	Despliega pantalla con información según sea la opción seleccionada por el administrador del DAC-S.

Fuente: Elaboración propia.

5.5 Diseñar la arquitectura del sistema.

5.5.1 Diagramas de base de datos

En las figuras 10 y 11 se muestran las estructuras de datos utilizadas para almacenar los datos de las señales detectadas por la herramienta de monitoreo que se ejecuta dentro del WS-RPI y el DAC-S, así como las diferentes funcionalidades como el procesamiento de inventario, estados y alertas.

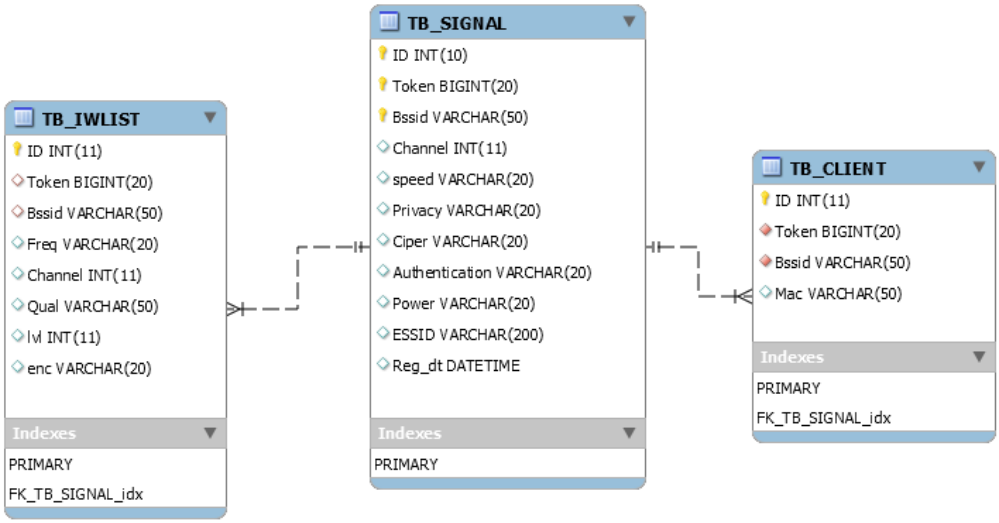


Figura 10: Diagrama de base de datos donde se almacena la información recolectada por las herramientas de escaneo dentro del WS-RPI.

Fuente: Elaboración propia.

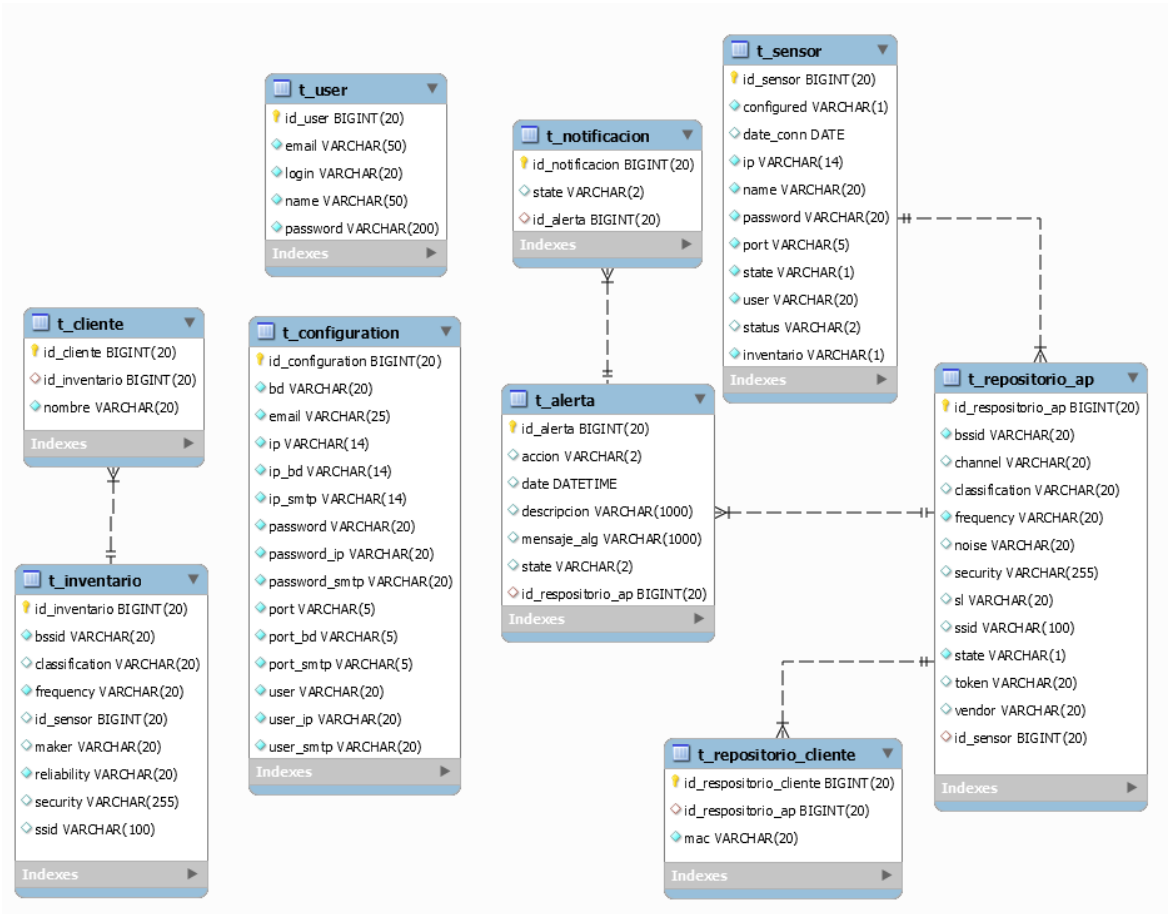


Figura 11: Diagrama de la estructura de base de datos utilizada por el DAC-S para almacenar la información recibida por los WS-RPI.

Fuente: Elaboración propia.

5.5.2 Arquitectura del WS-RPI

Según la figura 12 se muestra los principales elementos que conforman la arquitectura del WS-RPI, el cual es una Raspberry PI 3 en la que se instalaron y configuraron las tecnologías de código abierto necesarias para que pueda realizar las funcionalidades establecidas en los casos de uso. Entre estos elementos se tiene:

- Servicio Web-Socket: Programa desarrollado en Python, el cual inicia un Websocket con el cual el WS-RPI se puede comunicar con el DAC-S y viceversa. Adicionalmente, realiza otras funciones como controlar las señales del botón resetear y el estado de las luces de estado.
- Servicio GUI: Programa desarrollado en Node JS, el cual provee una interfaz de gestión por la cual el usuario puede configurar y verificar el estado del WS-RPI.
- Servicio MySQL: Servicio por el cual las tareas programadas de escaneo se pueden comunicar con el motor de base de datos y almacenar la información de las señales recolectadas en el repositorio de datos.
- Servicio SSH: Servicio de intérprete de órdenes seguro, por el cual el usuario puede ingresar remotamente al WS-RPI y realizar otras configuraciones no soportadas por la GUI.
- Logs: Carpetas definidas para almacenar las bitácoras de eventos asociados al funcionamiento del WS-RPI.
- Tarea programada analizar señales inalámbricas: Tarea programada que ejecuta cada 5 minutos la herramienta airdump-ng, la cual se encarga de recolectar y exportar los datos de las señales inalámbricas detectadas dentro del alcance del WS-RPI.

- Tarea programada limpieza de logs: Tarea programada que se ejecuta cada día y que se encarga de realizar una limpieza de los datos que ya no tienen utilidad en el WS-RPI, como lo son bitácoras, archivos temporales e información de la base de datos.

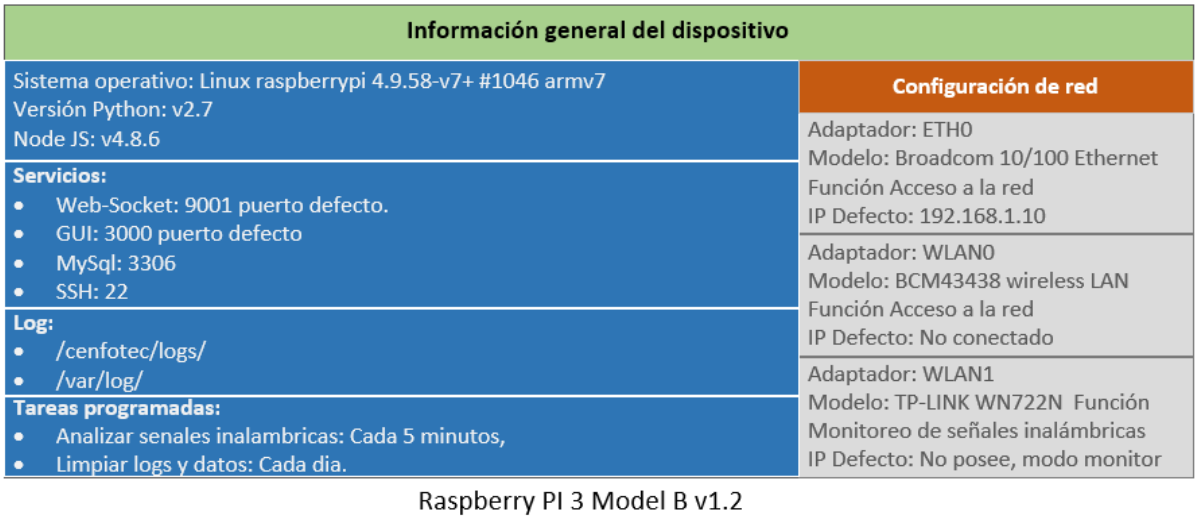


Figura 12: Diagrama de los principales elementos que conforman el WS-RPI.

Fuente: Elaboración propia.

En el anexo 1 se puede visualizar la apariencia física del dispositivo una vez completado su diseño.

5.5.3 Diagrama eléctrico del botón resetear y luces indicadoras

En el diagrama de la figura 13 se muestra los elementos electrónicos utilizados en el sensor para implementar las luces indicadoras y el botón de resetear a configuración de fábrica.

Se utiliza 2 diodos emisores de luz, un interruptor de presión y una resistencia de 220 ohmios, para el caso de los pines de la Raspberry PI se utilizó el #19 para lectura del interruptor, el #12 para enviar la señal del diodo color verde y el #16 para enviar la señal del diodo color amarillo.

Se detalla algunos aspectos básicos del funcionamiento de estos elementos:

- Luz verde encendida: El sensor fue configurado de forma exitosa.

- Luz verde intermitente: El sensor está procesando señales inalámbricas o recibiendo comandos del DAC-S.
- Luz amarilla fija: El sensor no está configurado o posee algún tipo de error en los servicios.
- Luz amarilla intermitente: El sensor ha iniciado el proceso de reinicio con configuración inicial por defecto.
- Botón Resetear: Debe estar oprimido por al menos 5 segundos para que el proceso de reinicio tome efecto.

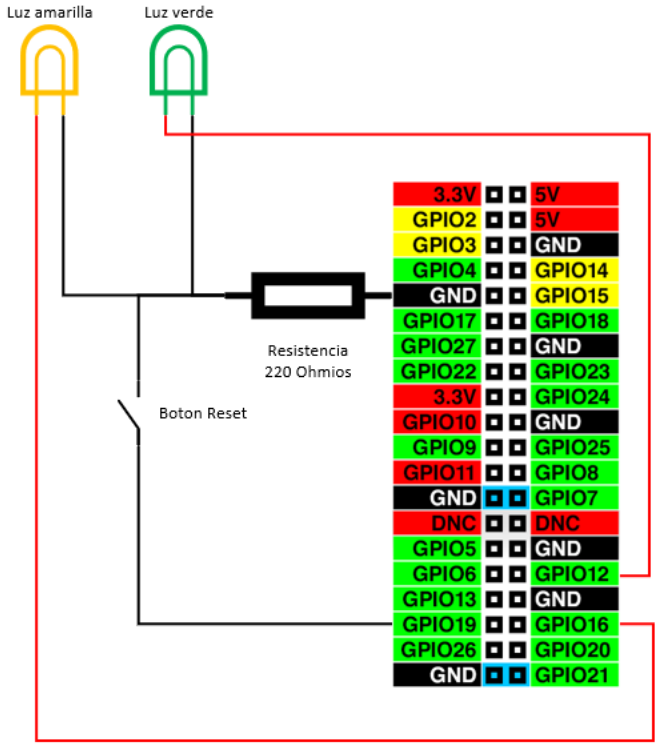


Figura 13: Diagrama de los componentes eléctricos con los que se implementó las luces indicadoras del sensor y el botón resetear.

Fuente: **(Kuo, s.f.)**.

En el anexo 2 se muestra el detalle de los elementos electrónicos que conforman el botón de resetear y luces indicadoras implementado en los pines de entrada y salida de señales digitales de la Raspberry PI.

5.5.4 Arquitectura del DAC-S

En la figura 14 se puede visualizar los principales elementos que conforman el DAC-S, el cual fue diseñado con las tecnologías de código abierto Java 1.8 y Angular 4, se procede a describir de forma general cada uno:

- Servicio Restful: Servicio publicado utilizando el lenguaje de programación Java 1.8 y el cual se ejecuta como la capa de acceso y datos de la aplicación(backend). Tiene acceso a otros elementos como la base de datos, tareas programadas y servicios.
- GUI: Componente de la aplicación desarrollado en Angular 4 y el cual realiza la función de frontal de la aplicación, por lo que se encarga de desplegar los datos generados por la parte trasera e interactuar con los datos y eventos ingresados por el usuario.
- LOGS: Directorio donde se almacenan todas las bitácoras y eventos de la aplicación en archivos de formato específico, los cuales poseen información como fecha y hora del evento, método que lo generó e información de parámetros.
- Servicio de análisis y procesamiento de señales: Servicio que se encarga de analizar las señales recolectadas por los sensores y generar las alertas correspondientes en caso de existir alguna anomalía.
- Servicio solicitar estatus del sensor: Servicio que se encarga de contactar periódicamente a lo sensores y les solicita el estatus de las señales para que posteriormente sean procesadas.
- Envío de notificaciones: Servicio que se encarga de tomar la información de las alertas generadas por el servicio que procesa las señales y envía las notificaciones mediante el servidor SMTP configurado en el DAC-S.

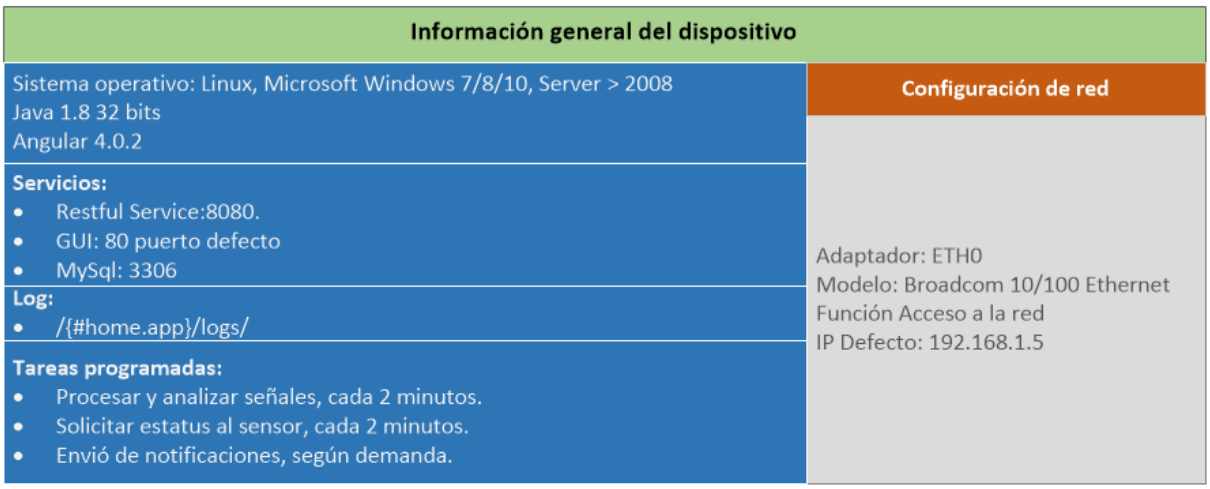


Figura 14: Diagrama de arquitectura de la solución del DAC-S.

5.5.5 Diagrama general de la solución

En la imagen de la figura 15 se puede visualizar una posible implementación del sistema de monitoreo de puntos de acceso inalámbricos no autorizados, donde se posee una red local con salida a internet protegido por un equipo de seguridad como puede ser un firewall. Internamente se tiene una red local principal, a la cual se conectan los puntos de acceso autorizados (color verde), los sensores inalámbricos (color naranja), los posibles equipos que brindan servicios y el equipo donde se instala el software DAC-S. En azul se muestran los puntos inalámbricos vecinos que puede generar señales que estén dentro del alcance del sensor y finalmente el punto de acceso no autorizado se representa de color rojo junto con el posible usuario malicioso que lo instaló.

