

Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Estudio de Cobertura para la Conectividad de Tótems de emergencia en el campus
Prosperina con el sistema Espol Alert

Proyecto Integrador

Previo la obtención del Título de:

Ingeniero en Telecomunicaciones

Presentado por:

Joyce Samira Ormaza Cali

Jesús Adrián Paredes Samaniego

Guayaquil - Ecuador

Año: 2023

Dedicatoria

El presente proyecto lo dedico a mis padres, cuya fortaleza y sabiduría han sido mi guía constante. Y de manera muy especial a mi mascota, Miley, mi fiel compañera, desde las largas horas de estudio hasta los breves pero significativos descansos, han sido iluminado por su compañía. Ella ha sido mi motivación constante, recordándome con cada gesto juguetón o mirada atenta, la importancia de la perseverancia y el disfrute de los simples momentos de la vida.

Joyce Ormaza Cali

El presente proyecto lo dedico a mi padre, cuyo apoyo incondicional ha sido fundamental para el cumplimiento de esta meta en esta nueva etapa de mi vida. A mi madre que, aunque ya no esté conmigo su esfuerzo y cariño han sido muy importantes a lo largo de toda mi carrera universitaria, a mi hermana y sobrino cuyas palabras fueron de gran aliento para no desistir, a mis amigos y compañeros con quienes compartí aulas a lo largo del trayecto, gracias a todos, han sido un pilar importante a lo largo de todo este camino.

Jesús Adrian Paredes

Agradecimientos

Mi más profundo agradecimiento al Ing. Félix Moncayo, por su invaluable orientación, paciencia y conocimientos. A mis profesores, gracias por su sabiduría y dedicación que han enriquecido mi formación. Un agradecimiento especial a mis padres, por su inquebrantable apoyo y confianza en mí. A mi compañero de proyecto, por su esencial colaboración. Finalmente, agradezco a mi líder en el trabajo, cuyo apoyo y enseñanzas han sido valiosos en mi desarrollo profesional.

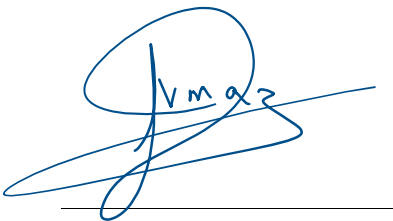
Joyce Ormaza Cali

Expreso mi agradecimiento a mis padres y familia cuyo apoyo y confianza depositada en mi ha sido muy importante para el cumplimiento de mis metas. Al Ingeniero Felix Moncayo por su calidez y orientación académica, al Ingeniero Jose Luis Asencio por haber asistido de manera oportuna todas las dudas presentadas en el desarrollo de este proyecto, a la ingeniera María Antonieta cuya retroalimentación ha sido de gran ayuda para el buen cumplimiento de nuestro proyecto integrador y a mis profesores por todos los conocimientos transmitidos a lo largo de los años, muchas gracias a todos.

Jesús Adrian Paredes

Declaración Expresa

“Los derechos de titularidad y explotación, nos corresponde conforme al reglamento de propiedad intelectual de la institución; Joyce Samira Ormaza Cali, y Jesús Adrián Paredes Samaniego damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”



Joyce Samira Ormaza
Cali



Jesús Adrián Paredes
Samaniego

Evaluadores

Ing. María Antonieta Alvarez Villanueva

Profesor de Materia

Ing. José Félix Moncayo Rea

Tutor de proyecto

Resumen

Este proyecto integrador se centra en mejorar la seguridad del campus Gustavo Galindo Velasco de la ESPOL mediante la implementación de tótems de emergencia conectados al sistema ESPOL ALERT. El objetivo es garantizar una comunicación efectiva y una respuesta rápida en situaciones críticas, aprovechando la tecnología de comunicación inalámbrica adecuada para una cobertura óptima. La justificación del proyecto radica en la necesidad de mejorar la seguridad en un campus de gran extensión geográfica, donde la conectividad efectiva es crucial para la gestión de emergencias.

Para el desarrollo, se realizaron estudios de cobertura utilizando herramientas como "Acrylic Wi-Fi Heatmaps" y "Wi-Fi Sweet Spots", evaluando la señal Wi-Fi en puntos estratégicos del campus. Se analizó la intensidad de la señal (RSSI), velocidad de datos y se utilizó la tecnología LoRaWAN para áreas de baja cobertura. Los resultados mostraron una variabilidad en la intensidad de la señal en diferentes áreas, resaltando la necesidad de optimizar la infraestructura de red existente y de implementar repetidores de señal en zonas clave.

Las conclusiones indican que la implementación de tótems de emergencia es viable tecnológica y económicamente, aprovechando la red Wi-Fi existente y mejorando la capacidad de respuesta a emergencias del sistema ESPOL Alert. Se recomienda una planificación detallada de la red Wi-Fi y la consideración de futuras expansiones y necesidades tecnológicas del campus.

Palabras Clave: Conectividad, Seguridad, Tótems de Emergencia, ESPOL ALERT, Cobertura Wi-Fi.

Abstract

This integrative project focuses on enhancing the safety of the Gustavo Galindo Velasco campus of ESPOL through the implementation of emergency totems connected to the ESPOL ALERT system. The aim is to ensure effective communication and rapid response in critical situations, leveraging suitable wireless communication technology for optimal coverage. The justification for the project lies in the need to improve security across a large geographical campus area, where effective connectivity is crucial for emergency management.

For development, coverage studies were conducted using tools like "Acrylic Wi-Fi Heatmaps" and "Wi-Fi Sweet Spots", assessing the Wi-Fi signal at strategic campus points. Signal strength (RSSI), data speed were analyzed, and LoRaWAN technology was used for low-coverage areas. The results showed signal intensity variability across different areas, highlighting the need to optimize existing network infrastructure and implement signal repeaters in key zones.

The conclusions indicate that the implementation of emergency totems is technologically and economically feasible, leveraging the existing Wi-Fi network and enhancing ESPOL Alert's emergency response capabilities. A detailed Wi-Fi network planning and consideration for future expansions and technological needs of the campus are recommended.

Keywords: *Connectivity, Security, Emergency Totems, ESPOL ALERT, Wi-Fi Coverage.*

INDICE

Resumen	I
Abstract	II
Abreviaturas	V
Simbología	VII
Índice de figuras	VIII
Índice de tablas	XII
Capítulo 1	1
1 Introducción	2
1.1 Descripción del Problema	2
1.2 Justificación del Problema	7
1.3 Objetivos	8
1.3.1 Objetivo general	8
1.3.2 Objetivos específicos.....	9
1.4 Marco Teórico	9
1.4.1 Comunicación inalámbrica.....	9
1.4.2 Red Wi-Fi.....	11
1.4.3 RSSI (Received Signal Strength Indicator).....	11
1.4.4 Tecnología LoRa (Long Range Radio)	12
1.4.5 Tótems de emergencia.....	17
1.4.6 Pérdida multipaso	17
Capítulo 2	19
2 Herramientas utilizadas para el estudio de cobertura de red institucional	20
2.1 Aplicación Wi-Fi SweetSpots	20
2.2 Aplicación Wi-Fi Analyzer (Open Source).....	22
2.3 Software Acrylic Wi-Fi Heatmaps	23