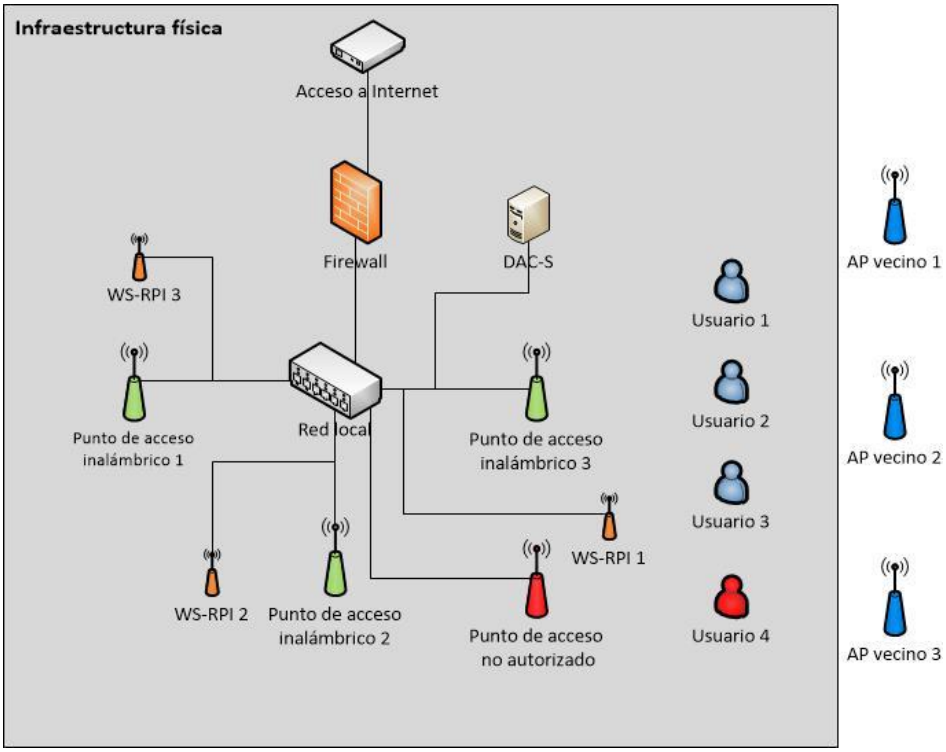


Figura 15: Diagrama de red de una posible implementación de la solución.

Fuente: Elaboración propia.

5.6 Desarrollar el software e interfaz de gestión del dispositivo.

5.6.1 WS-RPI

El software del sensor inalámbrico se desarrolla utilizando los lenguajes de programación Python y NodeJs, en conjunto con el repositorio de datos MySQL.

Para el caso de la GUI y el Websocket se utilizó el patrón de diseño modelo-vista- DAC-S, el cual se basa en que la aplicación debe tener al menos tres capas:

- Vista: Fuentes que sirven para representar o mostrar los datos a los usuarios, generalmente es la que se conoce como interfaz gráfica.
- DAC-S: Capa que se encarga de validar los datos que se ingresaron en la vista y se les debe dar algún tipo de procesamiento, además realiza otros tipos de validaciones como el acceso que tienen usuarios a funcionalidades según los roles que se les haya asignado.

- Modelo: Es la capa que se encarga de almacenar y cargar la información desde el repositorio de datos y que recibe o necesita el DAC-S.

Se describe a nivel macro como se encuentra estructurado el directorio que conforma los diferentes programas y funcionalidades que se implementaron en el sensor:

- /cenfotec/Config/: Directorio donde se almacena todos los archivos de configuración que necesitan los aplicativos para funcionar correctamente.
- /cenfotec/data/: Carpeta donde se almacena todos los archivos de datos generados por la herramienta de análisis de señales inalámbricas Airmon-ng y iwlist.
- /cenfotec/logs/: Carpeta donde se almacena todos los archivos de bitácoras y logs que genera la aplicación.
- /cenfotec/NodeJs/: Carpeta donde se instalaron todas las fuentes que conforman la GUI del sensor y que fueron desarrolladas en el lenguaje de programación NodeJs.
- /cenfotec/script/: Directorio donde se colocan todos los scripts binarios que utiliza el aplicativo, como lo son los que inician la configuración del dispositivo, la herramienta de escaneo de señales inalámbricas, configuración automática de red, entre otros.
- /cenfotec/socket/: Directorio donde se instalaron las fuentes desarrolladas en Python, las cuales se encargan de cargar la información de los archivos generados por la herramienta Airmon-ng en el repositorio de datos, controlar el botón de resetear, las luces indicadoras y publicar el Websocket con el que se comunica el DAC-S y el sensor.

De la figura 16 a la 19 se muestra el detalle de cómo se visualiza cada una de las pantallas que conforma el software gestor del sensor inalámbrico:

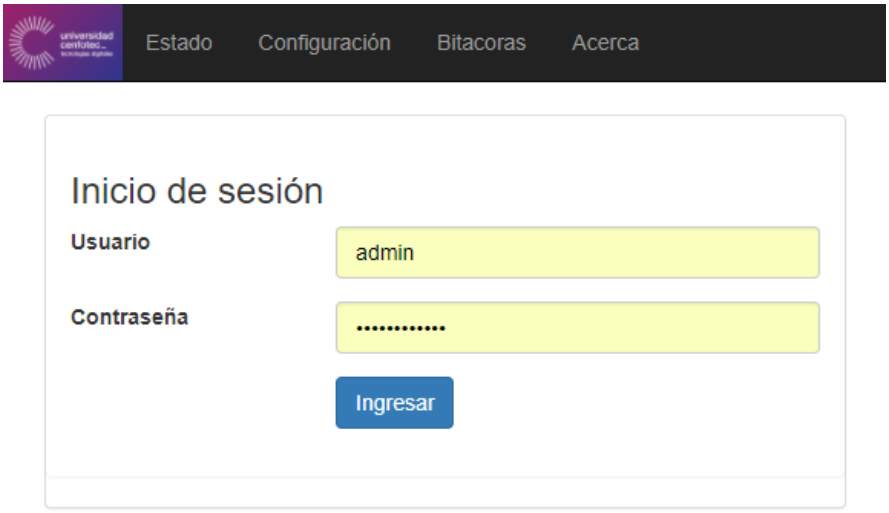


Figura 16: Detalle de la pantalla de inicio de sesión de la interfaz de gestión del sensor inalámbrico.

Fuente: Elaboración propia.

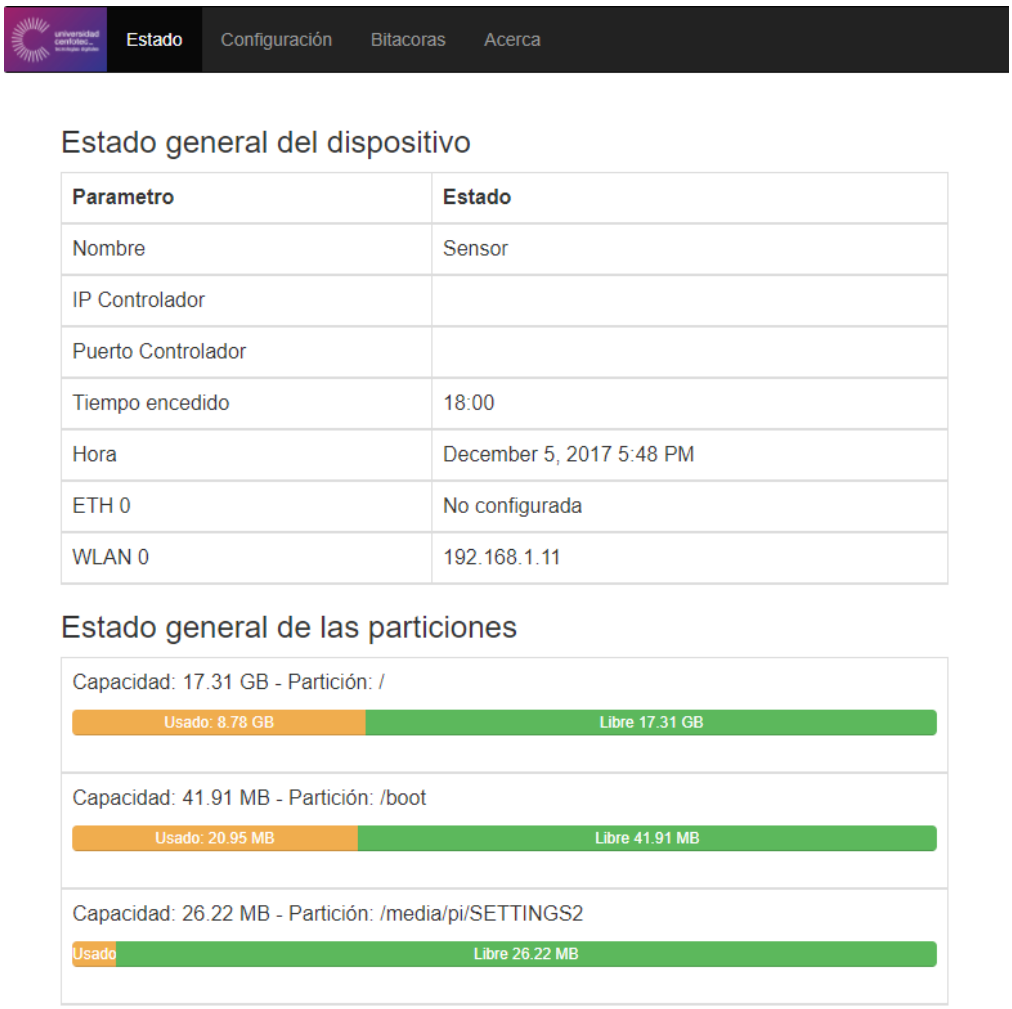


Figura 17: Pantalla con el detalle del estado de la configuración del sensor inalámbrico.

Fuente: Elaboración propia.

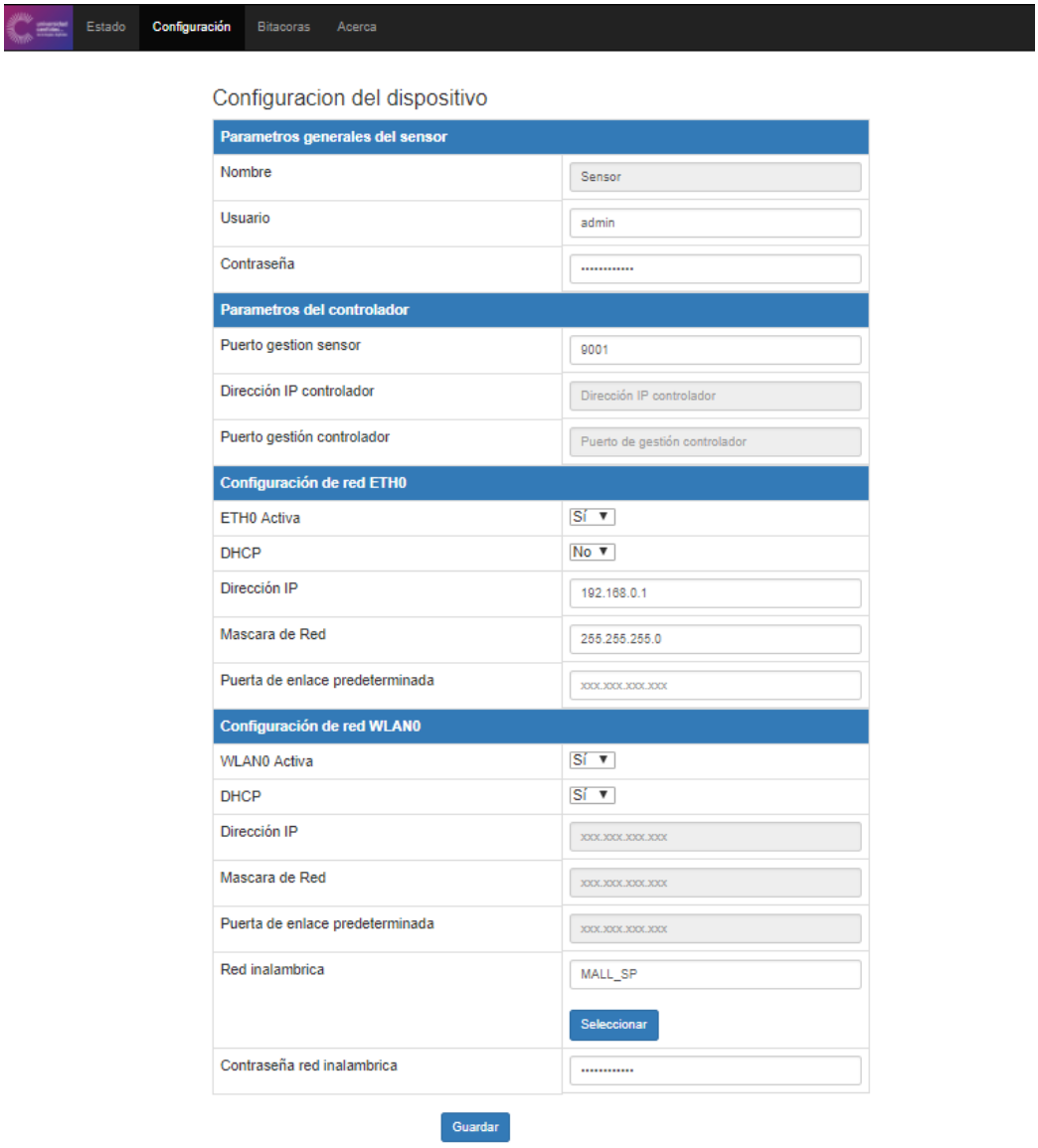


Figura 18: Pantalla donde se ingresan los parámetros de configuración del sensor inalámbrico.

Fuente: Elaboración propia.

```
root@raspberrypi:/cenfotec/data# cat airdump-201712020000-01.csv

BSSID, First time seen, Last time seen, channel, Speed, Privacy, Cipher, Authentication, Power, # beacons, # IV, LAN IP, ID-length, ESSID, Key
00:25:00:FF:94:73, 2017-12-02 00:02:19, 2017-12-02 00:02:46,  1,  -1, OPN, ,   ,  -1,        0,        1,   0.  0.  0.  0,   0, ,
E8:61:7E:80:CE:DF, 2017-12-02 00:00:05, 2017-12-02 00:03:20,  1,  54, WPA2, CCMP,PSK, -81,       27,        0,   0.  0.  0.  0,  16, PS4-EDC065976E8D,
00:23:6A:A7:2F:BB, 2017-12-02 00:00:05, 2017-12-02 00:03:24,  1,  54, WPA2 WPA, CCMP TKIP,PSK, -58,      356,      260,   0.  0.  0.  0,   5, OMEGA,
00:23:6A:A6:5A:90, 2017-12-02 00:00:05, 2017-12-02 00:03:24,  1,  54, WPA2 WPA, CCMP TKIP,PSK, -37,      394,      184,   0.  0.  0.  0,   6, Torito,

Station MAC, First time seen, Last time seen, Power, # packets, BSSID, Probed ESSIDs
E8:61:7E:80:CE:DF, 2017-12-02 00:00:20, 2017-12-02 00:01:02,  -1,        4, 00:23:6A:A7:2F:BB,
D0:03:4B:E8:7D:83, 2017-12-02 00:01:49, 2017-12-02 00:02:16, -77,        8, 00:23:6A:A7:2F:BB,
74:8D:08:58:F2:68, 2017-12-02 00:00:16, 2017-12-02 00:02:11, -73,      114, 00:23:6A:A7:2F:BB,
EA:11:A9:DA:62:57, 2017-12-02 00:02:19, 2017-12-02 00:02:46, -86,       45, 00:25:00:FF:94:73,
80:65:6D:39:FD:37, 2017-12-02 00:00:51, 2017-12-02 00:02:49, -61,        9, 00:23:6A:A6:5A:90,
6C:72:E7:11:1E:4E, 2017-12-02 00:00:06, 2017-12-02 00:02:49, -60,       10, 00:23:6A:A6:5A:90,
00:21:5C:B9:3F:F2, 2017-12-02 00:00:20, 2017-12-02 00:02:53, -51,       20, 00:23:6A:A6:5A:90,Torito
54:B1:21:7F:80:6C, 2017-12-02 00:00:52, 2017-12-02 00:02:57, -46,       11, 00:23:6A:A6:5A:90,
E0:AC:CB:32:31:21, 2017-12-02 00:01:49, 2017-12-02 00:03:24,  -1,       55, 00:23:6A:A7:2F:BB,
```

Figura 19: Detalle de los datos recolectados por la herramienta de análisis de señales inalámbricas Airmong-ng.

Fuente: Elaboración propia.

Ahora se muestran algunos de los fragmentos de código fuente de las principales funciones que realiza el WS-RPI, los cuales se muestran de la figura 20 a la 24:

gpio.py

```
import RPi.GPIO as GPIO

# Metodo que carga la configuracion inicial de la GPIO de la Raspberry.
def configure():
    GPIO.setmode(GPIO.BCM)
    GPIO.setwarnings(False)
    GPIO.setup(12, GPIO.OUT)
    GPIO.setup(16, GPIO.OUT)
    GPIO.setup(19, GPIO.IN, pull_up_down=GPIO.PUD_UP)

# Metodo que se encarga de encender y apagar el led de color verde de la Raspberry
# Parametros(State: 0->Apagado, 1->Encendido)
def set_ready_led(state):
    if state == 1:
        GPIO.output(12, GPIO.HIGH)
    elif state == 0:
        GPIO.output(12, GPIO.LOW)

# Metodo que se encarga de enceder y apagar el led de reset(color amarillo) de la Raspberry
# Parametros(0 = Apagado, 1 = Encendido)
def set_reset_led(state):
    if state == 1:
        GPIO.output(16, GPIO.HIGH)
    elif state == 0:
        GPIO.output(16, GPIO.LOW)

# Metodo que se encarga de leer la señal que recibe el boton de Reset de la Raspberry
# Retorna: 0-> Boton no presionado, 1->Boton presionado
def get_button_output():
    return GPIO.input(19)

# Metodo que se encarga de resetear el estado de la GPIO de la Raspberry, no recibe parametros ni retorna nada.
# Se utiliza cada vez que se apaga o inicia el dispositivo
def clear():
    GPIO.cleanup()
```

Figura 20: Detalle de los métodos que se encargan de configurar la GPIO de la Raspberry PI, así como encender-apagar leds y leer la señal del botón.

Fuente: Elaboración propia.

```
# metodo que se encarga de iniciar el Web Socket que funciona como modulo de comunicacion entre la Raspberry y el
# equipo centralizado
def start_server():
    global server
    conf = ConfigParser.ConfigParser()
    conf.read("/cenfotec/config/config.ini")

    port = int(conf.get("admin", "admin_port").strip())
    server = WebsocketServer(port, host='0.0.0.0')
    server.set_fn_new_client(new_client)
    server.set_fn_client_left(client_left)
    server.set_fn_message_received(message_received)
    tools.log.writelog("Servidor listo para recibir comandos en el puerto: " + str(port), 'INFO')
    gpio.set_ready_led(1)
    server.run_forever()
```

Figura 21: Detalle del código fuente que se encarga de iniciar el Web Socket (módulo de comunicación) en la Raspberry PI.

Fuente: Elaboración propia.

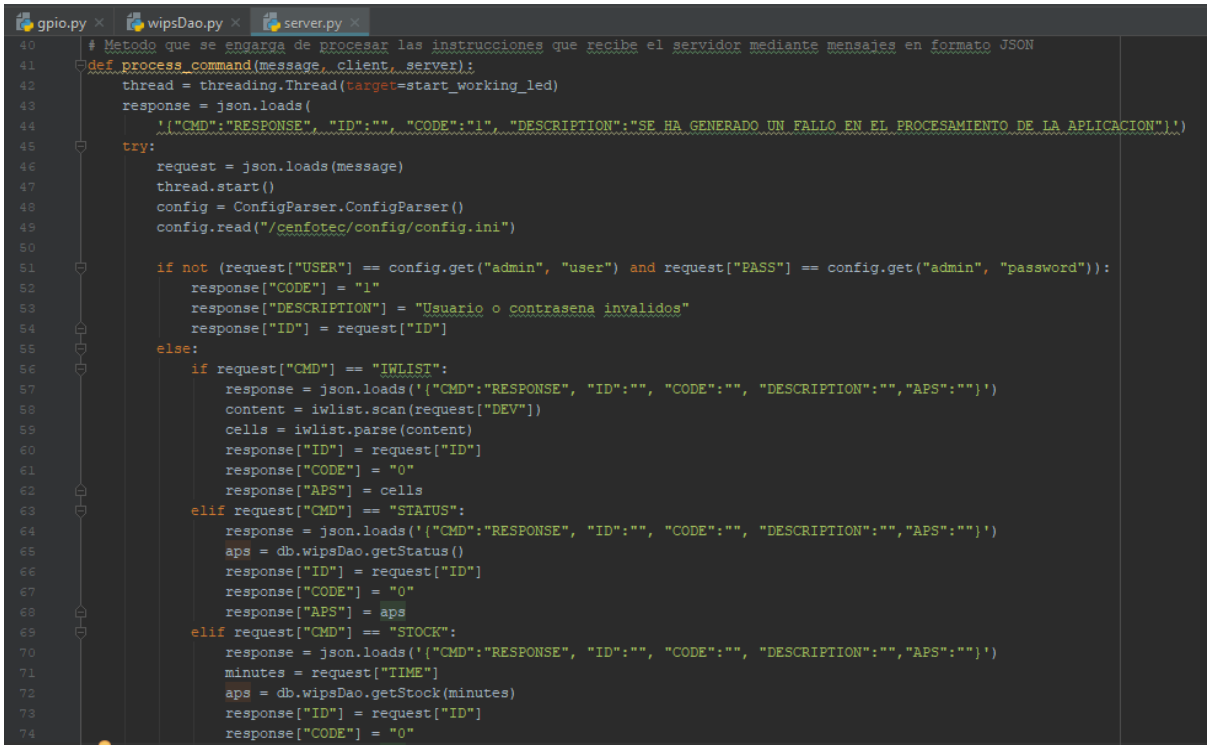


Figura 22: Detalle del código fuente del método que se encarga de procesar los comandos que recibe la Raspberry desde el DACS en formato JSON.

Fuente: Elaboración propia.

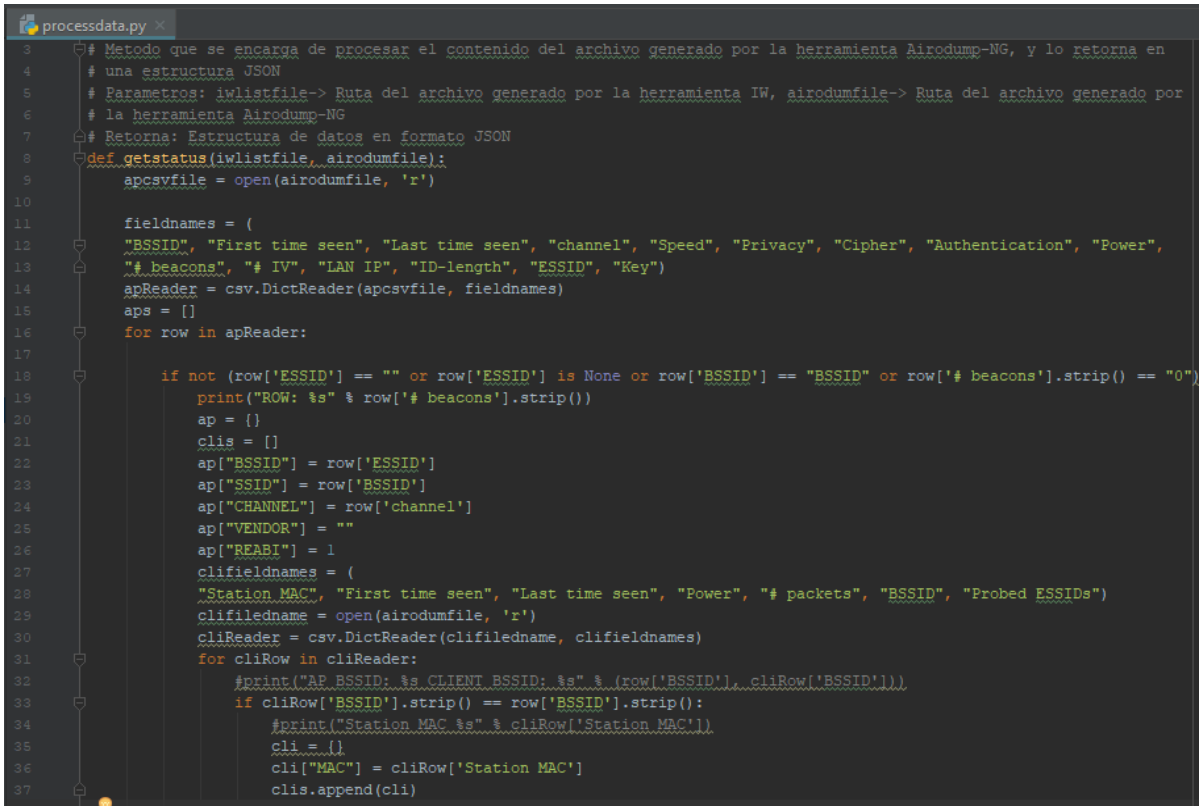


Figura 23: Detalle del código fuente del método que se encarga de procesar los datos generados por la herramienta de análisis de señales y la transforma a una estructura estandarizada en formato JSON.

Fuente: Elaboración propia.

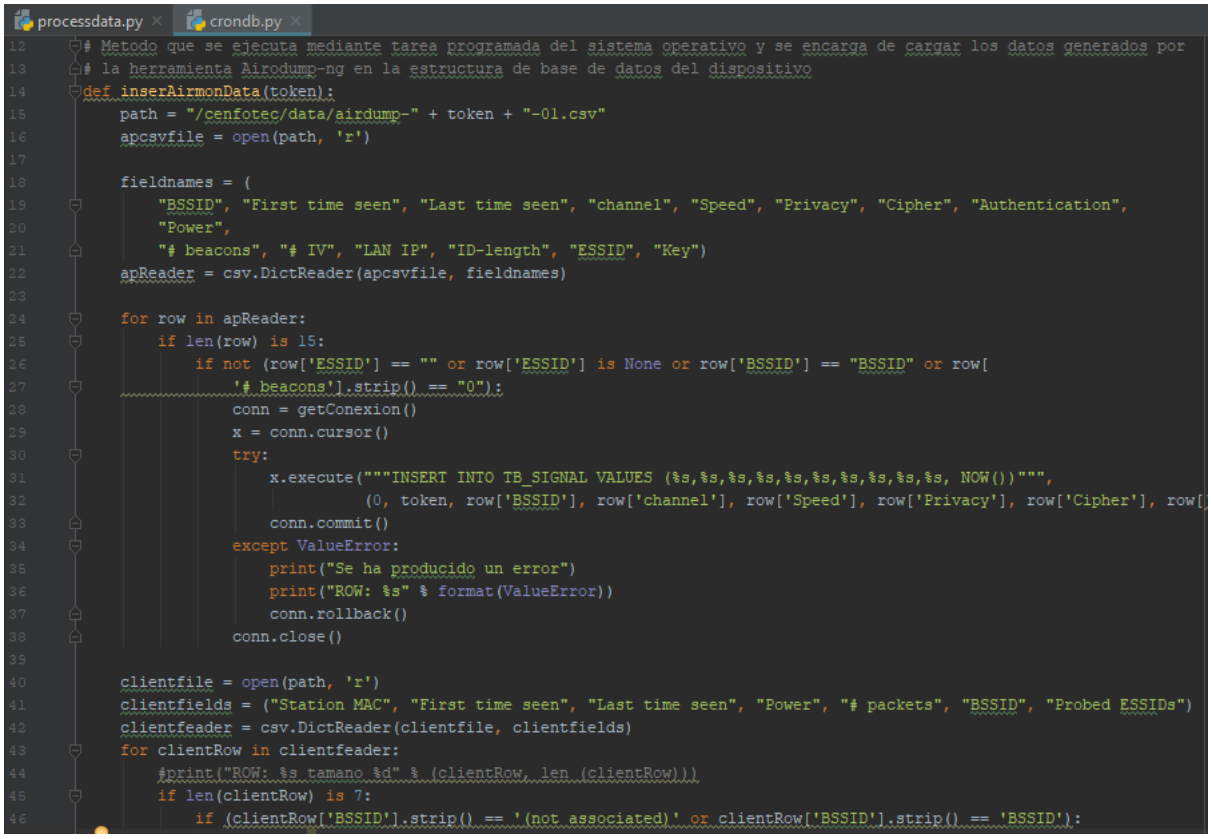


Figura 24: Detalle del código fuente del método que se ejecuta con una tarea programada del sistema operativo de la Raspberry, el cual se encarga de procesar los datos estandarizados generados por la herramienta de análisis de señales y la carga a la base de datos del dispositivo.

Fuente: Elaboración propia.

5.6.2 DAC-S

El software del DAC-S se desarrolla en las tecnologías de código abierto Java JDK 1.8 32bits, Angular 4 y el repositorio de datos MySQL. Debido a que la solución es una GUI se utiliza el patrón de diseño modelo-vista-controlador, el cual se basa en que la aplicación debe tener al menos tres capas:

- Vista: Fuentes que sirven para representar o mostrar los datos a los usuarios, generalmente es la que se conoce como interfaz gráfica. Esta capa fue desarrollada utilizando Angular.
- DAC-S: Capa que se encarga de validar los datos que se ingresaron en la vista y se les debe dar algún tipo de procesamiento, además realiza otros tipos de

validaciones como el acceso que tienen usuarios a funcionalidades según los roles que se les haya asignado.

- Modelo: Es la capa que se encarga de almacenar y cargar la información desde el repositorio de datos y que recibe o necesita el DAC-S.

De la figura 25 a la 30 se muestra algunas de las pantallas que se obtuvo como resultado del desarrollo del DAC-S del sistema de monitoreo.

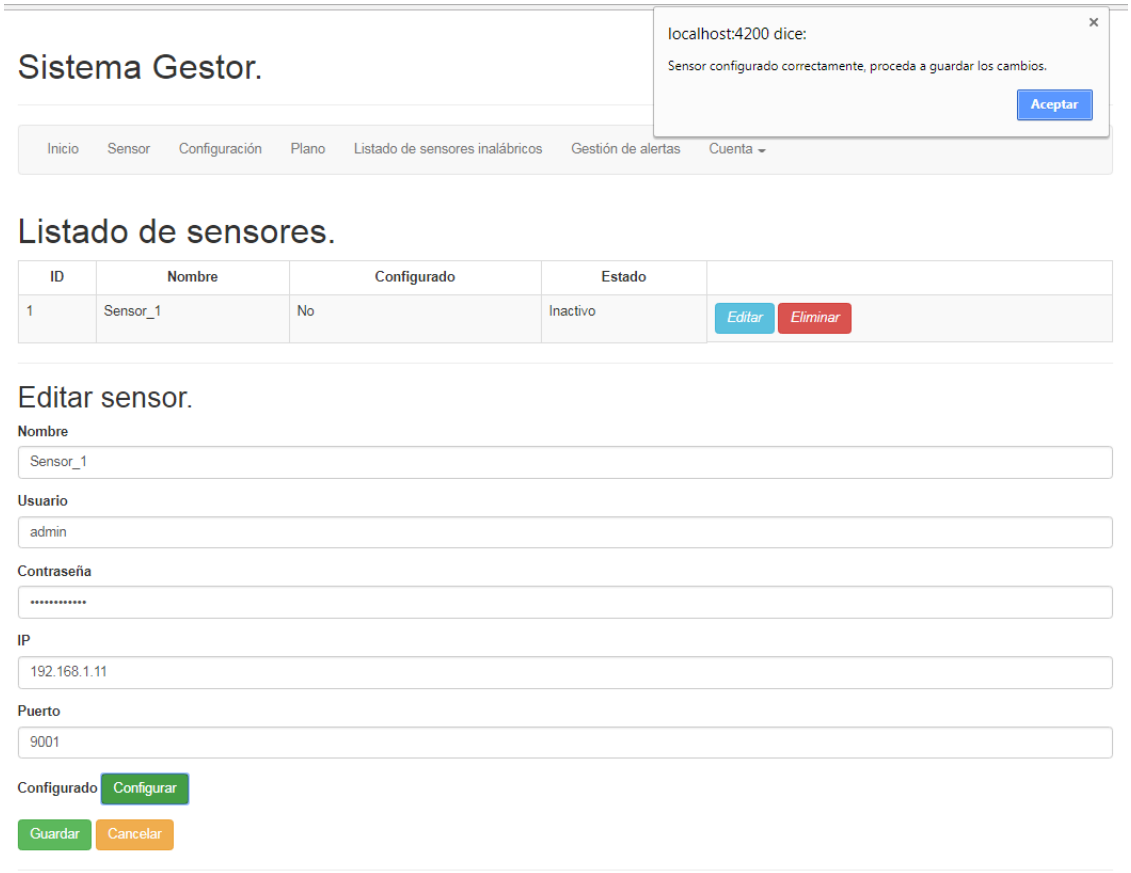


Figura 25: Pantalla del DAC-S donde se ingresa la configuración del sensor inalámbrico junto con mensaje de confirmación de configuración realizada con éxito.

Fuente: Elaboración propia.

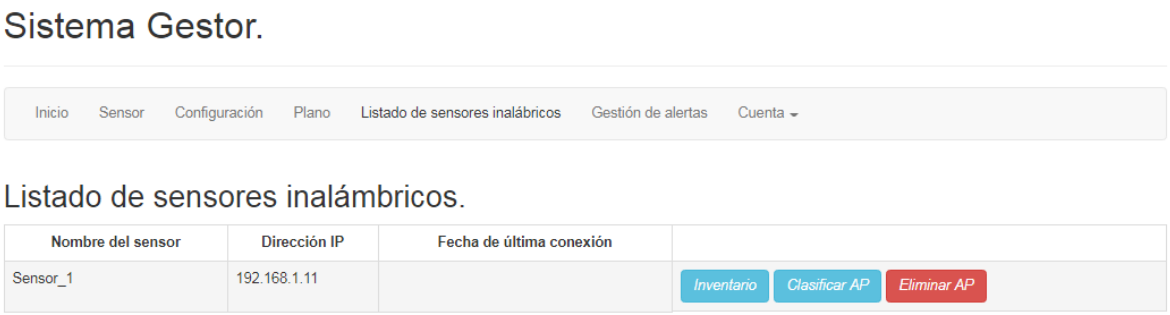


Figura 26: Pantalla del DAC-S donde se muestra el listado de sensores configurados.

Fuente: Elaboración propia.