2.4	Ubicación de los puntos de encuentro y zonas estratégicas – Equipo Etrex Garmin.....	32
Capítulo 3		36
3	Identificación de mejor tecnología inalámbrica: ESP32 y Lora.	37
3.1	Comparativa de Cobertura Wi-Fi: Áreas Académicas vs. Espacios Abiertos	38
3.2	Evaluación de Cobertura Wi-Fi en puntos de encuentro.....	40
3.2.1	Puntos de encuentro con cobertura óptima de red.....	41
3.2.2	Puntos de encuentro sin cobertura óptima de red.....	42
3.3	Análisis de cobertura en zonas estratégicas	43
3.4	Implementación del ESP32 en la Red de Tótems de Emergencia	46
3.4.1	Configuración y Programación del ESP32 para Conectividad Wi-Fi.....	47
3.4.2	Estrategias de Seguridad y Protección de Datos para el ESP32 en la Red ESPOL	48
3.4.3	Transmisión de alertas de emergencia desde el ESP32 a ESPOL ALERT	49
3.4.4	Configuración de la Infraestructura en la Nube para Gestión de alertas de Tótems	50
3.5	Implementación de Lora en la red de Tótems de Emergencia	51
3.5.1	Estrategias de Seguridad y Protección de Datos para Lora en la Red ESPOL	52
3.5.2	Transmisión de alertas de Emergencia desde dispositivos Lora a ESPOL ALERT	53
3.6	Análisis de Costos para la Implementación Tecnológica.....	55
3.6.1	Costos de implementación para ESP32.....	56
3.6.2	Costos de implementación para LoraWan	58
3.6.3	Costo total implementación tótems de emergencia.....	60
Capítulo 4		62
4	Conclusiones y recomendaciones.....	63
4.1	Conclusiones	63
4.2	Recomendaciones.....	64
REFERENCIAS		66
APÉNDICES		70

Abreviaturas

ESPOL	Escuela Superior Politécnica del Litoral
RSSI	Received Signal Strength Indicator
Wi-Fi	Wireless Fidelity
IoT	Internet of Things.
LoRa	Long Range.
LoRaWAN	Long Range Wide Area Network.
TCP/IP	Transmission Control Protocol/Internet Protocol.
UBEP	Bienestar Estudiantil y Politécnico
CIB	Centro de Información Bibliotecario
FIEC	Facultad de Ingeniería en Electricidad y Computación
FIMCP	Facultad de Ingeniería en Mecánica y Ciencias de la Producción
FICT	Facultad de Ingeniería en Ciencias de la Tierra
CELEX	Centro de Lenguas Extranjeras
FCSH	Facultad de Ciencias Sociales y Humanísticas
FCNM	Facultad de Ciencias Naturales y Matemáticas
FADCOM	Facultad de Arte, Diseño y Comunicación Audiovisual
FIMCM	Facultad de Ingeniería Marítima Y Ciencias del Mar
FCV	Facultad de Ciencias de la Vida de la ESPOL
I3LAB	Centro de Emprendimiento e Innovación
QR	Quick Response
GPS	Sistema de Posicionamiento Global
TTN	The Things Network
WiMAX	Worldwide Interoperability for Microwave Access
FSK	Modulación por desplazamiento de frecuencia
CSS	Chirp Spread Spectrum
SSM	Spread Spectrum Modulation
FHSS	Frequency Hopping Spread Spectrum
API	Application Programming Interfaces
ISM	Industrial, Scientific and Medical
AM	Amplitud modulada

JSON	Java Script Object Notation
EUI	Entity Unique Identifier
AES	Advanced Encryption Standard
AWS	Amazon Web Services
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MQTT	Message Queuing Telemetry Transport
IEEE	Institute of Electrical and Electronics Engineers
PCAP	Packet Capture
IDE	Integrated Development Environment
GPIO	General Purpose Input/Output
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Simbología

dB	Decibelios
dBm	Decibel - milivatio
Bps	Bits por segundo
Mbps	Mega bits por segundo
Gbps	Giga bits por segundo
Mhz	Megahercios
Ghz	Gigahercios

Índice de figuras

Figura 1.1	3
<i>Vista del campus Gustavo Galindo en satélite (Google maps)</i>	3
Figura 1.2	4
<i>Modo de operación ESPOL ALERT</i>	4
Figura 1.3	5
<i>Modelo inicial de tótems de emergencia en el campus Gustavo Galindo</i>	5
Figura 1.4	6
<i>Localización de Puntos de encuentro (Google Maps)</i>	6
Figura 1.5	7
<i>Ubicación Zonas Estratégicas (Google Earth)</i>	7
Figura 1.5	9
<i>Tipos de comunicaciones inalámbricas</i>	9
Figura 1.6	10
<i>Red inalámbrica</i>	10
Figura 1.7	11
<i>Red Wi-Fi</i>	11
Figura 1.8	13
<i>Red LoRaWan</i>	13
Figura 1.9	15
<i>Arquitectura de red LoRaWan</i>	15
Figura 1.10	18
<i>Propagación multipaso en una red inalámbrica</i>	18
Figura 2.1	21
<i>Medición periódica de potencia de señal recibida y velocidad de datos utilizando la aplicación “Wi-Fi Sweet Spots”</i>	21

Figura 2.2	23
<i>Medición de intensidad de señal recibida y análisis de canales en Access points del campus</i>	
<i>Gustavo Galindo</i>	23
Figura 2.3	24
<i>Mapa de calor generado por el programa Acrylic Wi-Fi Heatmaps.....</i>	24
Figura 2.4	25
<i>Ingreso de mapa del área a analizar.</i>	25
Figura 2.5	26
<i>Calibración de planos en área a estudiar</i>	26
Figura 2.6	26
<i>Calibración del mapa por guía satelital.</i>	26
Figura 2.7	27
<i>Superposición de mapas en software Acrylic Wi-Fi Heatmaps</i>	27
Figura 2.8	28
<i>Escaneo en zona de interés</i>	28
Figura 2.9	28
<i>Barrido de muestras en mapa dentro del software</i>	28
Figura 2.10	29
<i>Mapa de calor (RSSI) generado por Acrylic Wi-Fi Heatmaps.</i>	29
Figura 2.11	30
<i>Mapa de calor visualizado en aplicación “Google Earth”</i>	30
Figura 2.12	31
<i>Rango de colores, intensidad máxima y mínima de señal recibida</i>	31
Figura 2.13	32
<i>Equipo de medición GPS Etrex.....</i>	32
Figura 3.1	39

<i>Pérdida de señal en áreas verdes</i>	39
Figura 3.2	39
<i>Pérdida de señal Wi-Fi en espacios abiertos.</i>	39
Figura 3.3	44
<i>Puntos estratégicos con cobertura alta o moderada</i>	44
Figura 3.4	53
<i>Plataforma TTN (The Things Network)</i>	53
Figura A1.....	71
<i>Mapa de cobertura Rectorado</i>	71
Figura A2.....	72
<i>Mapa de cobertura CIB</i>	72
Figura A3.....	73
<i>Mapa de cobertura CELEX</i>	73
Figura A4.1.....	74
<i>Mapa de cobertura FCSH</i>	74
Figura A4.2.....	75
<i>Mapa de cobertura FCSH (Edificio administrativo)</i>	75
Figura A5.....	76
<i>Mapa de cobertura FIMCP</i>	76
Figura A6.1.....	77
<i>Mapa de cobertura FIEC (Redes ESPOL, ESPOL Wi-Fi & Eduroam)</i>	77
Figura A6.2.....	78
<i>Mapa de Cobertura FIEC (Redes FIEC & FIEC Wireless)</i>	78
Figura A7.....	79
<i>Mapa de Cobertura FCNM</i>	79
Figura A8.....	80

<i>Mapa de Cobertura FICT</i>	80
Figura A9.....	81
<i>Mapa de Cobertura FADCOM</i>	81
Figura A10.....	82
<i>Mapa de Cobertura FIMCM</i>	82
Figura A11.....	83
<i>Mapa de Cobertura FCV</i>	83
Figura A12.....	84
<i>Mapa de Cobertura UBEP</i>	84
Figura A13.....	85
<i>Mapa de Cobertura I3LAB</i>	85