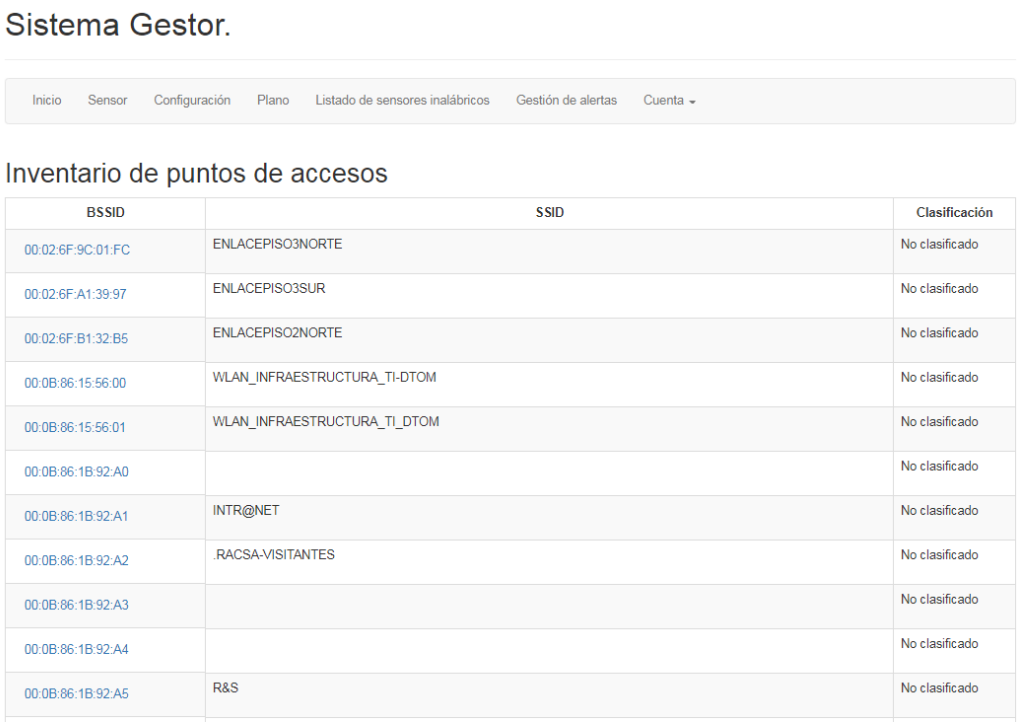


Figura 27: Pantalla del DAC-S donde se muestra la información de inventario obtenida por un sensor.

Fuente: Elaboración propia.

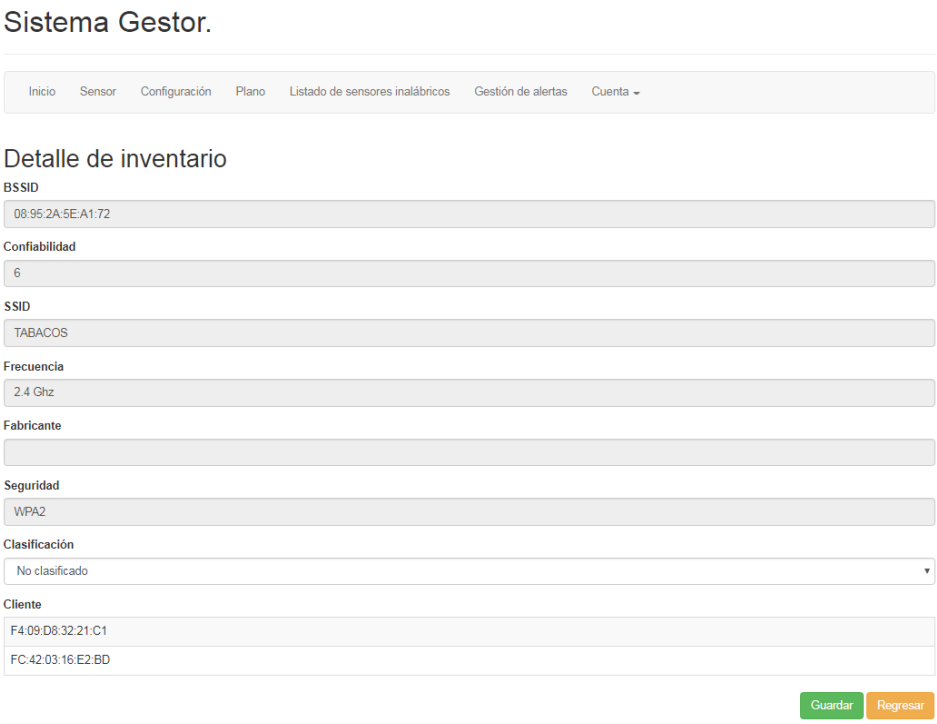
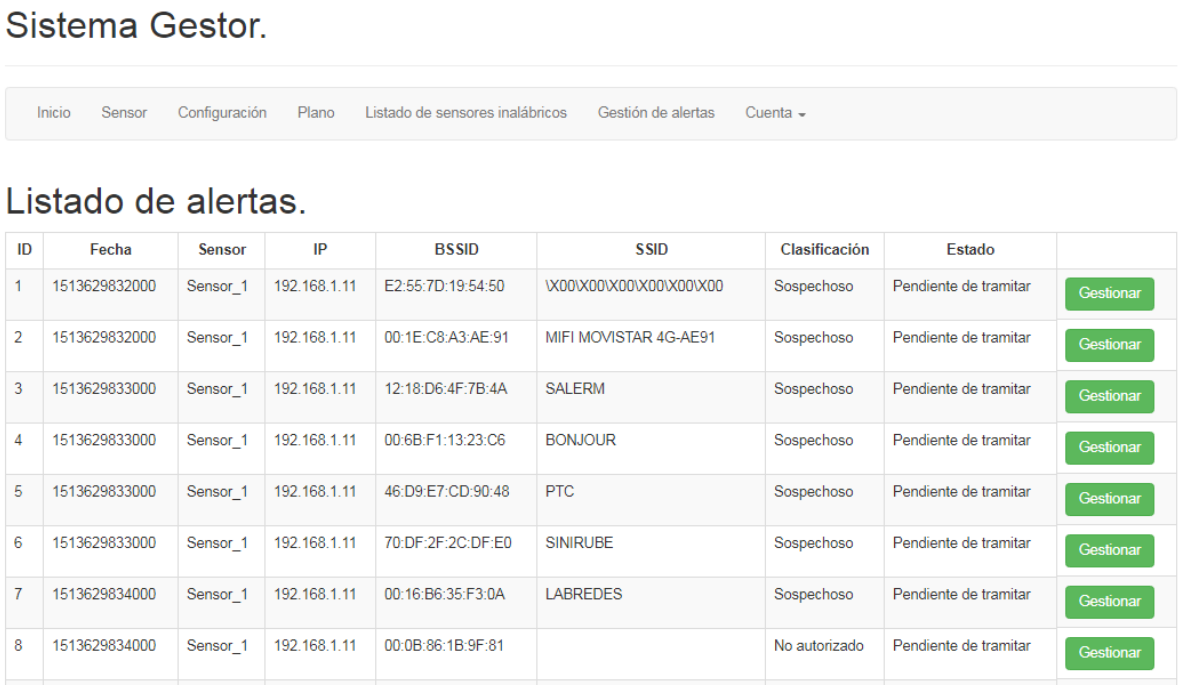


Figura 28: Pantalla del DAC-S donde se ingresa la clasificación de cada uno de los puntos de accesos detectados en el proceso de inventario del sensor inalámbrico.

Fuente: Elaboración propia.



ID	Fecha	Sensor	IP	BSSID	SSID	Clasificación	Estado	
1	1513629832000	Sensor_1	192.168.1.11	E2:55:7D:19:54:50	\X00\X00\X00\X00\X00\X00	Sospechoso	Pendiente de tramitar	Gestionar
2	1513629832000	Sensor_1	192.168.1.11	00:1E:C8:A3:AE:91	MIFI MOVISTAR 4G-AE91	Sospechoso	Pendiente de tramitar	Gestionar
3	1513629833000	Sensor_1	192.168.1.11	12:18:D6:4F:7B:4A	SALERM	Sospechoso	Pendiente de tramitar	Gestionar
4	1513629833000	Sensor_1	192.168.1.11	00:6B:F1:13:23:C6	BONJOUR	Sospechoso	Pendiente de tramitar	Gestionar
5	1513629833000	Sensor_1	192.168.1.11	46:D9:E7:CD:90:48	PTC	Sospechoso	Pendiente de tramitar	Gestionar
6	1513629833000	Sensor_1	192.168.1.11	70:DF:2F:2C:DF:E0	SINIRUBE	Sospechoso	Pendiente de tramitar	Gestionar
7	1513629834000	Sensor_1	192.168.1.11	00:16:B6:35:F3:0A	LABREDES	Sospechoso	Pendiente de tramitar	Gestionar
8	1513629834000	Sensor_1	192.168.1.11	00:0B:86:1B:9F:81		No autorizado	Pendiente de tramitar	Gestionar

Figura 29: Pantalla del DAC-S donde se muestran las alertas generadas como el resultado de analizar del estatus de las señales enviadas por el sensor inalámbrico.

Fuente: Elaboración propia.

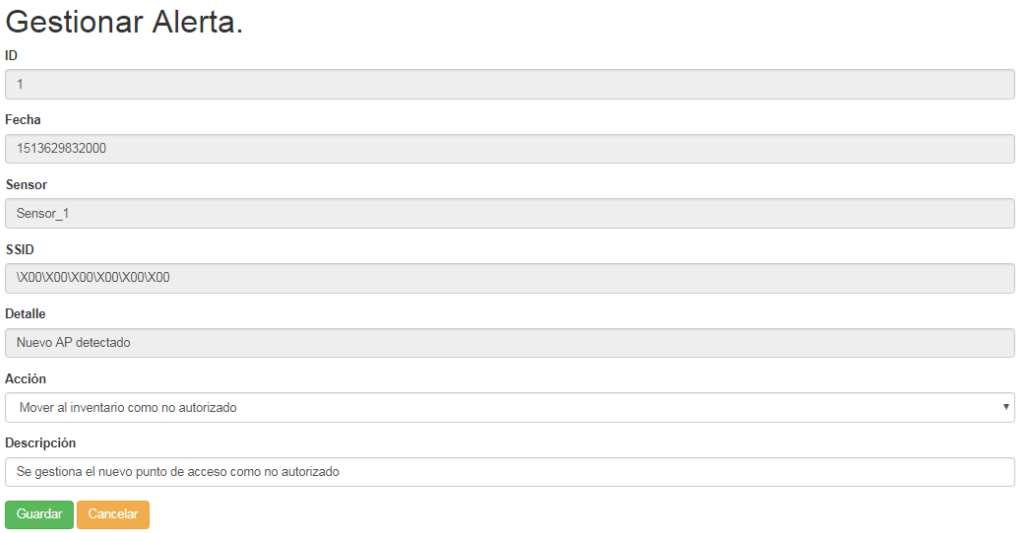


Figura 30: Pantalla del DAC-S donde se puede gestionar las alertas generadas como resultado del procesamiento de las señales inalámbricas detectadas por el sensor inalámbrico.

Fuente: Elaboración propia.

De la figura 31 a la figura 36 se puede visualizar algunos de los principales algoritmos que se utilizaron para implementar las funcionalidades del sistema DAC-S, como se visualiza a continuación:

```
USE gestor_db;

DROP FUNCTION IF EXISTS verify_clients;

DELIMITER $$
CREATE FUNCTION verify_clients(v_id_respositorio_ap bigint)
RETURNS VARCHAR(10)
BEGIN
    DECLARE done INT DEFAULT FALSE;
    DECLARE v_mac varchar(20);
    DECLARE v_count INT;
    DECLARE resultado varchar(10);

    DECLARE cur_rep_ap_cli CURSOR FOR
        SELECT mac FROM t_repositorio_cliente WHERE id_respositorio_ap = v_id_respositorio_ap;
    DECLARE CONTINUE HANDLER FOR NOT FOUND SET done = TRUE;


    SET resultado = '0';

    OPEN cur_rep_ap_cli;
    read_loop: LOOP
        FETCH cur_rep_ap_cli INTO v_mac;

        IF done THEN
          LEAVE read_loop;
        END IF;

        # verificar si el cliente AP_D estuvo conectado a un AP_I Miembro
        SELECT COUNT(1)
        INTO v_count
        FROM t_cliente tc, t_inventario ti
        WHERE tc.id_inventario = ti.id_inventario
        AND ti.classification = '1' AND tc.nombre = v_mac;

        IF v_count > 0 THEN
          SET resultado = '1';
        END IF;


    END LOOP;
    CLOSE cur_rep_ap_cli;



    RETURN resultado;
END $$
```

Figura 31: Código fuente de función desarrollada a nivel de base de datos, la cual permite determinar si un cliente que pertenece a un punto de acceso miembro se está conectado a un punto de acceso que no pertenece a esa categoría.

Fuente: Elaboración propia.

RespositorioAPService.java

```java
@Service
public class RespositorioAPService {

    @Autowired
    SensorRepository sensorRepository;

    @Autowired
    RepositorioAPRepository repositorioAPRepository;

    @Autowired
    ServicioClienteWS servicioClienteWS;

    public void getStatus() {

        try {
            String respuesta;

            //Obtiene el listado de sensores (activos y configurados).
            List<Sensor> listSensor = sensorRepository.findByStateAndConfiguredAndInventario("1", "1", EnumConstante.SENSOR_INVENTARIO_CLASIFICADO.getConstante());

            //Para cada sensor se solicita el status y se almacena el resultado en el repositorio.
            for (Sensor sensor : listSensor) {
                try {
                    respuesta = servicioClienteWS.sendMessage(sensor.getIp(), sensor.getPort(), UtilMessage.getSTATUSMessage(sensor));

                    JSONObject jsonObj = UtilMessage.convertToJSONObject(respuesta);
                    if("0".equals(jsonObj.get("CODE"))){
                        List<RepositorioAP> listRepositorioAP = UtilMessage.convertJsonToRespositorioAP(jsonObj, sensor);
                        // Guardar los Puntos de Acceso detectados
                        for (RepositorioAP objAP : listRepositorioAP) {
                            repositorioAPRepository.save(objAP);
                        }

                        sensor.setStatus(EnumConstante.SENSOR_STATUS_OK.getConstante());
                        sensor.setDateConn(new Date());
                        sensorRepository.save(sensor);
                    }else {
                        sensor.setStatus(EnumConstante.SENSOR_STATUS_FAIL_CONFIGURATION.getConstante());
                        sensorRepository.save(sensor);
                    }
                }catch (Exception e) {
                    sensor.setStatus(EnumConstante.SENSOR_STATUS_WITHOUT_COMMUNICATION.getConstante());
                    sensorRepository.save(sensor);
                    e.printStackTrace();
                }
            }

        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Figura 32: Código fuente de método desarrollado en Java con el que se puede verificar el estatus de los sensores, mediante este método se puede valorar si se genera una alerta por falta de conectividad o porque el sensor se encuentra desconfigurado.

Fuente: Elaboración propia.

```sql
USE gestor_db;
DROP PROCEDURE IF EXISTS sp_procesar_repo;

delimiter //
CREATE PROCEDURE sp_procesar_repo ()
BEGIN
    DECLARE done INT DEFAULT FALSE;

    # Variables ap detectado
    DECLARE v_apd_id_respositorio_ap, v_apd_id_sensor bigint(20);
    DECLARE v_apd_bssid, v_apd_frequency, v_apd_vendor VARCHAR(40);
    DECLARE v_apd_ssid VARCHAR(100);
    DECLARE v_apd_security VARCHAR(255);
    /*Variables inventario*/
    DECLARE v_api_id_sensor bigint(20);
    DECLARE v_api_ssid VARCHAR(100);
    DECLARE v_api_bssid, v_api_frequency, v_api_maker VARCHAR(40);
    DECLARE v_api_classification VARCHAR(20);

    DECLARE cur_rep_ap CURSOR FOR
        SELECT id_respositorio_ap, id_sensor, ssid, bssid, frequency, vendor, security FROM t_repositorio_ap WHERE state = '0';
    DECLARE CONTINUE HANDLER FOR NOT FOUND SET done = TRUE;

    OPEN cur_rep_ap;

    read_loop: LOOP
        FETCH cur_rep_ap INTO v_apd_id_respositorio_ap, v_apd_id_sensor, v_apd_ssid, v_apd_bssid, v_apd_frequency, v_apd_vendor, v_apd_security;

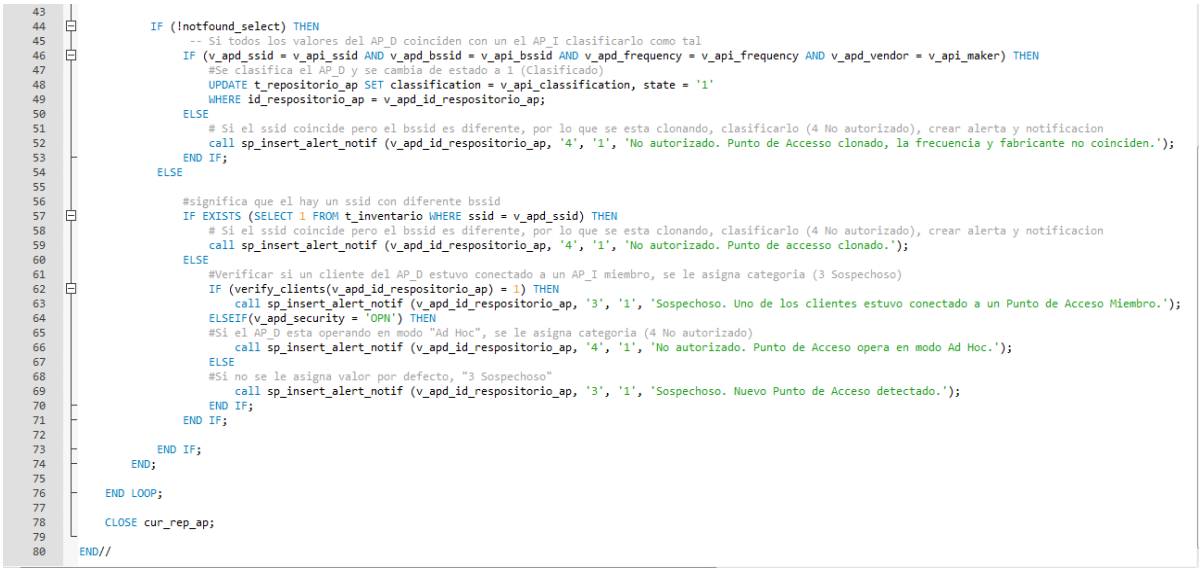
        IF done THEN
          LEAVE read_loop;
        END IF;

        /* Punto de Acesso Detectado (AP_D)
           Verificar si el AP_D se encuentra en el inventario */
        BEGIN
            DECLARE notfound_select INT DEFAULT FALSE;
            DECLARE CONTINUE HANDLER FOR NOT FOUND SET notfound_select = TRUE;

            SELECT id_sensor, ssid, bssid, frequency, maker, classification
            INTO v_api_id_sensor, v_api_ssid, v_api_bssid, v_api_frequency, v_api_maker, v_api_classification
            FROM t_inventario WHERE bssid = v_apd_bssid AND ssid = v_apd_ssid;
```

Figura 33: Detalle de código fuente de función de base de datos desarrollada para realizar la clasificación de los puntos de acceso una vez se haya cargado la información del inventario.

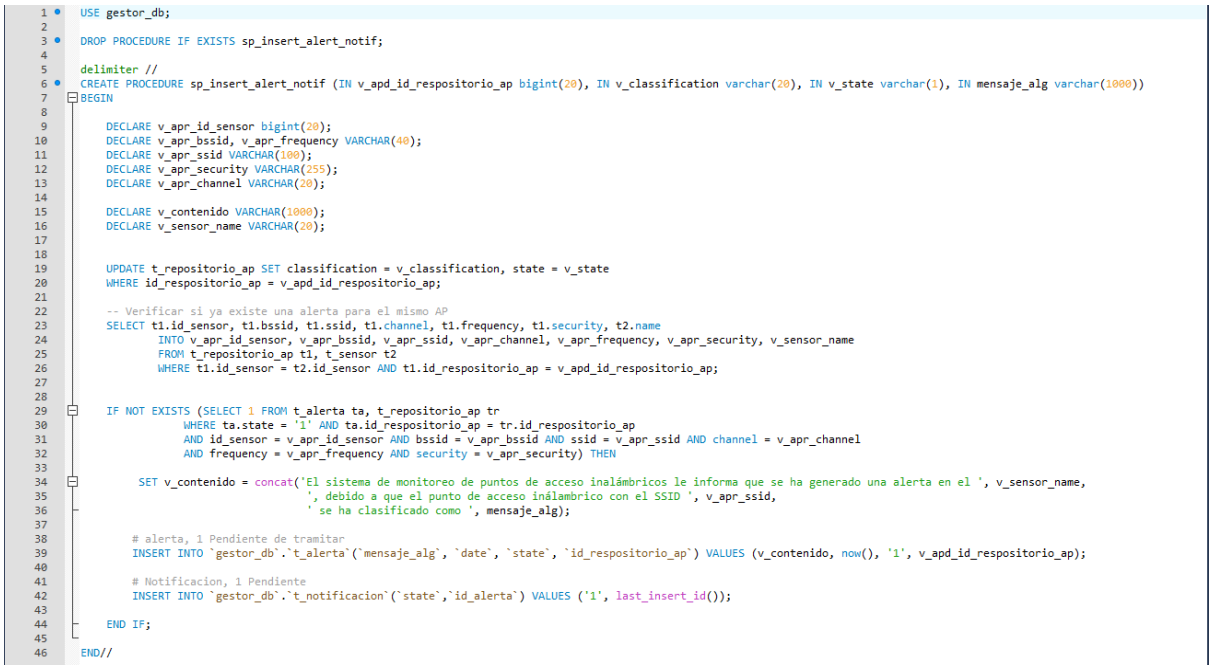
Fuente: Elaboración propia.



```
43
44          IF (!notfound_select) THEN
45                -- Si todos los valores del AP_D coinciden con un el AP_I clasificarlo como tal
46              IF (v_apd_ssid = v_api_ssid AND v_apd_bssid = v_api_bssid AND v_apd_frequency = v_api_frequency AND v_apd_vendor = v_api_maker) THEN
47                  #Se clasifica el AP_D y se cambia de estado a 1 (Clasificado)
48                  UPDATE t_repositorio_ap SET classification = v_api_classification, state = '1'
49                  WHERE id_respositorio_ap = v_apd_id_respositorio_ap;
50              ELSE
51                  # Si el ssid coincide pero el bssid es diferente, por lo que se esta clonando, clasificarlo (4 No autorizado), crear alerta y notificacion
52                  call sp_insert_alert_notif (v_apd_id_respositorio_ap, '4', '1', 'No autorizado. Punto de Accesso clonado, la frecuencia y fabricante no coinciden.');
53              END IF;
54           ELSE
55
56              #significa que el hay un ssid con diferente bssid
57              IF EXISTS (SELECT 1 FROM t_inventario WHERE ssid = v_apd_ssid) THEN
58                  # Si el ssid coincide pero el bssid es diferente, por lo que se esta clonando, clasificarlo (4 No autorizado), crear alerta y notificacion
59                  call sp_insert_alert_notif (v_apd_id_respositorio_ap, '4', '1', 'No autorizado. Punto de accesso clonado.');
60              ELSE
61                  #Verificar si un cliente del AP_D estuvo conectado a un AP_I miembro, se le asigna categoria (3 Sospechoso)
62                  IF (verify_clients(v_apd_id_respositorio_ap) = 1) THEN
63                      call sp_insert_alert_notif (v_apd_id_respositorio_ap, '3', '1', 'Sospechoso. Uno de los clientes estuvo conectado a un Punto de Acceso Miembro.');
64                  ELSEIF(v_apd_security = 'OPN') THEN
65                  #Si el AP_D esta operando en modo "Ad Hoc", se le asigna categoria (4 No autorizado)
66                      call sp_insert_alert_notif (v_apd_id_respositorio_ap, '4', '1', 'No autorizado. Punto de Acceso opera en modo Ad Hoc.');
67                  ELSE
68                  #Si no se le asigna valor por defecto, "3 Sospechoso"
69                      call sp_insert_alert_notif (v_apd_id_respositorio_ap, '3', '1', 'Sospechoso. Nuevo Punto de Acceso detectado.');
70                  END IF;
71              END IF;
72
73          END IF;
74      END;
75
76  END LOOP;
77
78  CLOSE cur_rep_ap;
79
80 END//
```

Figura 34: Detalle de código fuente de función de base de datos desarrollada para realizar la clasificación de los puntos de acceso una vez se haya cargado la información del inventario, segunda parte.

Fuente: Elaboración propia.