Índice de tablas

Tabla 1.1.....	16
<i>Comparación entre Wi-Fi, LoRaWan y SigFox.....</i>	<i>16</i>
Tabla 2.1.....	33
<i>Localización de puntos de encuentro Campus Gustavo Galindo</i>	<i>33</i>
Tabla 2.2.....	34
<i>Localización de puntos estratégicos Campus Gustavo Galindo</i>	<i>34</i>
Tabla 3.1.....	42
<i>Puntos de encuentro en zonas con cobertura alta o moderada</i>	<i>42</i>
Tabla 3.2.....	43
<i>Puntos de encuentro en zonas con cobertura baja o nula.....</i>	<i>43</i>
Tabla 3.3.....	44
<i>Puntos estratégicos con cobertura alta o moderada</i>	<i>44</i>
Tabla 3.4.....	57
<i>Costo inicial implementación ESP32</i>	<i>57</i>
Tabla 3.5.....	59
<i>Costo inicial implementación LoraWan.....</i>	<i>59</i>
Tabla 3.6.....	60
<i>Costo total implementación tótems de emergencia.....</i>	<i>60</i>

Capítulo 1

1 Introducción

El campus Gustavo Galindo Velasco, dada su extensa área geográfica, es susceptible a situaciones de emergencia. Para abordarlas de manera efectiva, se ha implementado el sistema de seguridad ESPOL ALERT, conectado a la central de alarmas ESPOL 911. Este sistema dispone de una aplicación y un sitio web, a través de los cuales se pueden reportar e ingresar diversas emergencias, incluyendo información detallada y localización específica.

Como medida de seguridad adicional se planifica la instalación de distintos tótems de emergencia, estos estarán ubicados en zonas previamente identificadas como puntos de encuentro entre facultades y senderos. Sin embargo, la conectividad de estos tótems es esencial para garantizar una respuesta inmediata en situaciones críticas. Este estudio se enfoca en evaluar la cobertura de red institucional en diversas ubicaciones y proponer soluciones para asegurar la conectividad de estos dispositivos de emergencia. Los resultados de esta investigación servirán como guía para una implementación efectiva de los tótems.

El objetivo principal de este estudio es evaluar la cobertura de la red institucional en diferentes ubicaciones de interés en el campus y proponer soluciones que garanticen la conectividad de los tótems de emergencia. Estas soluciones no solo fortalecerán el sistema ESPOL ALERT, sino que también desempeñarán un papel fundamental en la mejora de la seguridad y la capacidad de respuesta a situaciones críticas en nuestro campus.

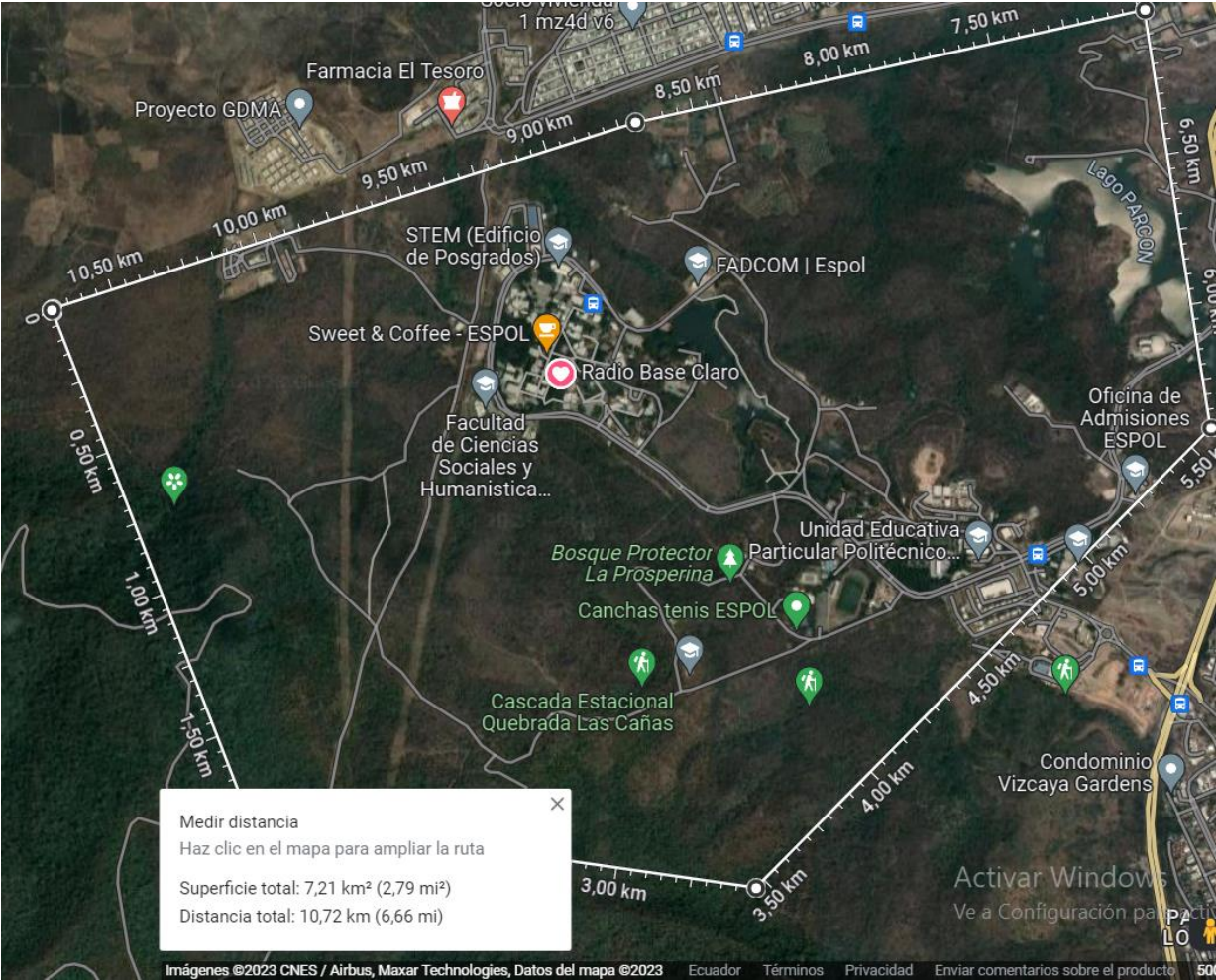
1.1 Descripción del Problema

El Campus Gustavo Galindo Velasco, perteneciente a la Escuela Superior Politécnica del Litoral (ESPOL), comprende una extensa área de 700 hectáreas, el 28%, que representan 200 hectáreas, han sido edificadas con aulas, áreas recreativas y administrativas; el 72% restante forma parte del Bosque Protector Prosperina [1].

La ESPOL cuenta con un sistema de monitoreo de seguridad llamado ESPOL 911, desde el mes de enero del año 2016, tiene la capacidad de coordinar y responder posibles emergencias dentro del Campus Gustavo Galindo Velasco.

Figura 1.1

Vista del campus Gustavo Galindo en satélite (Google maps)



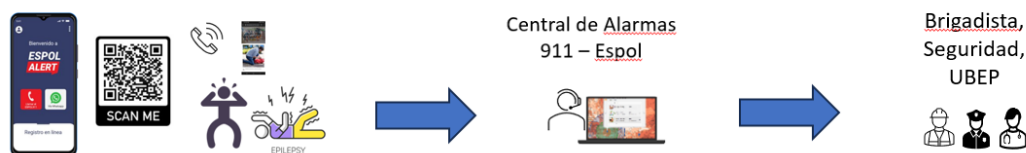
Nota. La figura muestra un estimado del área del campus Gustavo Galindo haciendo uso de herramientas de medición en Google Maps.