```
1  USE gestor_db;
2
3  DROP PROCEDURE IF EXISTS sp_insert_alert_notif;
4
5  delimiter //
6  CREATE PROCEDURE sp_insert_alert_notif (IN v_apd_id_respositorio_ap bigint(20), IN v_classification varchar(20), IN v_state varchar(1), IN mensaje_alg varchar(1000))
7  BEGIN
8
9      DECLARE v_apr_id_sensor bigint(20);
10     DECLARE v_apr_bssid, v_apr_frequency VARCHAR(40);
11     DECLARE v_apr_ssid VARCHAR(100);
12     DECLARE v_apr_security VARCHAR(255);
13     DECLARE v_apr_channel VARCHAR(20);
14
15     DECLARE v_contenido VARCHAR(1000);
16     DECLARE v_sensor_name VARCHAR(20);
17
18
19     UPDATE t_repositorio_ap SET classification = v_classification, state = v_state
20     WHERE id_respositorio_ap = v_apd_id_respositorio_ap;
21
22     -- Verificar si ya existe una alerta para el mismo AP
23     SELECT t1.id_sensor, t1.bssid, t1.ssid, t1.channel, t1.frequency, t1.security, t2.name
24             INTO v_apr_id_sensor, v_apr_bssid, v_apr_ssid, v_apr_channel, v_apr_frequency, v_apr_security, v_sensor_name
25             FROM t_repositorio_ap t1, t_sensor t2
26             WHERE t1.id_sensor = t2.id_sensor AND t1.id_respositorio_ap = v_apd_id_respositorio_ap;
27
28
29     IF NOT EXISTS (SELECT 1 FROM t_alerta ta, t_repositorio_ap tr
30                 WHERE ta.state = '1' AND ta.id_respositorio_ap = tr.id_respositorio_ap
31                 AND id_sensor = v_apr_id_sensor AND bssid = v_apr_bssid AND ssid = v_apr_ssid AND channel = v_apr_channel
32                 AND frequency = v_apr_frequency AND security = v_apr_security) THEN
33
34         SET v_contenido = concat('El sistema de monitoreo de puntos de acceso inalámbricos le informa que se ha generado una alerta en el ', v_sensor_name,
35                                  ', debido a que el punto de acceso inálambrico con el SSID ', v_apr_ssid,
36                                  ' se ha clasificado como ', mensaje_alg);
37
38         # alerta, 1 Pendiente de tramitar
39         INSERT INTO `gestor_db`.`t_alerta`(`mensaje_alg`, `date`, `state`, `id_respositorio_ap`) VALUES (v_contenido, now(), '1', v_apd_id_respositorio_ap);
40
41         # Notificacion, 1 Pendiente
42         INSERT INTO `gestor_db`.`t_notificacion`(`state`,`id_alerta`) VALUES ('1', last_insert_id());
43
44     END IF;
45
46 END//
```

Figura 35: Detalle del código fuente de función desarrollada a nivel de base de datos, la cual se encarga de analizar los datos del estatus del sensor y el inventario configurado y en caso de que detecte alguna anomalía genera las alertas y notificaciones correspondientes al administrador de la aplicación.

Fuente: Elaboración propia.

5.7 Plan de pruebas del funcionamiento de la solución en un ambiente controlado.

Según se definió en la sección de la metodología de la investigación, los escenarios de pruebas son limitados y no abarcan todas las posibilidades de condiciones y configuraciones a las que se puede enfrentar el sistema de monitoreo de puntos de acceso inalámbrico. En la metodología se definió que las pruebas se realizarán mediante escenarios de observación, los cuales serán ejecutados basándose en la configuración de red que se muestra en la figura 36, el cual fue creado con base en la experiencia profesional del grupo de investigación.

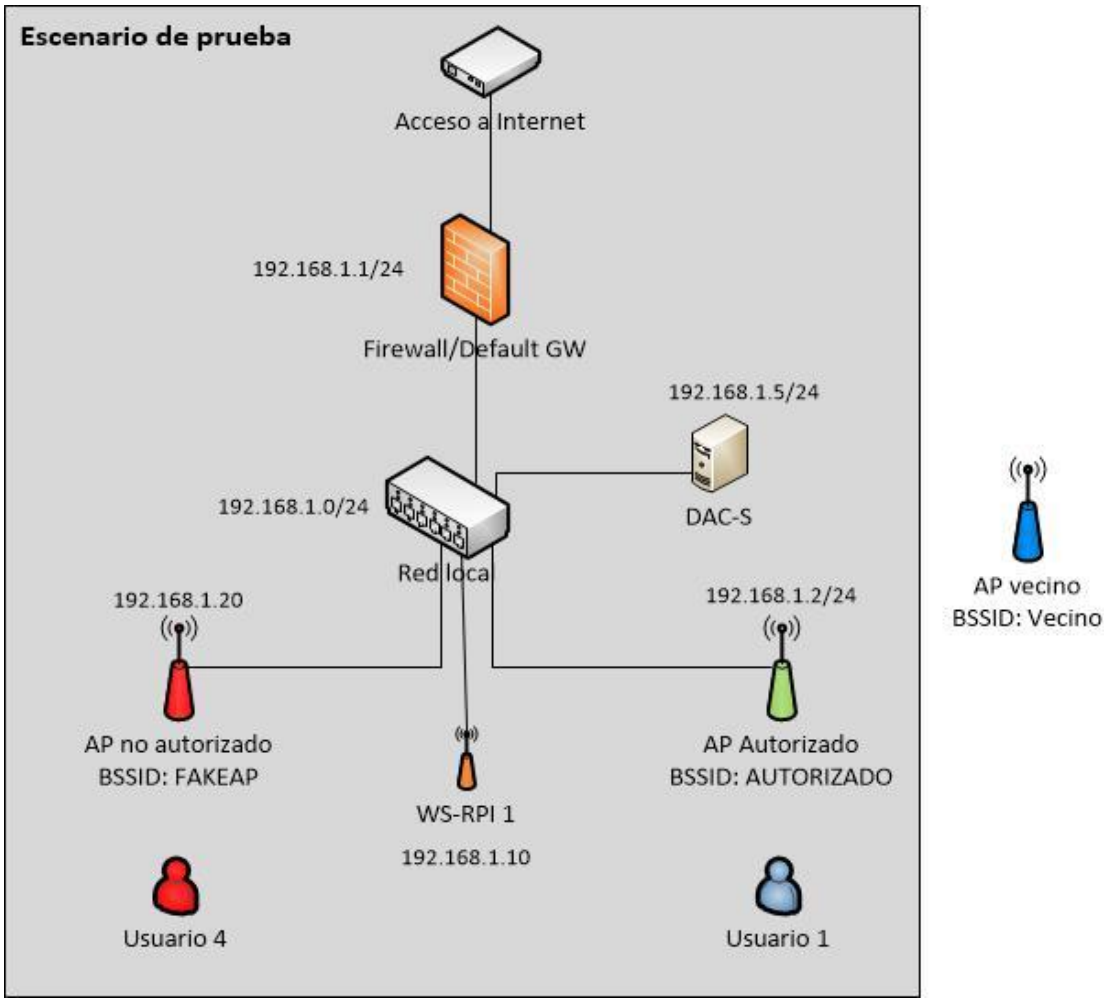


Figura 36: Diagrama de la configuración de red que se va a utilizar para ejecutar los guiones de observación de las pruebas.

Fuente: Elaboración propia.

5.7.1 Escenarios de observación y resultados

5.7.1.1 Escenario 1: Configurar dispositivo

Tabla 47: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de configurar el sensor inalámbrico.

Datos de entrada
• Usuario: admin • Contraseña: defaultAdmin • Puerto Gestor: 9001 • ETH0 Activa: Si • Dirección IP: 192.168.1.10 • Máscara de red: 255.255.255.0 • WLAN Activa: No • DHCP: Si
Escenario de observación
1. Se abre el navegador y se ingresa a la dirección 192.168.1.10:3000. 2. En la pantalla de inicio de sesión se ingresa el usuario y la contraseña. 3. Se oprime el menú “Configuración”. 4. Se ingresa los parámetros de configuración. 5. Se oprime el botón guardar. 6. Se reinicia el sensor. 7. Se verifica que la configuración se generó con éxito.
Resultados
• Resultado exitoso. • En el anexo 3 se puede visualizar el archivo de configuración generado por el dispositivo.

Fuente: Elaboración propia.

5.7.1.2 Escenario 2: Iniciar configuración

Tabla 48: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de iniciar configuración del sensor inalámbrico.

Datos de entrada
• Usuario: admin • Contraseña: defaultAdmin • Puerto Gestor: 9001

- ETH0 Activa: Si
- Dirección IP: 192.168.1.10
- Mascara de red: 255.255.255.0
- WLAN Activa: No
- DHCP: Si

Escenario de observación
1. Se desconecta la fuente de alimentación eléctrica del sensor. 2. Se vuelve a conectar la fuente de alimentación eléctrica del sensor 3. Se espera que el dispositivo encienda el indicador de configuración cargada con éxito. 4. Se verifica que la configuración de red del dispositivo sea la misma que se almacenó en el archivo de configuración".
Resultados
• Resultado exitoso. • En el anexo 4 y 5 se puede visualizar la luz indicadora del estado del sensor y la configuración del sensor una vez iniciada.

Fuente: Elaboración propia.

5.7.1.3 Escenario 3: Reiniciar a fábrica

Tabla 49: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de reiniciar a fábrica el sensor inalámbrico.

Datos de entrada
• No aplica.
Escenario de observación
1. Se inicia el sensor y se espera hasta que encienda la luz indicadora de que la configuración se cargó con éxito. 2. Se oprime el botón resetear durante 5 segundos hasta que la luz indicadora de configuración de fábrica empiece a parpadear. 3. Se reinicia el dispositivo. 4. Se verifica que el dispositivo inicie con la configuración por defecto que se indicó en el caso de uso 5.4.3.
Resultados
• Resultado exitoso. • En el anexo 6 y 7 se puede visualizar la luz indicadora de resetear a

configuración de fábrica y el estado de la configuración de red una vez inicia el dispositivo.

Fuente: Elaboración propia.

5.7.1.4 Escenario 4: Tomar inventario

Tabla 50: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de tomar inventario.

Datos de entrada
• Comando: {"CMD":"STOCK", "ID":"0001", "USER":"admin", "PASS":"defaultAdmin", "TOKEN":"000000", "TIME":"30"}. • Dirección IP del sensor: 192.168.1.10. • Puerto del websocket: 9001.
Escenario de observación
1. Se inicia el dispositivo y se espera hasta que la configuración se haya cargado con éxito. 2. Se abre una conexión del websocket 3. Se envía el comando con la sintaxis de los datos de entrada. 4. Se espera por la respuesta del sensor. 5. Se carga el contenido de la respuesta del sensor y se carga en una herramienta que verifique formato JSON, se valida que cumpla con lo establecido en el caso de uso 5.4.4.
Resultados
• Resultado exitoso. • En el anexo 8 se puede visualizar parte del contenido de la respuesta obtenida al enviar el comando de obtener estatus al sensor inalámbrico.

Fuente: Elaboración propia.

5.7.1.5 Escenario 5: Obtener estatus

Tabla 51: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de obtener estatus del sensor inalámbrico.

Datos de entrada
• Comando: {"CMD":"STATUS", "ID":"0001", "USER":"admin", "PASS":"defaultAdmin", "TOKEN":"000000"} • Dirección IP del sensor: 192.168.1.10. • Puerto del websocket: 9001.
Escenario de observación

1. Se inicia el dispositivo y se espera hasta que la configuración se haya cargado con éxito.
2. Se abre una conexión del websocket
3. Se envía el comando con la sintaxis de los datos de entrada.
4. Se espera por la respuesta del sensor.
5. Se captura el contenido de la respuesta del sensor y se carga en una herramienta que verifique formato JSON, se valida que cumpla con lo establecido en el caso de uso 5.4.5.

Resultados
• Resultado exitoso. • En el anexo 9 se puede visualizar parte del contenido de la respuesta obtenida al enviarle el comando de obtener estatus al sensor inalámbrico.

Fuente: Elaboración propia.

5.7.1.6 Escenario 6: Envío de notificaciones

Tabla 52: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de envío de correos mediante el módulo de notificaciones.

Datos de entrada
• Servidor de correo: mail.google.com • Dirección de correo: alertas.smpana@gmail.com • Puerto: 25 TCP/IP. • Título: Notificación de alarma en Sensor 1. • Contenido: Se notifica que el Sensor 1 ha generado una nueva alerta debido a que se detectó la señal de un punto de acceso inalámbrico sospechoso. • Dirección destino: juretana1@gmail.com.
Escenario de observación
1. Se inicia la tarea programada que envía las notificaciones del DAC-S. 2. En la cola de notificaciones se carga la información de la notificación, con los datos de entrada definidos previamente. 3. Se espera que se ejecute la tarea programada que envía las notificaciones. 4. Se verifica que el resultado de enviar la notificación haya sido “Enviada exitosa”. 5. Se verifica en el correo destinatario que la notificación se recibió correctamente.

Resultados
• Resultado exitoso. • En el anexo 10 se puede visualizar el detalle de la notificación que se recibió por parte del módulo de envió de notificaciones.

Fuente: Elaboración propia.

5.7.1.7 Escenario 7: Agregar sensor inalámbrico

Tabla 53. Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de agregar sensor inalámbrico en el DAC-S.

Datos de entrada
• Comando: {"CMD":"CONFIG", "ID":"0001", "IP":"192.168.1.5", "PORT":"5000", "USER":"admin", "PASS":"defaultAdmin", "TOKEN":"ABCRDE48747", "SENSOR_NAME":"SENSOR_1"}. • Nombre sensor: Sensor_1. • Usuario: admin. • Contraseña: defaultAdmin. • Dirección IP: 192.168.1.10. • Puerto: 9001.
Escenario de observación
1. Se ingresa en el DAC-S y se oprime el botón “Agregar WS-RPI”. 2. En el formulario de agregar el sensor se ingresa la información definida en los datos de entrada. 3. Se oprime el botón “Agregar”. 4. Se verifica que el DAC-S muestre un mensaje de confirmación de que el sensor se agregó correctamente.
Resultados
• Resultado éxito. • En el anexo 11 y 12 se puede visualizar las imágenes con el detalle del procesamiento de agregar un sensor inalámbrico en el DAC-S.

Fuente: Elaboración propia.

5.7.1.8 Escenario 8: Obtener información del inventario.

Tabla 54: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de obtener inventario del sensor inalámbrico desde el DAC-S.

Datos de entrada

- Tiempo: 30 minutos.
- Confiabilidad: >=10%.
- Puntos de acceso(SSID): Vecino y Autorizado.
- Sensor: Sensor_1(192.168.1.10).
- Comando: {"CMD":"STOCK", "ID":"0001", "USER":"admin", "PASS":"defaultAdmin", "TOKEN":"000000", "TIME":"30"}

Escenario de observación

1. Se ingresa a la interfaz de gestión del DAC-S.
2. Se ingresa a la opción de listado de sensores inalámbricos configurados.
3. Se selecciona el sensor 1 y se oprime el botón obtener inventario.
4. Se ingresa a la pantalla con el formulario de obtener inventario, en el tiempo y valor de confiabilidad se coloca los valores indicados en los datos de entrada.
5. Se espera por la respuesta del sensor.
6. Se verifica que en el listado de puntos de acceso detectados por el sensor se muestren los SSID con el nombre “Autorizado” y “Vecino”.

Resultados

- Resultado exitoso.
- En el anexo 13 se puede visualizar la pantalla del DAC-S con el resultado del inventario obtenido por el sensor 1.

Fuente: Elaboración propia.

5.7.1.9 Escenario 9: Obtener estatus del sensor.

Tabla 55: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de obtener estatus del sensor inalámbrico desde el DAC-S.

Datos de entrada

- Comando: {"CMD":"STATUS", "ID":"0001", "USER":"admin", "PASS":"defaultAdmin", "TOKEN":"000000"}.
- Sensor: Sensor_1.
- Puntos de acceso en inventario(SSID): Vecino y Autorizado.
- Punto de acceso desconocido(SSID): FakeAp.

Escenario de observación

1. Se inicia la tarea programada del DAC-S que se encarga de solicitar estatus al sensor.

2. Se envía el comando con solicitud de estatus al sensor inalámbrico.
3. Se espera por la respuesta del sensor inalámbrico.
4. Se verifica que en el listado de puntos de acceso inalámbricos detectados por el sensor vengan los que se identifican con el nombre “Vecino”, “Autorizado” y “FakeAp”.

Resultados

- Resultado exitoso.
- En el anexo 14 se puede visualizar la respuesta del sensor inalámbrico en formato JSON cuando se le envió el comando de obtener estatus.

Fuente: Elaboración propia.

5.7.1.10 Escenario 10: Clasificar las señales del inventario.

Tabla 56: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de clasificar las señales del inventario desde el DAC-S.

Datos de entrada

- Señales: Obtenidas en el guion 8, puntos de acceso identificados con los nombres “Vecino” y “Autorizado”.

Escenario de observación

1. Se ingresa a la interfaz de gestión del DAC-S.
2. Se ingresa en la opción de listado de sensores inalámbricos configurados.
3. Se selecciona el sensor 1 y se oprime el botón “Inventario”.
4. Se verifica que el DAC-S liste en el inventario la información de los puntos de acceso identificados con el nombre “Vecino”, “Autorizado” y que se encuentren en el estado no clasificados.
5. Para el punto de acceso identificado con el nombre “Vecino” se selecciona la clasificación “Vecino”.
6. Se guarda la configuración.
7. Se verifica que el sistema despliegue mensaje de confirmación indicando que la configuración se realizó con éxito.
8. Para el punto de acceso identificado con el nombre “Autorizado” se selecciona la clasificación “Miembro”.
9. Se guarda la configuración.
10. Se verifica que el sistema despliegue mensaje de confirmación indicando que la configuración se realizó con éxito.

Resultados
• Resultado exitoso. • En el anexo 15 y 16 se puede visualizar el listado de señales en inventario y la clasificación que se le asignó a cada una en el DAC-S.

Fuente: Elaboración propia.

5.7.1.11 Escenario 11: Procesar estatus de las señales.

Tabla 57: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de procesar señales inalámbricas obtenidas de los sensores.

Datos de entrada
• Señales: Obtenidas en el guion 8, puntos de acceso identificados como inventario con los nombres “Vecino” y “Autorizado”. • Señales: Obtenidas en el guion 9, puntos de acceso identificados con el estado del sensor con los nombres “Vecino”, “Autorizado” y “FakeAp”. • Clasificación asignada en el guion de observación 10, donde el punto de acceso identificado como “Vecino” se le asigna categoría de vecino, y el punto de acceso identificado como “Autorizado” se le asigna la categoría de miembro.
Escenario de observación
1. Se verifica que el inventario y estatus del sensor devuelvan los datos indicados en el guion de observación 8 y 9. 2. Se verifica que las señales del inventario posean la clasificación indicada en el guion de observación 10. 3. Se espera que se ejecute la tarea programada que solicita estatus de señales inalámbricas al sensor y realiza el análisis de las mismas. 4. Se verifica que el algoritmo de procesamiento no genere ninguna alerta para la señal del punto de acceso identificado como “Autorizado”. 5. Se verifica que el algoritmo de procesamiento no genere ninguna alerta para la señal del punto de acceso identificado como “Vecino”. 6. Se verifica que el algoritmo de procesamiento genere una alerta para la señal del punto de acceso identificado como “FakeAp”. 7. Se verifica que el DAC-S envié notificación al administrador del DAC-S vía correo electrónico indicando que se ha generado una nueva alerta.
Resultados

- Resultado exitoso.
- En el anexo 17 y 18 se puede visualizar la pantalla de alertas del DAC-S, donde se verifica que la señal identificada con el nombre “FakeAp” fue considerada como sospechosa por el algoritmo que procesa los datos de las señales. Además, se muestra el detalle de la notificación que recibió el administrador del DAC-S.

Fuente: Elaboración propia.

5.7.1.12 Escenario 12: Atender alertas pendientes de resolver

Tabla 58: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad atender alertas generadas por el DAC-S en el procesamiento de señales inalámbricas.

Datos de entrada
• Listado de alertas generadas en el guion de observación 11. • Las alertas generadas se les asigna la categoría de “Mover al inventario como no autorizado”.
Escenario de observación
1. Se ingresa a la interfaz de gestión del DAC-S. 2. Se oprime la opción “Listado de alertas”. 3. Se espera para que el sistema despliegue el listado de alertas que ha generado el DAC-S. 4. Para cada una de las alertas se procesa con la opción “Mover al inventario como no autorizado”. 5. Se oprime el botón guardar. 6. Se verifica que el DAC-S muestre un mensaje indicando que la configuración fue guardada con éxito. 7. Se verifica que en el listado de las alertas no aparezca ninguna pendiente de tramitar.
Resultados
• Resultado exitoso. • En el anexo 19 y 20 se puede visualizar el estado de las alertas generadas una vez que fueron atendidas, así como la información de los puntos de acceso que fueron ingresados al inventario como consecuencia de las alertas que fueron procesadas.

Fuente: Elaboración propia.

5.7.1.13 Escenario 13: Graficar dispositivo en el plano.

Tabla 59: Tabla con los datos de entrada y pasos a seguir para verificar la funcionalidad de graficar dispositivos en el plano.

Datos de entrada
• Detalle del sensor ingresado en el guion de observación 7.
Escenario de observación
1. Se ingresa a la página principal de la interfaz de gestión del DAC-S. 2. Se verifica que en el plano se grafique el WS-RPI identificado como “WS-RPI _1”. 3. Se coloca el cursor sobre el icono del sensor. 4. Se verifica que aparezca información del WS-RPI así como los menús de visualizar inventario y alertas.
Resultados
• Resultado exitoso. • En el anexo 21 se puede visualizar la información del sensor graficado en el plano del DAC-S.

5.8 Discusión de resultados

Después de ejecutar los escenarios de pruebas con los que se pretende corroborar el correcto funcionamiento de la aplicación, se puede verificar que se encuentra acorde con lo que se especificó en los casos de uso y se cumple con la mayoría de las funcionalidades de soluciones comerciales que se encuentran actualmente en el mercado.

Tanto el DAC-S como el WS-RPI se lograron construir con las tecnologías de código abierto que se establecieron en capítulos anteriores de la investigación, no obstante, cabe recalcar que no fue una tarea fácil, especialmente con la Raspberry PI y las herramientas recolectoras de datos, pues dicho dispositivo utiliza arquitectura de procesador ARM 7 para la cual no se encuentran disponibles los controladores de la tarjeta inalámbrica que se utilizó y lo cual implicó al grupo de

investigación buscar los códigos fuentes del fabricante y recompilar los controladores para esa arquitectura en específico; una vez superado este obstáculo los resultados obtenidos al momento de realizar el escaneo de señales inalámbricas fue bastante satisfactorio.

Por otra parte, en el sensor se logró implementar otras funcionalidades como el inicio de configuración automatizado, interfaz de gestión, luces indicadoras y botón resetear, que si bien es cierto no están relacionadas directamente con la seguridad de la información, son sumamente útiles para que se convierta en una solución escalable y amigable, capaz de ser utilizada y mejorada por el grupo de investigación u otras personas en un futuro. Adicionalmente, se logró demostrar como un dispositivo cómo la Raspberry PI los cuales se empiezan a popularizar debido a la tendencia de las tecnologías del internet de las cosas puede ser utilizado como un elemento que ayuda a proteger la seguridad de la información. Una limitante que se encontró en este dispositivo es que no se mostró robusto ante el exceso de procesamiento, pues en varias ocasiones durante la investigación se tuvo que realizar optimizaciones en la forma como se procesaban los datos, debido a que genera alarmas asociadas al umbral de temperatura máxima.

De igual forma el DAC-S se logró desarrollar utilizando las tecnologías de código abierto propuestas en otras secciones de la investigación, el cual logró demostrar ser una aplicación fácil de usar y capaz de procesar la información de las señales recolectadas como se definió en los casos de uso. Si bien es cierto, por una cuestión de tiempo se documentó un conjunto de pruebas muy limitadas, el grupo de investigación ejecutó otros escenarios que permitió verificar el correcto funcionamiento del algoritmo de procesamiento de señales inalámbricas en condiciones como cuando un punto de acceso clona la información de un punto de

acceso miembro, un equipo que se conectó a un punto de acceso miembro luego se conectó a un punto de acceso vecino, sospecho o no autorizado, cuando un punto de acceso trabaja en modo Ad-hod y utilizando varios sensores, entre otros. Si bien es cierto el objetivo principal de la investigación estaba orientado a la seguridad de la información en redes inalámbricas, con el desarrollo del software del DAC-S se pudo poner en práctica otros conocimientos adquiridos en los cursos de maestría, como diseño y arquitectura de soluciones seguras, comunicaciones seguras, cifrado de información, certificados de seguridad, análisis de vulnerabilidades, entre otros.

Finalmente, aunque se logró cumplir con los objetivos del proyecto, el grupo de investigación considera que nuevas funcionalidades pueden ser desarrolladas en trabajos futuros; ya sea por el mismo equipo de trabajo o terceros que quieran participar en una comunidad de colaboración, de tal forma que la aplicación adquiera la robustez y escalabilidad necesarias para que se pueda utilizar a gran escala e inclusive pueda competir con soluciones que se encuentran actualmente en el mercado.

Capítulo 6. Conclusiones y recomendaciones

- A pesar de que existen muchas arquitecturas para soluciones de monitoreo de puntos de acceso inalámbrico no autorizado, se concluye que las principales opciones son el análisis de paquetes a nivel de red y análisis de señales inalámbricas mediante sensores.
- Las soluciones de monitoreo mediante análisis de paquetes son más baratas, las que se basan en el análisis de señales inalámbricas son más efectivas, especialmente cuando se trata de puntos de acceso no autorizados que no están conectados directamente a la red que se desea proteger.
- Los dos elementos fundamentales que conforman una solución de monitoreo de puntos de acceso inalámbrico no autorizados basado en el análisis de señales son: el sensor inalámbrico(WS-RPI) y el controlador(DAC-S). Mientras el primero recolecta información de señales que tiene a su alcance, el segundo realiza el análisis de los datos de forma centralizada.
- Se logró demostrar que dispositivos asociados al internet de las cosas como la Raspberry PI son muy escalables y pueden ser utilizados en muchas aplicaciones (incluyendo seguridad de la información). El hecho de que posea un conjunto de pines que pueden ser utilizados como entrada o salida de señales análogas y digitales es una característica adicional que la da mayor adaptabilidad.
- Tecnologías de código abierto como MySql, NodeJS, Python y Java son opciones robustas con las que se puede crear gran cantidad de aplicaciones sin ningún tipo de limitación debido a su condición de ser de uso libre. Para el caso de la investigación fueron capaces de cumplir con todos los requerimientos establecidos.

- La herramienta Airmong-ng demostró ser un elemento de software importante para poder realizar escaneo y análisis de señales inalámbricas, si bien es cierto las configuraciones necesarias son más complejas que las de herramientas como iw y iwlist, fue más eficaz para obtener información de los clientes conectados a los puntos de acceso inalámbrico que se están analizando.
- Mediante la investigación se logró comprobar que una solución como la desarrollada requiere un amplio conocimiento acerca de seguridad de la información, el cual implica conocimientos en áreas como redes inalámbricas, diseño y desarrollo de aplicaciones seguras, arquitectura de seguridad, cifrado de información, comunicaciones seguras, buenas prácticas de administración de dispositivos, entre otros. Temas que fueron fortalecidos en el grupo de investigación como consecuencia del trabajo realizado.
- La solución desarrollada demostró ser eficaz y eficiente en el monitoreo y detección de puntos de acceso inalámbricos no autorizados, todos los escenarios de prueba ejecutados en el ambiente controlado fueron exitosos, inclusive en las pruebas adicionales que se realizaron y que no estaban especificadas en el documento de investigación.
- Durante la ejecución de los escenarios de pruebas se logró determinar que depurar correctamente el inventario es un factor fundamental para el correcto funcionamiento de las soluciones de monitoreo que se basan en el análisis de señales inalámbricas, especialmente en ambientes muy cargados de puntos de acceso inalámbricos como edificios, universidades, centros comerciales, entre otros; debido a que la fluctuación en las señales es muy fuerte, generando falsos positivos de forma frecuente cuando se está iniciando la implementación de la solución.

- Se recomienda implementar en futuras mejoras de la aplicación funcionalidades independientes al monitoreo, las cuales permitan anular con métodos como inyección de paquetes puntos de acceso que se hayan detectado como sospechosos o no autorizados, de esta manera sería más robusta y permitiría a los administradores de red tomar acciones correctivas de manera casi explícita.

Capítulo 7. Trabajos futuros

Si bien es cierto por una cuestión de tiempo y recursos la aplicación se orientó a que su principal funcionalidad fuera la detección y monitoreo de puntos de acceso inalámbrico, el grupo de investigación considera que es sumamente provechoso implementarle funciones de defensa en futuras versiones, en las cuales el dispositivo WS-RPI tome medias en tiempo real para deshabilitar la señal que emita puntos de acceso sospechosos o no autorizados mediante técnicas como inyección de paquetes.

Adicionalmente, aunque se logró alcanzar los objetivos planteados en la investigación dentro del alcance establecido, existe un compromiso del grupo de investigación en documentar a nivel técnico el proyecto y publicarlo en sitios relacionados con el uso de tecnologías de información, código abierto y Raspberry PI, para que sirva como punto de referencia a personas que quieran aprender del tema o realizarle mejoras; de esta manera se lograría que el proyecto de investigación genere impacto académico a nivel internacional en un futuro.

Glosario de términos

- **Ad-hoc:** En las redes de comunicación, puntualmente redes inalámbricas, se denomina red ad hoc a aquella que no tiene un nodo central, ya que todos los dispositivos están en condiciones de igualdad.
- **Amenaza:** La posibilidad de que un evento, malintencionado o no, que podría dañar o poner en peligro un activo.
- **Análisis de tráfico de red:** Proceso de inferir información a partir de captura de los paquetes que viajan a través de la red.
- **Ataque de hombre en el medio:** Tipo de amenaza en que un atacante desvía o controla las comunicaciones entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.
- **BSSID (Basic Service Set Identifier):** es un identificador único, formado por la dirección MAC (6 bloques hexadecimales), del punto de acceso inalámbrico al que se conecte.
- **Capa 1:** La capa física, la más baja del modelo OSI, se encarga de la transmisión y recepción de una secuencia no estructurada de bits sin procesar a través de un medio físico.
- **Capa 3:** Es el tercer nivel del modelo OSI, llamada capa de red.
- **Capa de red:** Controla el funcionamiento de la subred, decidiendo qué ruta de acceso física deberían tomar los datos en función de las condiciones de la red, la prioridad de servicio y otros factores.
- **DAC-S:** Aplicación desarrollada como parte de los objetivos de la investigación, la cual es capaz de controlar los diferentes dispositivos WS-RPI, al mismo tiempo que analiza la información generada por estos y genera alertas a los

usuarios administradores cuando detecta un patrón anormal en las señales inalámbricas escaneadas.

- **Dbm:** Decibelio-milivatio, es una unidad de medida de potencia expresada en decibelios (dB) relativa a 1 milivatio (mW).
- **Dirección MAC:** Es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). MAC significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particular.
- **Firewall:** Es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
- **Protocolo 802.11:** El protocolo IEEE 802.11 es una tecnología de acceso a la red que permite proporcionar conectividad entre estaciones wireless e infraestructuras de red cableadas. Las especificaciones de este estándar proporcionan la base para los productos con redes inalámbricas que hacen uso de la marca Wi-Fi.
- **Puerta de enlace predeterminada:** Es el dispositivo o la computadora que sirve como enlace entre dos redes informáticas, es decir, es aquel dispositivo que conecta y dirige el tráfico de datos entre dos o más redes.
- **Puerta de ingreso trasera:** Una manera indocumentada de acceso a un programa, a un servicio en línea o a un equipo informático entero. Abre una brecha de seguridad, posibilitando la entrada de terceros. Se evitan así los mecanismos normales de autenticación.

- **RSSI (Received Signal Strength Indicator):** es una escala de referencia para medir el nivel de potencia de las señales recibidas por un dispositivo en las redes inalámbricas.
- **Segmento de red:** Es un sinónimo de LAN: es un conjunto de equipos (computadoras y periféricos) conectados en red.
- **Sensor de red inalámbrico:** Es un pequeño dispositivo, autónomo y distribuido físicamente, instalado para monitoreo, con la capacidad obtener información de su entorno, procesarla localmente, y comunicarla a través de enlaces inalámbricos hasta un nodo central de coordinación.
- **SOAP/XML (Simple Object Access Protocol/Extensible Markup Language):** es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.
- **SSID (Service Set Identifier):** es una secuencia de 0-32 octetos incluida en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. A menudo se le conoce como el nombre de la red.
- **Usuario malicioso:** Usuario con malas intenciones que intenta explotar vulnerabilidades en redes y sistema de información para llevar a cabo actos tipificados por ley como criminales.
- **Web Socket:** Es una tecnología que permite establecer un canal de comunicación bidereccional sobre un único socket TCP. Esta tecnología nace con el fin de satisfacer necesidades de comunicación entre navegadores y servidores Web también puede ser utilizado en cualquier otro tipo de arquitectura cliente servidor.
- **WS-RPI:** Wireless Sensor Raspberry PI, dispositivo desarrollado como parte de los objetivos de la investigación, el cual se instala en las diferentes ubicaciones

físicas que se desea monitorear y se encarga de recolectar datos de las señales inalámbricas que tiene al alcance, para posteriormente enviarlas al DAC-S.

Referencias bibliográficas

Aircrack-ng. (s.f.). Aircrack-ng. Recuperado el 01 de 12 de 2017, de https://www.aircrack-ng.org/

Ceria, S. (2001). Casos de Uso: Un método práctico para explorar requerimientos. Recuperado el 15 de 08 de 2017, de http://www-2.dc.uba.ar/materias/isoft1/2001_2/apuntes/CasosDeUso.pdf

Cisco Systems. (2014). Cisco Wireless Intrusion Prevention System. Recuperado el 15 de 08 de 2017, de www.cisco.com: https://www.cisco.com/c/en/us/products/collateral/wireless/adaptive-wireless-ips-software/data_sheet_c78-501388.pdf

Dhiman, D. (2014). WLAN Security Issues and Solutions. IOSR Journal of Computer Engineering.

Fluke Networks. (2012). AirMagnet Enterprise. Recuperado el 15 de 08 de 2017, de http://airmagnet.flukenetworks.com/assets/datasheets/AirMagnet_Enterprise_Datasheet.pdf

Ganesh B., B., Vidya S., D., & Siddharth A., P. (2012). Rogue Access Point Detection System in Wireless LAN. International Journal of Computer Technology and Electronics Engineering (IJCTEE).

Hamid, R. A. (2003). Wireless LAN: Security Issues and Solutions. SANS Institute Reading Room.

Hewlett-Packard. (05 de 2013). HP Mobility Security IDS/IPS System Series. Recuperado el 15 de 08 de 2017, de http://h17007.www1.hpe.com/docs/picasso/4AA2-9840ENW.pdf

Juniper Networks. (16 de 12 de 2016). Understanding Rogue Access Points. Recuperado el 15 de 08 de 2017, de https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/wireless-rogue-ap.html

Kuo, D. (s.f.). Hackster.io. Recuperado el 03 de 12 de 2017, de https://www.hackster.io/4808/push-button-sample-b7745e

Mongo DB. (s.f.). Mongo DB. Recuperado el 15 de 10 de 2017, de https://www.mongodb.com/

Naranjo Zeledon , L. (04 de 2017). Proyecto de Investigacion Aplicada 1 - La Revision de Literatura - Aparato Crítcio. San José, San José, Costa Rica.

Naranjo Zeledón, L. (04 de 2017). Proyecto de Investigación Aplicada 1 - Enfoque Alternativo. San José, San José, Costa Rica.

National Institute of Standards and Technology. (08 de 2006). Guide to Integrating Forensic Techniques into Incident Response . United States of America.

NetScoup Solutions. (s.f.). AirMagnet Enterprise. Recuperado el 15 de 08 de 2017, de http://enterprise.netscout.com/content/datasheet-airmagnet-enterprise

NetSpot Community. (s.f.). Qué es RSSI y su relación con una red Wi-Fi. Recuperado el 15 de 08 de 2017, de https://www.netspotapp.com/es/what-is-rssi-level.html

Node JS Foundation. (s.f.). Node JS. Recuperado el 14 de 10 de 2017, de https://nodejs.org/es/

Offensive Security. (s.f.). Kali Linux Penetration Testing Tools. Recuperado el 16 de 10 de 2017, de https://tools.kali.org/tools-listing

Open Web Application Security Project(OWASP). (31 de 08 de 2015). Man-in-the-middle attack. Recuperado el 13 de 08 de 2017, de https://www.owasp.org/index.php/Man-in-the-middle_attack

Oracle Corporation. (s.f.). MySql The world's most popular open source database. Recuperado el 15 de 10 de 2017, de https://www.mysql.com/

Oracle. (s.f.). Introducción a Java® SE Embedded en Raspberry Pi. Recuperado el 14 de 10 de 2017

PostgreSQL Global Development Group. (s.f.). PostgreSQL. Recuperado el 15 de 10 de 2017, de https://www.postgresql.org/

Python Software Foundation. (s.f.). Recuperado el 10 de 14 de 2017, de https://www.python.org/

Sachin R. , S., Sandeep P. , C., & Ajeet A. , G. (2013). Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN. International Journal of Advanced Research in Computer Science and Software Engineering.

Servicio Nacional de Capacitación y Empleo de Chile. (s.f.). Instrumentos de Evaluación. Recuperado el 10 de 10 de 2017, de http://www.sence.cl/601/articles-4777_recurso_10.pdf

Taghavi Zargar, S., Joshi, J., & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE COMMUNICATIONS SURVEYS & TUTORIALS.

Tecnología Educativa Unefa. (10 de 2012). SEMINARIO DE INVESTIGACIÓN- CAPÍTULO II y III. Recuperado el 15 de 08 de 2017, de https://tecnologiaeducativaunefa.files.wordpress.com/2012/10/capitulo-iii1.pdf

Telelink Company. (2013). rogue access point. Recuperado el 15 de 08 de 2017, de http://itsecurity.telelink.com/rogue-access-points/

The Internet Engineering Task Force (IETF). (11 de 1987). DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. Recuperado el 15 de 08 de 2017, de https://tools.ietf.org/html/rfc1035

The official Linux Wireless wiki. (s.f.). The official Linux Wireless wiki. Recuperado el 01 de 12 de 2017, de https://wireless.wiki.kernel.org/en/users/documentation/iw

Tourrilhes, J. (29 de 08 de 2008). Wireless Tools for Linux. Obtenido de https://hewlettpackard.github.io/wireless-tools/Tools.html

UNIVERSIDAD INTERAMERICANA PARA EL DESARROLLO. (2014). Técnicas e instrumentos de recolección de datos. Recuperado el 15 de 08 de 2017, de UNID - Repositorio de documentos digitales: http://brd.unid.edu.mx/recursos/Taller%20de%20Creatividad%20Publicitaria/TC03/lecturas%20PDF/05_lectura_Tecnicas_e_Instrumentos.pdf

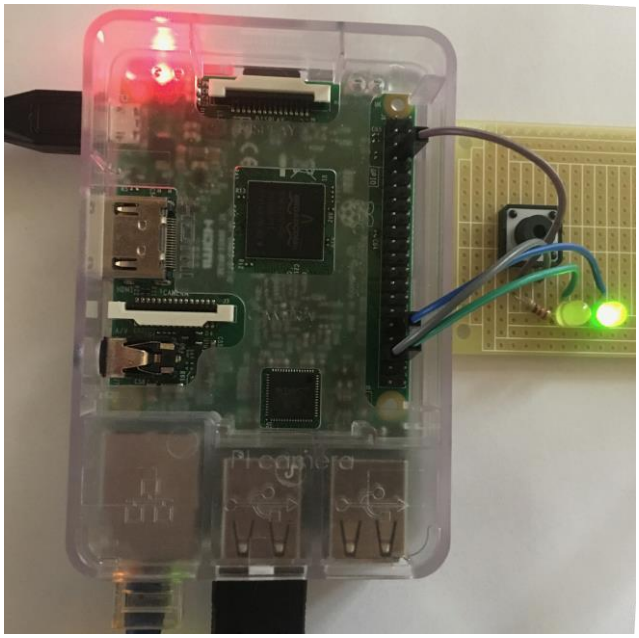
Wonder How To. (s.f.). Buy the Best Wireless Network Adapter for Wi-Fi Hacking in 2017. Recuperado el 26 de 09 de 2017, de https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2017-0178550/

Capítulo 8. Anexos

- **Anexo 1:** Fotografía del WS-RPI terminado y con la tarjeta inalámbrica conectada.



- **Anexo 2:** Fotografía de los elementos eléctricos del WS-RPI que conforman el botón resetear y las luces indicadoras soldados y conectados a los pines de la Raspberry PI.



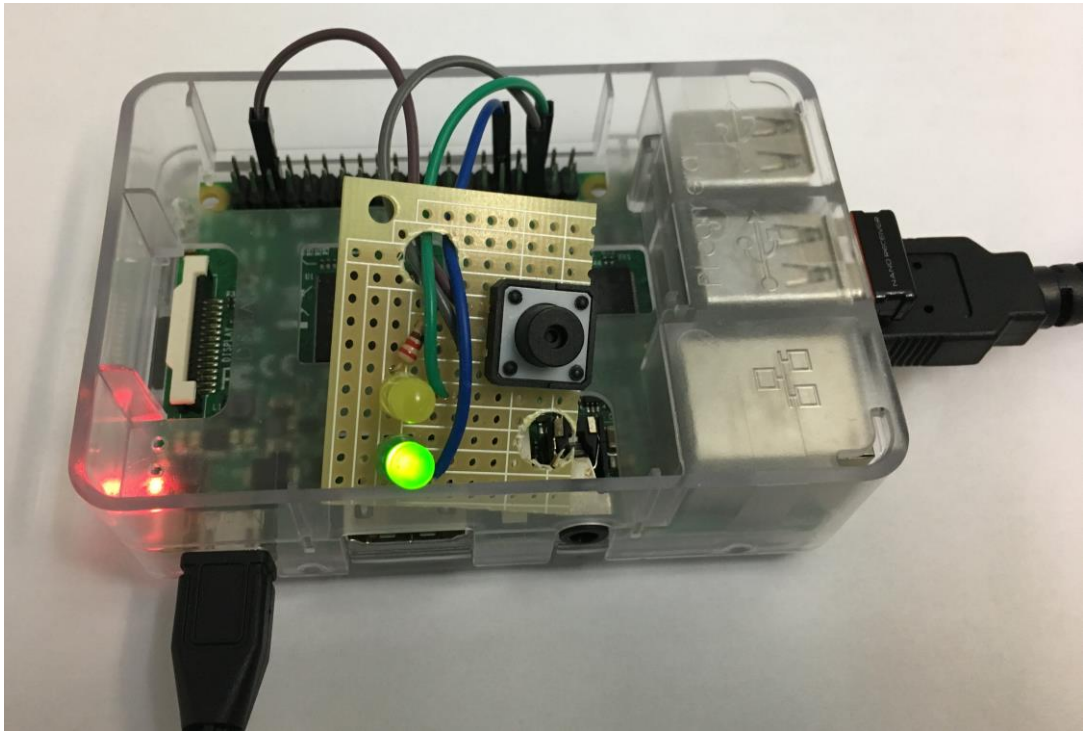
- **Anexo 3:** Archivo de configuración generado en el escenario de observación

```
root@raspberrypi:/cenfotec/config#
[admin]
user=admin
password=defaultAdmin
token=00000
sensor_name=Sensor
admin_port=9001

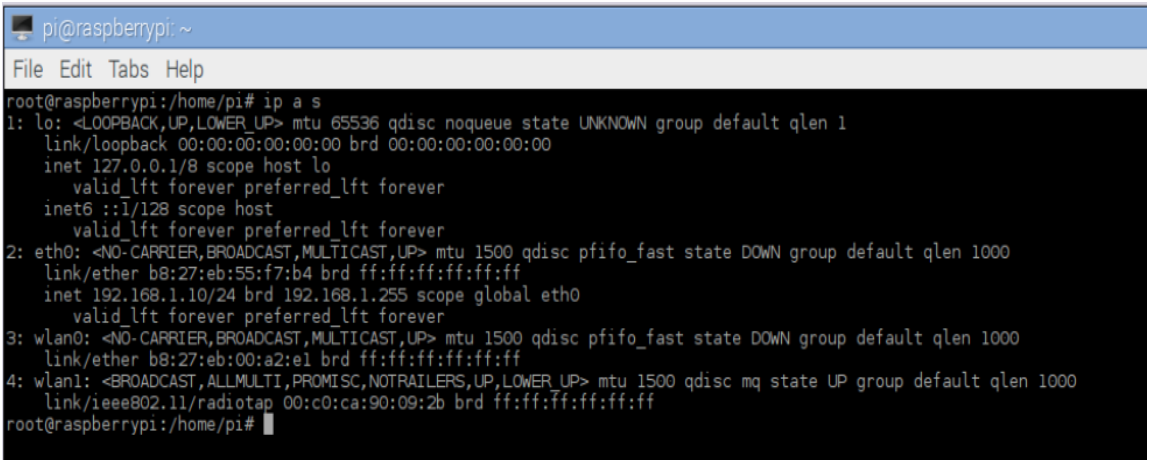
[controler]
controler_ip=
controler_port=
config=N