En la figura 1.1 se puede observar el campus Gustavo Galindo desde el satélite, utilizando herramientas de medición presentes en Google Maps se puede abarcar un área aproximada a las 700 hectáreas de extensión en la cual podemos notar una mayor proporción para el bosque protector Prosperina y áreas verdes en general.

En un esfuerzo por fortalecer la seguridad en el campus, se ha lanzado el proyecto institucional ESPOL ALERT en 2022. Este proyecto colabora con los brigadistas de ESPOL 911 y ofrece una aplicación web y móvil diseñada para proporcionar una alerta temprana y notificación de eventos de emergencia en tiempo real. En la figura 1.2 se puede observar el mecanismo de funcionamiento del sistema de alarma. Mediante la aplicación móvil los estudiantes y/o personal administrativo son capaces de reportar una emergencia en el campus a través de la plataforma, una vez ingresada la emergencia la central de alarmas de ESPOL 911 se encarga de notificar dicho evento y procede a enviar respuesta inmediata a través de un brigadista cercano al lugar de la emergencia.

Figura 1.2

Modo de operación ESPOL ALERT



Nota: La figura muestra el modo de operación para el reporte de una emergencia dentro del campus a través de la aplicación móvil, adaptado de ESPOL ALERT (2023).

Adicionalmente a la aplicación, también se desarrollan tótems de emergencia los cuales están ubicados estratégicamente alrededor de todo el campus, estos estarán ubicados en los puntos de encuentro de cada facultad y áreas estratégicas identificadas. Mediante estos tótems se puede reportar un incidente tanto de manera virtual a través del escaneo de un código QR como también de forma manual a través de un botón de pánico el cual envía los datos de la emergencia a la central de alarmas de ESPOL 911 con la localización de este para que un brigadista responda y acuda inmediatamente al lugar del siniestro. En la figura 1.3 se observa el diseño inicial de estos tótems de emergencia.

Figura 1.3

Modelo inicial de tótems de emergencia en el campus Gustavo Galindo



Nota. La figura muestra el contenido disponible para el uso del sistema ESPOL ALERT a través de un código QR. Adaptado de ESPOL ALERT (2023).

La problemática identificada es el estudio y análisis del método de comunicación más adecuado para garantizar la conectividad de estos tótems al sistema de ESPOL ALERT dentro del campus Gustavo Galindo Velasco, considerando factores geográficos y tecnológicos, para ser activados en cualquier momento cuando se suscite una emergencia, de esta forma la inmediata activación de dichos tótems brinda una respuesta más eficiente ante cualquier emergencia presentada.

El valor y la importancia del proyecto radican en realizar las consideraciones necesarias mediante el estudio de cobertura a fin de identificar propuestas adecuadas para la conectividad de los tótems de emergencia con la finalidad de mejorar la seguridad de la comunidad politécnica al asegurar una comunicación efectiva en situaciones de emergencia, fortaleciendo así el sistema ESPOL ALERT y proporcionando una guía para la implementación exitosa de estos dispositivos durante la fase de implementación del proyecto, de esta forma se tiene una base sólida para considerar el tipo de tecnología a utilizar y los posibles costos que conllevan cada uno de los mismos. De la misma forma, al tener una referencia acerca de la cobertura de red institucional se

pueden ubicar estratégicamente dichos dispositivos a fin de asegurar una comunicación de respuesta efectiva ante situaciones de emergencia.

Figura 1.4

Localización de Puntos de encuentro (Google Maps)



Nota: La figura muestra la localización de los puntos de encuentro alrededor del campus Gustavo Galindo, lugar tentativo de instalación de los tótems de emergencia.

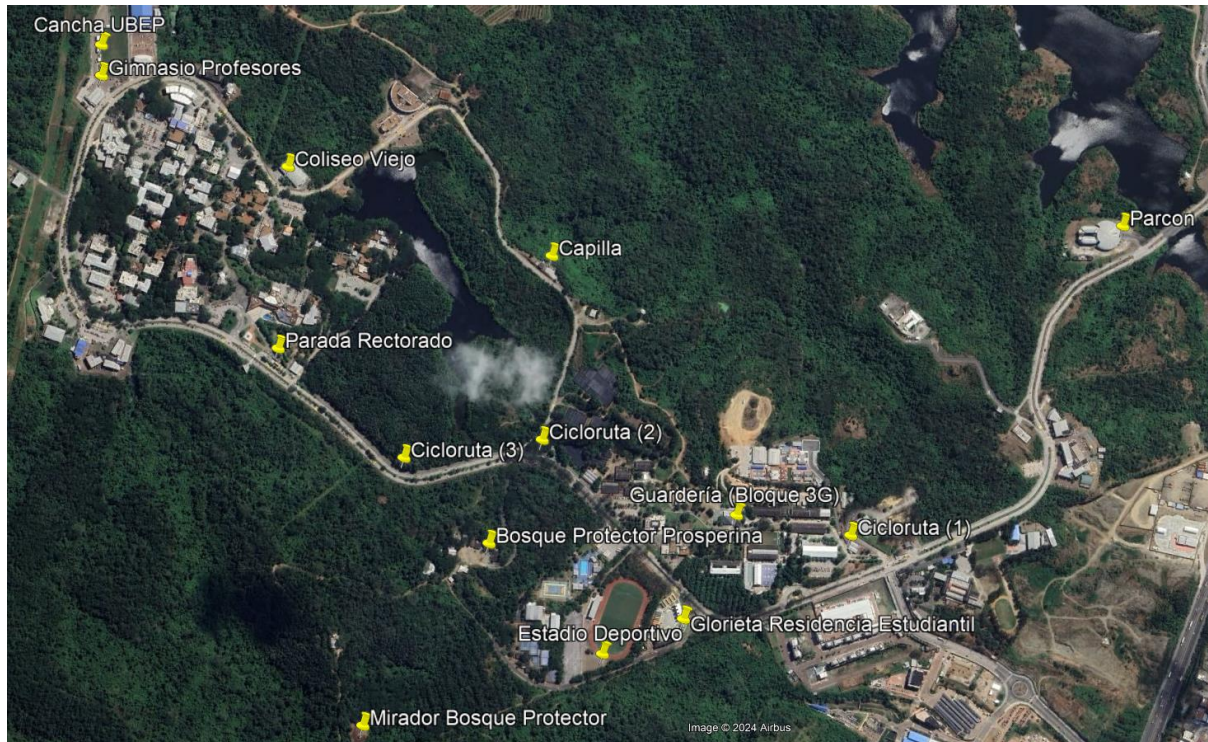
En la figura 1.4 se observa la localización de los distintos puntos de encuentro presentes en el campus Gustavo Galindo, dichos puntos sirven como referencia para la ubicación inicial de los tótems de emergencia donde dependiendo de la cobertura de red institucional se proponen posibles soluciones para la conectividad de cada uno de los mismos, analizando datos importantes como la velocidad de datos, RSSI, entre otros. Todo esto con la finalidad de garantizar una conexión estable a fin de evitar intermitencias en la comunicación de estos puntos.

Adicionalmente a los puntos de encuentro existen zonas de interés en las cuales se podrían ubicar equipos adicionales para abarcar una mayor cobertura de respuesta ante situaciones de emergencia, al estar ubicados en zonas periféricas del campus serán considerados a parte de los

puntos de encuentro que por lo general se encuentran en las zonas centrales del campus y facultades.

Figura 1.5

Ubicación Zonas Estratégicas (Google Earth)



Nota. La figura muestra la ubicación de los puntos estratégicos en zonas periféricas del campus Gustavo Galindo.

Como se puede observar en la figura 1.5 al estar ubicados en zonas alejadas del campus la cobertura en estas zonas es deficiente o nula razón por la cual se analizan estos puntos de manera independiente, sin embargo, existen pocos puntos que disponen de cobertura de red institucional, debido a esto debe realizarse un análisis de cada uno de los puntos mencionados.

1.2 Justificación del Problema

La conectividad de los tótems de emergencia con el sistema ESPOL ALERT es esencial para garantizar una respuesta eficaz a situaciones críticas que puedan surgir en el campus. En tales situaciones, la falta de conectividad presenta un problema pues puede poner en riesgo la vida de

las personas y los bienes, lo cual hace necesaria la implementación de una solución ante esta problemática.

El campus Gustavo Galindo Velasco comprende una amplia extensión, debido a esto es importante identificar ciertos puntos ciegos de conectividad donde podrían existir fallos de cobertura para la instalación de los tótems de emergencia, estos puntos seleccionados se escogen estratégicamente para brindar una mejor cobertura ante alguna emergencia a ser atendida por parte del sistema ESPOL ALERT.

El producto final del proyecto es un estudio que abarque propuestas para la conectividad de los tótems de emergencia en el campus Gustavo Galindo Velasco al sistema de ESPOL ALERT. Esto implica la definición de la mejor opción para comunicación inalámbrica dependiendo de la zona de ubicación del tótem, asegurando que sea apropiada para el entorno del campus. El estudio resultante comprende una propuesta completa de una red inalámbrica que incluirá la ubicación de distintos tótems en varios puntos de encuentro y áreas estratégicamente identificadas garantizando así la conectividad de los mismos con el sistema ESPOL ALERT.

El desarrollo de este estudio es importante además para definir un presupuesto que contemple los costos asociados a la implementación de la infraestructura necesaria para la conectividad de estos puntos. Este enfoque garantizará que la solución propuesta sea viable en términos prácticos, facilitando su implementación y mejorando de manera significativa la capacidad de respuesta a emergencias en ESPOL.

1.3 Objetivos

1.3.1 Objetivo general

Realizar el estudio de cobertura mediante la selección y aplicación de la tecnología de comunicación inalámbrica más adecuada, considerando puntos de ubicación estratégicos para la

conectividad de los tótems de emergencia en el Campus Gustavo Galindo Velasco con el sistema ESPOL ALERT.

1.3.2 Objetivos específicos

- Identificar la tecnología de comunicación inalámbrica más adecuada para la conectividad efectiva de los tótems de emergencia al sistema ESPOL ALERT.
- Evaluar zonas estratégicas para abarcar mayor cobertura de respuesta y comunicación fiable durante situaciones de emergencia a través de la recopilación de datos relevantes que incluyen detalles topográficos del terreno, características de la vegetación circundante y evaluación de cobertura de red institucional.
- Realizar un análisis presupuestario que englobe los dispositivos esenciales requeridos para la conectividad de los tótems de emergencia en el campus Gustavo Galindo Velasco al sistema ESPOL ALERT mediante la recolección de información de proveedores que ofrezcan los componentes necesarios para la implementación de la red de sensores inalámbricos.

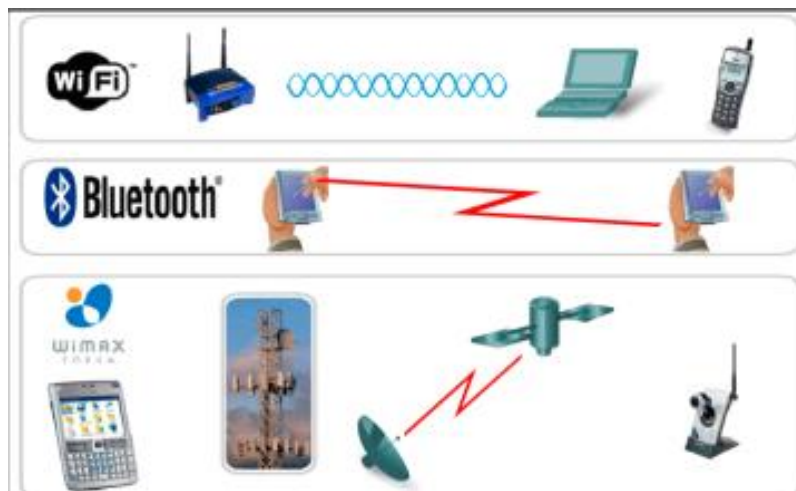
1.4 Marco Teórico

1.4.1 Comunicación inalámbrica

La comunicación inalámbrica se caracteriza por prescindir de un medio de propagación físico para transmitir información. En lugar de depender de conductores físicos, este enfoque se basa en la modulación de ondas electromagnéticas que se propagan a través del espacio sin requerir un soporte material. En este contexto, los únicos componentes físicos presentes son el dispositivo emisor y el dispositivo receptor, tales como antenas, computadoras portátiles, teléfonos móviles y otros dispositivos similares [2].

Figura 1.6

Tipos de comunicaciones inalámbricas



Nota. La figura muestra distintos tipos de enlaces inalámbricos dependiendo de cada tecnología de información (Wi-Fi, Bluetooth, Wimax, etc)

Una red inalámbrica, si bien posee similitudes con las redes físicas convencionales, se distingue por su capacidad de enlazar dispositivos sin recurrir a la infraestructura de cables o medios guiados. Este principio se ilustra en la Figura 1.6. La categorización de una red inalámbrica se basa en sus radios de cobertura y su rango de frecuencia, y estas características permiten su clasificación y diferenciación. [3]

Figura 1.7

Red inalámbrica



Nota. La figura muestra una red inalámbrica básica donde varios dispositivos pueden anclarse a un punto de acceso.

1.4.2 Red Wi-Fi

Una red Wi-Fi representa la convergencia de una infraestructura de comunicación fija con dispositivos que funcionan de manera inalámbrica, tal como se ejemplifica en la Figura 1.7. Esto posibilita el acceso a Internet y la comunicación entre diversos dispositivos sin necesidad de cables. La conectividad de los dispositivos a Internet se logra mediante la conexión a un punto de acceso inalámbrico, comúnmente conocido como "router," lo que permite la conexión de los dispositivos a la red designada.[4]

Figura 1.8

Red Wi-Fi



Nota. La figura muestra varios equipos comunicándose inalámbricamente a través de tecnología Wi-Fi.

1.4.3 RSSI (Received Signal Strength Indicator)

Como sus siglas lo denotan, RSSI hace mención a la indicación de fuerza de señal recibida es una medida de la potencia de señal en radiofrecuencia detectado por un dispositivo terminal (teléfono móvil, ordenador, dispositivo Wi-Fi). Se expresa generalmente en decibelios lo cual proporciona información sobre la potencia de la señal en dicho punto, un valor RSSI negativo indica una señal débil mientras que un valor alto es representado por números positivos o cercanos a 0.

1.4.4 Tecnología LoRa (Long Range Radio)

LoRa hace referencia a la capa física de la modulación inalámbrica que permite establecer enlaces de largo alcance. Esta tecnología utiliza una técnica de modulación basada en espectro ensanchado, similar a la modulación por desplazamiento de frecuencia (FSK), y una variante del espectro de dispersión de chirrido (CSS) para modular datos a través de diferentes canales y velocidades. Esto asegura que no haya interferencias mutuas, creando un conjunto virtual de canales. Como resultado, la capacidad del Gateway (puerta de enlace) se incrementa. Además, esta técnica incluye mecanismos de corrección de errores y opera mediante la activación periódica de los dispositivos para conservar la energía de manera eficiente [5].

LoRaWAN se ha diseñado para satisfacer las demandas de la Internet de las cosas, como la necesidad de comunicación a larga distancia, eficiencia energética y capacidad de comunicación bidireccional para la conectividad de dispositivos [5]. Esta tecnología inalámbrica emplea una modulación de radiofrecuencia específica (ilustrada en la Figura 1.5). Lo que la distingue es su capacidad para resistir las interferencias, ofrecer un alcance de cobertura significativo de 10 a 20 kilómetros y, al mismo tiempo, mantener un consumo de energía reducido, lo que le permite funcionar de manera efectiva durante largos períodos de tiempo.[6]

Hay 3 clases de dispositivos terminales Lora, clase A, B y C con características importantes cada uno tales como:

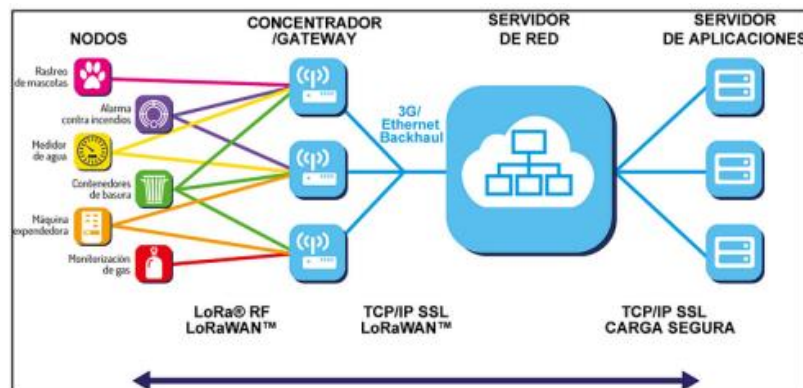
- **Clase A:** Es el más eficiente en términos de consumo de energía, ofrece espacios para downlink después de transmitir un mensaje, al utilizar 2 ventanas de recepción con un tiempo de escucha limitado es ideal para enlaces que solo requieren comunicación descendente una vez que el nodo o terminal haya transmitido información ascendente hacia una puerta de enlace. Una vez que envía data el dispositivo entra en modo de bajo consumo

de energía hasta volver a enviar o recibir datos lo cual los hace ideales para equipos que utilicen baterías como fuente de alimentación. [25]

- **Clase B:** Estos dispositivos poseen mayor número de ventanas de recepción lo cual les permite recibir información en horarios establecidos, el dispositivo final recibe balizas sincronizadas (*beacon*) con la hora de envío por parte del gateway lo cual permite al servidor conocer cuando el dispositivo está en modo de escucha (Chinchilla, 2019). Sin embargo, estas ventanas adicionales consumen más energía por lo tanto es menos eficiente en cuanto a consumo que los de clase A.
- **Clase C:** Estos dispositivos están diseñados para recibir datos continuamente si no se transmite data, utilizan más potencia que la clase A y B, por lo que son los menos eficientes en consumo energético. [24]

Figura 1.9

Red LoRaWan



Nota. La figura muestra una red inalámbrica utilizando la tecnología LoraWan, al comunicarse con un servidor es posible almacenar y enviar datos en la nube para ser utilizados por diversas aplicaciones (De ser necesario se utilizan API's para la compatibilidad entre diferentes aplicaciones). [6]

Los gateways de la red pueden recibir información de múltiples nodos simultáneamente, ya que operan en varios canales. Además, la red LoRaWAN ajusta su tasa de datos para adaptarse

a las necesidades de comunicación, lo que permite la recepción de mensajes en múltiples canales al mismo tiempo.

LoRaWAN implementa dos capas de seguridad: una capa de seguridad de red que verifica la autenticidad de los nodos y una capa de seguridad de aplicación que garantiza que solo el usuario final tenga acceso a los datos. La modulación LoRa también integra un esquema de corrección de errores variable, lo que mejora la robustez de la señal transmitida, aunque agrega redundancia. [7]

La tecnología LoRa opera en la banda de frecuencia ISM (Industrial, Scientific and Medical), que está reservada para aplicaciones sin necesidad de licencia, lo que permite la investigación y el desarrollo sin restricciones. Debido al producto de ancho de banda-tiempo considerable y la naturaleza asincrónica de las señales LoRa, esta tecnología es altamente resistente a interferencias tanto dentro como fuera de la banda. Dado que el período de símbolos en LoRa puede ser más largo que la duración de las conmutaciones en sistemas de espectro ensanchado por saltos de frecuencia (FHSS), ofrece una inmunidad excepcional a mecanismos de interferencia de pulsos de amplitud modulada (AM). Esto se traduce en la capacidad de tener un receptor selectivo fuera del canal de 90 dB y un rechazo co-canal de más de 20 dB. [7]

Debido a la banda ancha de los pulsos chirp utilizados por LoRa, esta tecnología se adapta especialmente bien a entornos urbanos. La modulación LoRa emplea factores de propagación ortogonales, lo que permite transmitir múltiples señales de propagación al mismo tiempo en el mismo canal sin una degradación significativa de la sensibilidad del receptor.

Las señales moduladas con diferentes factores de propagación se interpretan como ruido en el receptor de destino y se pueden tratar como tal. Una característica fundamental de LoRa es su capacidad para discriminar linealmente entre errores de tiempo y frecuencia. Por lo tanto, LoRa se presenta como una modulación idónea para aplicaciones como radar y, en consecuencia, es apropiada para aplicaciones de alcance y localización en tiempo real. [7]

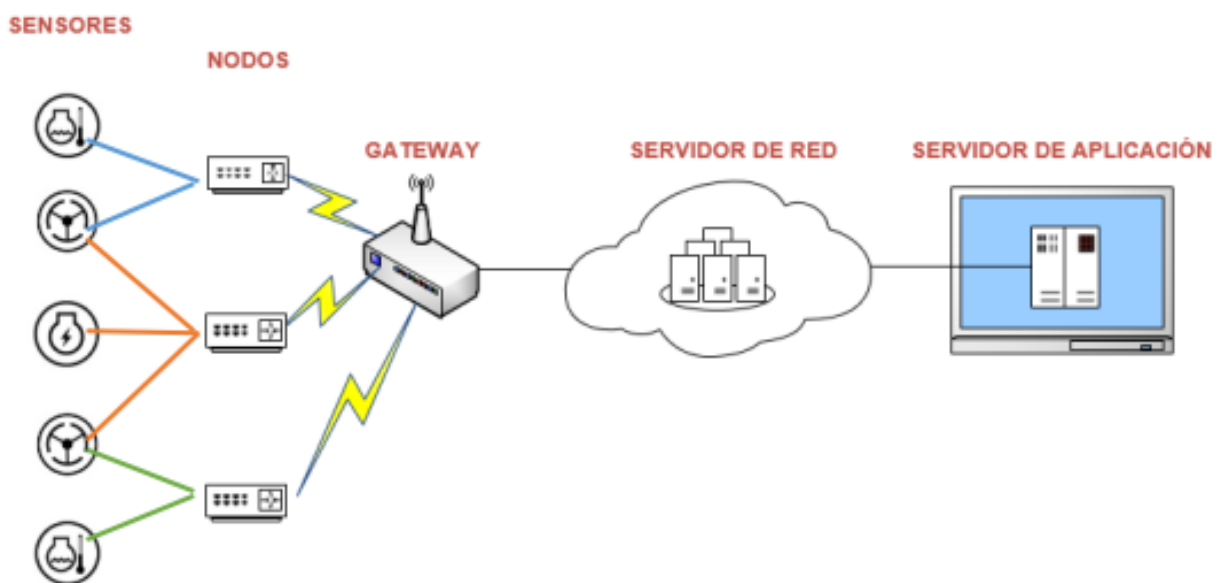
La topología de red utilizada generalmente en este contexto es la de estrella. En esta configuración, la red consta de diversos componentes, que incluyen los dispositivos finales o nodos, los concentradores o gateways, servidores ubicados en la nube y un servidor de aplicaciones, como se ilustra en la Figura 1.9.

Los nodos desempeñan un papel fundamental al actuar como puntos de recolección de datos. Estos nodos se conectan con sensores y permiten la transmisión inalámbrica de datos, a través de un solo salto, hacia uno o varios gateways, utilizando diferentes frecuencias y tasas de datos. Mediante el intercambio de mensajes en formato JSON la información o data transmitida es capaz de llegar a un dispositivo central “gateway” el cual se encarga de transmitir dicha información a un servidor de red central.

Los gateways, por su parte, cumplen una función clave al convertir inicialmente el protocolo inalámbrico de capa física LoRa en protocolos de red IP estándar, lo que facilita la transmisión de los datos a un servidor central de red. [8]

Figura 1.10

Arquitectura de red LoRaWan



Nota. La figura muestra una arquitectura simple para la implementación de redes LoraWan.

El servidor de red se encarga de gestionar aspectos más avanzados, como protocolos de capa superior, la implementación de filtros y políticas de seguridad, así como la administración de parámetros como la velocidad de datos y la potencia de salida de radiofrecuencia (RF) para cada nodo en la red. Finalmente, el servidor de aplicaciones desempeña un papel crucial al procesar los datos recopilados y presentarlos de manera gráfica y comprensible para el usuario final.

Para lograr una red en estrella de largo alcance, es fundamental que el gateway tenga una alta capacidad para recibir mensajes desde múltiples nodos. Esto se logra mediante la implementación de técnicas como el espectro ensanchado secuencial (SSM) y el uso de la velocidad de datos adaptativa (ADR). La combinación de estas estrategias permite la creación de múltiples canales de frecuencia, cada uno con diferentes velocidades de transmisión, teniendo en cuenta factores como el tiempo requerido para transmitir un mensaje y el tamaño del mensaje en cuestión. [8]

Tabla 1.1

Comparación entre Wi-Fi, LoRaWan y SigFox

Tecnología			
Inalámbrica	Wi-Fi	LoRaWan	SigFox
Alcance Máximo	0.1 - 1.5 Km	2 - 20 Km	3 Km - 50 Km
Rendimiento	54 Mbps - 1.3 Gbps	10 kbps - 50 kbps	Up to 1000 bps
Ancho de Banda	20, 40, 80, 160 MHz	125 kHz	100 Hz
Consumo de energía	Medio	Bajo	Bajo
Costo Continuo	Una vez	Una vez	Periódico
Costo del Modulo	Menos de \$10	\$8 - \$15	Menos de \$5
Topología de red	Estrella, Malla	Estrella	Estrella
Uso Común	Conexiones de alta velocidad en interiores y aplicaciones de consumo	IoT industrial, monitoreo de sensores a larga distancia	IoT industrial, monitoreo de sensores a larga distancia

Requiere			
infraestructura	Sí (enrutadores, puntos de		Sí (base stations,
centralizada	acceso)	Sí (gateways, servidores)	servidores)

Nota. La tabla muestra una comparativa entre distintas tecnologías de comunicación inalámbrica.

1.4.5 Tótems de emergencia

El propósito principal de estos dispositivos reside en agilizar la atención de emergencias de diversa naturaleza. Esto se logra mediante la simple acción de presionar un botón situado en el panel principal del dispositivo. Esta acción desencadena una alerta que se transmite de manera inmediata a los brigadistas de ESPOL 911, quienes se movilizarán rápidamente hacia el lugar para atender la emergencia. Esta solución es especialmente valiosa en situaciones en las que un individuo no dispone de un teléfono celular o de otro dispositivo telefónico para comunicarse con el servicio de emergencia 9-1-1. Además, es fundamental destacar que este servicio es de acceso gratuito y se caracteriza por su facilidad de uso.

1.4.6 Pérdida multipaso

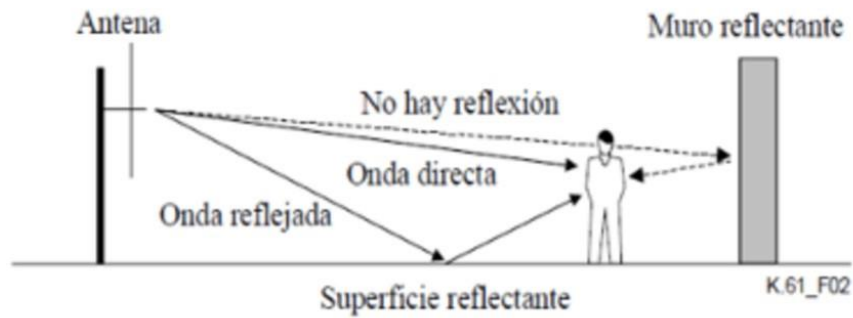
La pérdida de potencia es causada por varios motivos como la interferencia constructiva y destructiva entre distintas señales inalámbricas o el efecto multipaso por la característica de propagación en ráfaga característico de la tecnología WI-FI IEEE 802.11a/b/d/g/n. La presencia de obstáculos dificulta la penetración de señal sin mencionar las pérdidas debido al desvanecimiento de sombra presente en redes inalámbricas. Para motivos prácticos se basará este estudio en modelos de propagación desarrollados para las bandas de frecuencia de 2.4 GHz y 5 GHz.

El término “Desvanecimiento de la señal” se refiere a que dicha señal es atenuada debido a la pérdida en el espacio, los obstáculos y resistencia que debe traspasar durante toda su trayectoria hasta llegar al destino. Este desvanecimiento se refleja como baja o mala potencia recibida en el

terminal receptor lo que resulta en un nivel RSSI muy bajo. El desvanecimiento tiene carácter probabilístico [9].

Figura 1.11

Propagación multipaso en una red inalámbrica



Nota. La figura muestra el efecto de propagación multipaso presente en los enlaces inalámbricos, pueden ser estimados de manera probabilística (Óscar Barrera, 2018).

Capítulo 2

2 Herramientas utilizadas para el estudio de cobertura de red institucional

En este capítulo se detallan las herramientas utilizadas para realizar el estudio de cobertura y obtener un mapeo de zonas con alta intensidad de señal Wi-Fi de tal forma que se disponga de una referencia gráfica para seleccionar los sitios de interés para la ubicación de los respectivos tótems de emergencia con el sistema ESPOL ALERT.

Actualmente existen diversos equipos utilizados para la medición de niveles de potencia RSSI enfocado en redes inalámbricas, sin embargo, el acceso a estos está limitado por el costo puesto que la mayoría son equipos de media y alta gama por lo cual se procedió a realizar estudios de cobertura y recepción de señal a través de aplicaciones móviles y mediante el uso de un computador portátil el cual a través de programas licenciados pueden realizar diversas mediciones en los puntos de interés anteriormente mencionados.

Se requiere del uso de mapas para realizar un bosquejo del área a analizar motivo por el cual se utilizó la herramienta “Google Maps” para obtener dichos planos a ser utilizados por el programa. Mediante la herramienta de software “Acrylic Wi-Fi Heatmaps” se pueden mapear distintos puntos haciendo uso de otras herramientas de medición y analizadores de red tal cual se revisó en el capítulo 1. Utilizando la herramienta de medición “Wi-Fi SweetSpots” se logró tomar un aproximado de 100 muestras por punto de encuentro y sus alrededores a fin de llevar un barrido de valores y estimar su promedio en dicho sector.

2.1 Aplicación Wi-Fi SweetSpots

Wi-Fi Sweetspots es un producto de ASSIA, Inc. La aplicación se encuentra disponible en Google Play para ser utilizado en celulares, es una herramienta de encuesta de velocidad de Wi-Fi, mediante esta aplicación se puede observar la velocidad de datos en distintos puntos a lo largo de un recorrido establecido como también el nivel de intensidad de señal recibida. Se toman

muestras periódicamente en un mismo punto para poder observar la variación de niveles de potencia y velocidad de datos respectivamente.

Con estos datos se pueden establecer comparaciones al momento de realizar el estudio de cobertura en cada uno de los puntos de encuentro a lo largo del campus Gustavo Galindo como se puede observar en la figura 2.1.

Figura 2.1

Medición periódica de potencia de señal recibida y velocidad de datos utilizando la aplicación “Wi-Fi Sweet Spots”.

Spot Date	Speed SSID/BSSID	Signal
Rectorado ? 23-11-01 05:09 PM	30.37 Mbps ESPOL-Wifi(a0:0f:37:e1:0a:a2)	-64 dBm
Celex ? 23-11-01 05:00 PM	62.65 Mbps ESPOL-Wifi(24:81:3b:55:a0:ed)	-73 dBm
FCNM (Laboratorios Química) ? 23-11-01 04:22 PM	33.15 Mbps ESPOL-Wifi(24:81:3b:55:5d:4c)	-78 dBm
FCNM (Sweet Y Coffee) 23-11-01 04:22 PM	131.99 Mbps ESPOL-Wifi(4c:42:1e:ff:5f:0d)	-62 dBm
I3LAB 23-11-01 04:22 PM	31.40 Mbps ESPOL-Wifi(d0:ec:35:7cae:60)	-81 dBm
FICT (Facultad) 23-11-01 04:17 PM	190.81 Mbps ESPOL-Wifi(4c:42:1e:ff:5e:4d)	-50 dBm
FIMCP (Facultad) 23-11-01 04:06 PM	34.69 Mbps ESPOL-Wifi(00:59:dc:8b:1b:6f)	-75 dBm
Marítima (Biblioteca) 23-11-01 11:54 AM	37.65 Mbps ESPOL-Wifi(24:81:3b:55:97:22)	-67 dBm
Marítima (Ancla) 23-11-01 11:50 AM	19.38 Mbps ESPOL-Wifi(00:59:dc:8b:24:80)	-72 dBm
Marítima (Laboratorio Acuicultura 2) 23-11-01 11:50 AM	21.80 Mbps ESPOL-Wifi(00:38:df:2b:18:80)	-71 dBm
FADCOM 23-11-01 11:11 AM	94.96 Mbps ESPOL-Wifi(4c:e1:75:a4:fc:6d)	-59 dBm
FIMCP (Auditorio) 23-11-01 11:02 AM	7.54 Mbps ESPOL-Wifi(24:81:3b:55:94:82)	-62 dBm
FIEC (Parqueadero) 23-11-01 10:56 AM	46.63 Mbps ESPOL-Wifi(dc:f7:19:3aa8:2f)	-75 dBm
UBEP (Coliseo) ! 23-11-01 10:41 AM	12.42 Mbps ESPOL-Wifi(84:f1:47:15:e9:20)	-81 dBm

Nota. La figura muestra el barrido de muestras detectadas por el dispositivo celular a través de la aplicación “Wi-Fi Sweet Spots”, se establecen promedios de potencia y velocidad en base a las distintas muestras recibidas.

En el análisis de los puntos de acceso Wi-Fi para la implementación de tótems de emergencia en ESPOL ALERT, se identifica que la ubicación Celex, con una señal de -73 dBm y una velocidad de 62.65 Mbps, ofrece una conectividad adecuada para transmitir alertas. En contraste, los Laboratorios Química de FCNM, con -78 dBm y 33.15 Mbps, podrían necesitar una mejora en la infraestructura para asegurar la comunicación durante emergencias. El Sweet Y Coffee de FCNM y la FICT (Facultad) son destacables por sus señales robustas y altas velocidades, siendo puntos óptimos para la ubicación de tótems debido a su rendimiento superior, que asegura una transmisión de datos rápida y fiable. La Biblioteca ubicada en la facultad de marítima ofrece una señal medianamente estable, lo que puede no ser suficiente para alertas básicas. El Parqueadero de FIEC, aunque tiene una señal y velocidad justas, requiere atención para asegurar una conexión confiable debido a su ubicación distante de los edificios principales. Este análisis subraya la importancia de una red inalámbrica fiable y bien distribuida para mantener los tótems de emergencia interconectados y funcionales, garantizando así una respuesta efectiva en situaciones críticas.

2.2 Aplicación Wi-Fi Analyzer (Open Source)

Wi-Fi Analyzer (open source) es un analizador de red de código abierto el cual es utilizado para la optimización de redes Wi-Fi al tener la capacidad de detectar interferencias, el uso de canales y la velocidad de datos.

Una herramienta importante para detectar posibles retardos e interferencia en la red es a través de analizadores Wi-Fi, estos se encuentran disponibles para varios sistemas operativos y no requieren de una licencia para ser utilizados.

Haciendo uso de la herramienta “Wi-Fi Analyzer” se puede recopilar información relevante acerca de las redes cercanas tales como intensidad de señal, velocidad de datos promedio y

estimación de canales lo cual es esencial para mantener descongestionada la red del tráfico que podría ser enviado por otros canales al momento de enviar data a través de la red institucional.

Figura 2.2

Medición de intensidad de señal recibida y análisis de canales en Access points del campus Gustavo Galindo



Nota. La figura muestra los distintos niveles de potencia RSSI de varios puntos de acceso alrededor del campus Gustavo Galindo.

Como se puede apreciar en la figura 2.2 a través de aplicaciones móviles como “Wi-Fi Analyzer” se pueden recolectar varios datos importantes acerca del estado de los distintos puntos de acceso cercanos a los sitios de interés, se puede visualizar datos como RSSI y optimización del uso de canales.

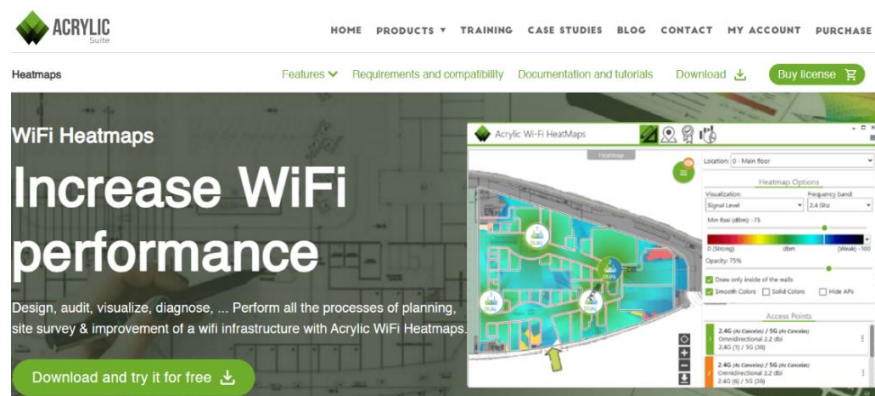
2.3 Software Acrylic Wi-Fi Heatmaps

Para tener una visualización gráfica de dichos valores de intensidad de señal recibida se ha decidido trabajar con un software licenciado llamado “Acrylic Wi-Fi Heatmaps”. Este programa es utilizado para realizar estudios de cobertura Wi-Fi pues al ser una herramienta de planificación permite diseñar y analizar datos importantes en el área de estudio, de esta forma se logra tener un análisis detallado de la cobertura Wi-Fi en un área específica. “Acrylic Wi-Fi Heatmaps” es una

herramienta de software creada por la empresa Tarlogic Security, compañía española especializada en ciberseguridad. La forma en como la herramienta de software interpreta la data recibida es a través de muestras periódicas las cuales serán tomadas por el operador del ordenador en el cual este programa se encuentre instalado y previamente licenciado. Para esto es necesario ingresar una referencia satelital al programa para poder calibrar la zona de trabajo donde se van a tomar dichas muestras periódicamente.

Figura 2.3

Mapa de calor generado por el programa Acrylic Wi-Fi Heatmaps



Nota. La figura muestra el mapeo de una red Wi-Fi utilizando el programa Acrylic