[network]
eth0_ip=192.168.0.1
eth0_enable=Y
eth0_dhcp=N
eth0_mask=255.255.255.0
eth0_gw=
wlan0_enable=N
wlan0_dhcp=
wlan0_ip=
wlan0_mask=
wlan0_gw=
wlan0_wl_nm=
wlan0_wl_pass=
```

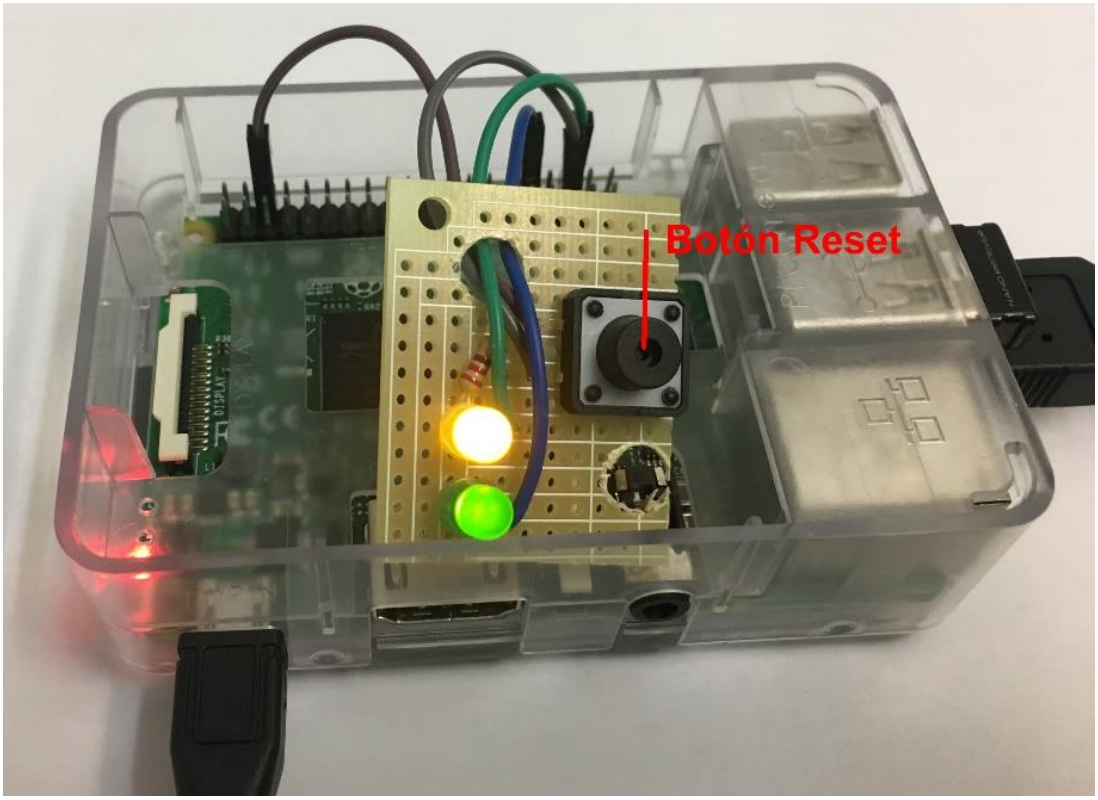
- **Anexo 4:** Luz indicadora de configuración cargada con éxito en el WS-RPI.



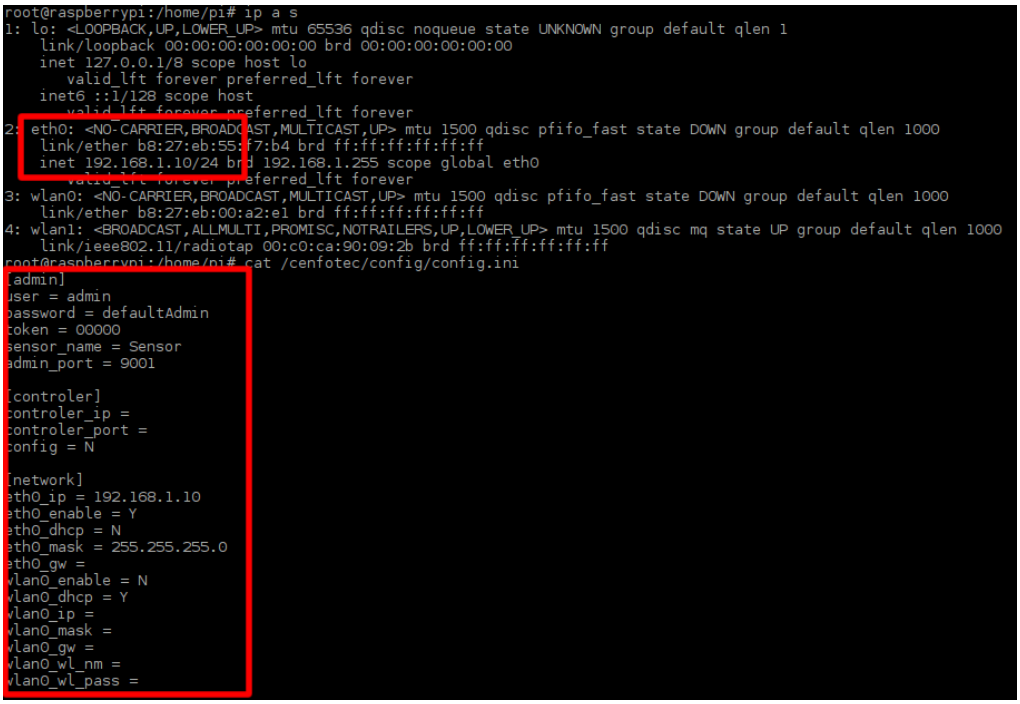
- **Anexo 5:** Estado de la configuración de red del WS-RPI una vez que toda la configuración fue cargada después de que se reinició el dispositivo.



- **Anexo 6:** Botón resetear y luz indicadora de que el proceso de configuración de fábrica ha iniciado.



- **Anexo 7:** Detalle de la configuración de red y archivo de configuración del dispositivo después de que se aplicó la configuración de fábrica.



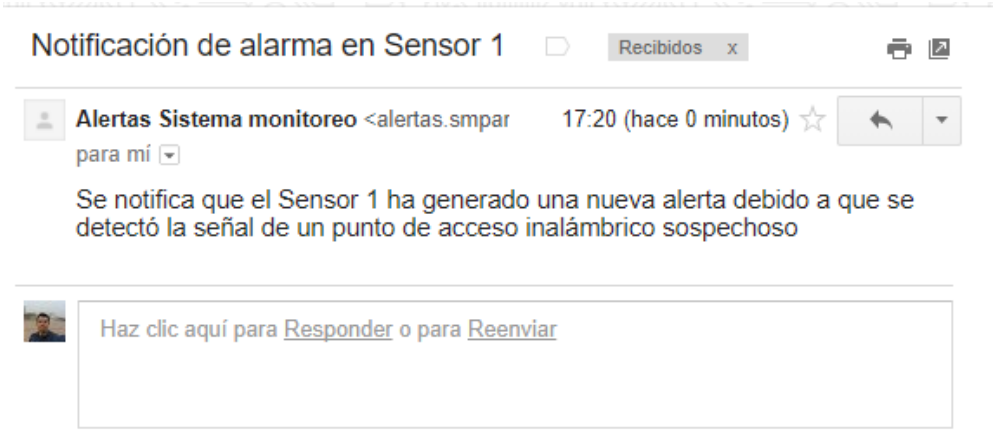
- **Anexo 8:** Detalle de los datos que devuelve el WS-RPI al enviarle comando de obtener el inventario.


```
"C-BSSID":[
    {
        "MAC":"6C:72:E7:11:1E:4E"
    },
    {
        "MAC":"B8:27:EB:00:A2:E1"
    },
    {
        "MAC":"C0:EE:FB:D9:EB:40"
    },
    {
        "MAC":"F8:DA:0C:5C:A9:C1"
    }
],
"VENDOR":"",
"SSID":"MALL_SP",
"BSSID":"48:F8:B3:20:7E:A6",
"READI":6,
"FREQ":"2.412",
"SECURITY":"WPA2 WPA"
```

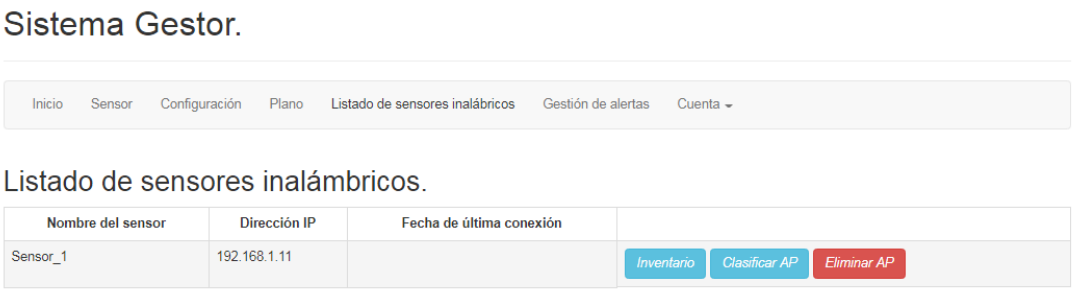
- **Anexo 9:** Detalle de los datos que devuelve el WS-RPI al enviarle comando de obtener estatus.


```
"C-BSSID":[
    {
        "MAC":"B8:27:EB:00:A2:E1"
    },
    {
        "MAC":"6C:72:E7:11:1E:4E"
    },
    {
        "MAC":"F8:DA:0C:5C:A9:C1"
    },
    {
        "MAC":"C0:EE:FB:D9:EB:40"
    }
],
"NOISE":-64,
"VENDOR":"",
"SSID":"MALL_SP",
"BSSID":"48:F8:B3:20:7E:A6",
"TOKEN":201712071845,
"SL":"46/70",
"SECURITY":"WPA2 WPA",
"FREQ":"2.412",
"CHANNEL":1
},
{...},
{...},
{...},
{...}
],
"CMD":"RESPONSE",
"CODE":"0",
"ID":"0001",
"DESCRIPTION":""
}
```


- **Anexo 10:** Detalle de la notificación recibida por el módulo de envió de notificaciones del DAC-S.



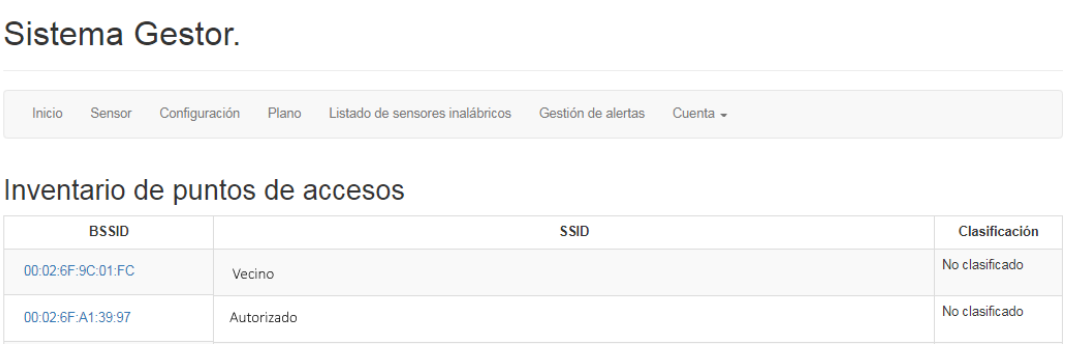
- **Anexo 11:** Detalle de la pantalla del DAC-S una vez que se ha configurado un WS-RPI.



- **Anexo 12.** Detalle de la configuración del WS-RPI una vez que se ingresó la configuración del DAC-S.



- **Anexo 13:** Pantalla del DAC-S donde se puede visualizar los resultados obtenidos en una solicitud de inventario al WS-RPI.



- **Anexo 14:** Estructura de datos devuelta por el WS-RPI cuando se le envía el comando de obtener estatus.


```
{
  "APS": [
    {
      "C-BSSID": [
      ],
      "NOISE":"1",
      "SSID":"Autorizado",
      "TOKEN":201712092010,
      "SL":"1",
      "SECURITY":"WPA2 WPA",
      "FREQ":"5.800",
      "CHANNEL":3
    },
    {
      "C-BSSID": [3],
      "NOISE":-85,
      "SSID":"FakeAp",
      "TOKEN":201712092010,
      "SL":"25/70",
      "SECURITY":"WPA2 WPA",
      "FREQ":"2.412",
      "CHANNEL":1
    },
    {
      "C-BSSID": [6],
      "NOISE":-28,
      "SSID":"Vecino",
      "TOKEN":201712092010,
      "SL":"70/70",
      "SECURITY":"WPA2 WPA",
      "FREQ":"2.412",
      "CHANNEL":1
    }
  ],
  "CMD":"RESPONSE",
  "CODE":"0",
  "ID":"0001",
  "DESCRIPTION":""
}
```


- **Anexo 15:** Pantalla donde se visualiza el inventario de puntos de acceso inalámbricos asociados al WS-RPI.

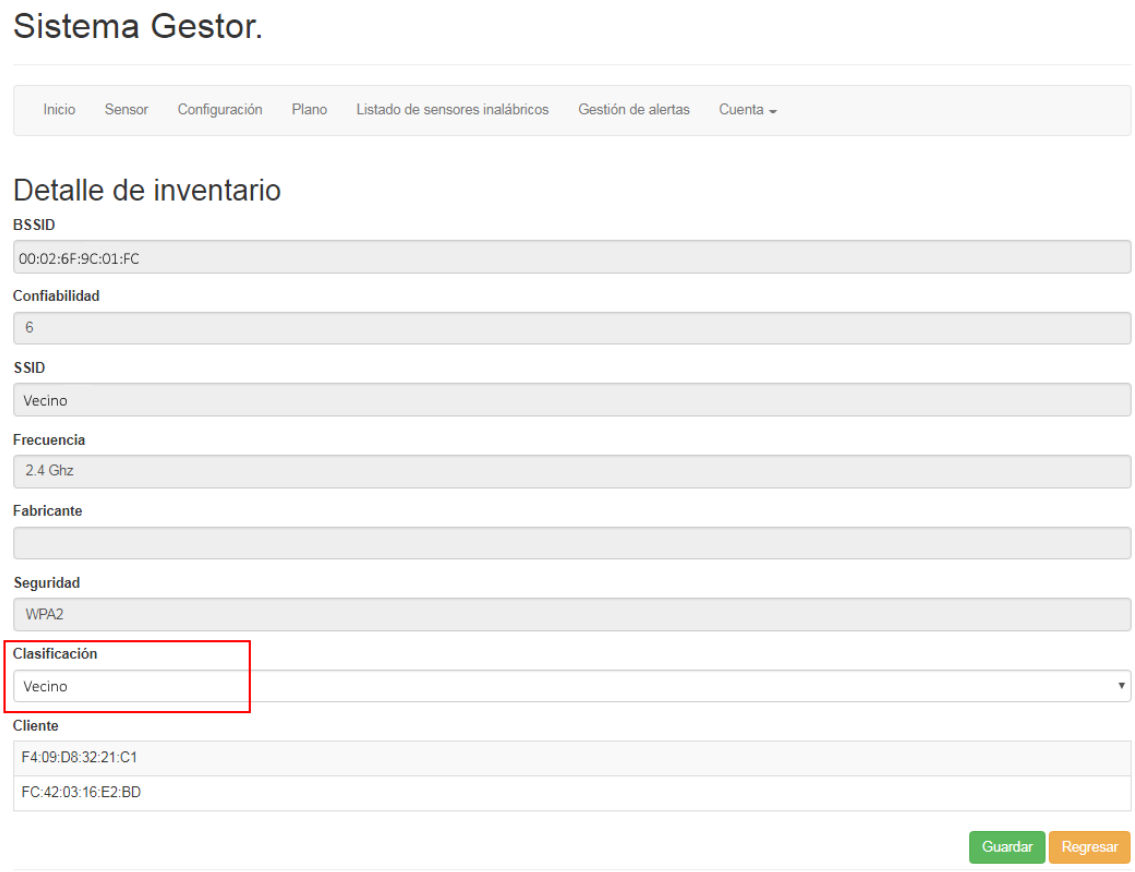
Sistema Gestor.

Inicio Sensor Configuración Plano Listado de sensores inalábricos Gestión de alertas Cuenta

Inventario de puntos de accesos

BSSID	SSID	Clasificación
00:02:6F:9C:01:FC	Vecino	Vecino
00:02:6F:A1:39:97	Autorizado	Autorizado

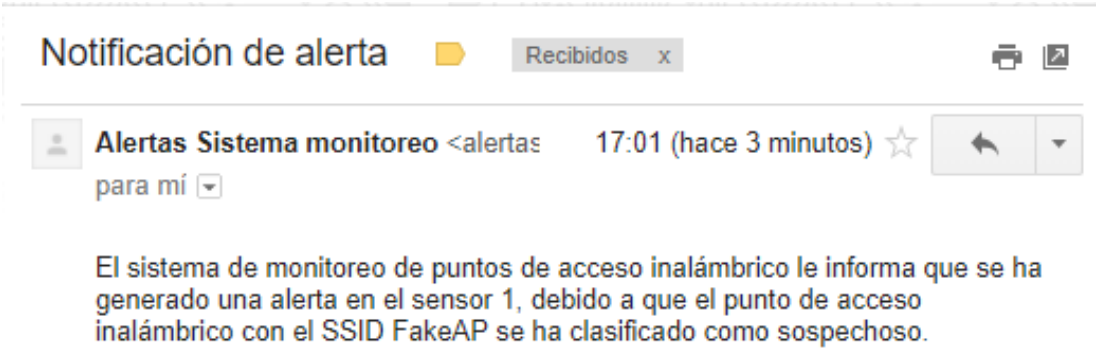
- **Anexo 16:** Pantalla donde se visualiza la clasificación que se le asignó a la señal del inventario.



- **Anexo 17:** Pantalla con el detalle de las alertas generadas en el DAC-S cuando se ejecuta el algoritmo que procesa los datos de las señales inalámbricas detectadas.



- **Anexo 18:** Detalle de la notificación recibida por el administrador del DAC-S cuando se genera una nueva alerta.



- **Anexo 19:** Detalle del listado de alertas en el DAC-S una vez que se han sido atendidas.



- **Anexo 20:** Detalle de señales ingresadas en el inventario como consecuencia de atender alertas generadas por el algoritmo de análisis de datos de señales inalámbricas.

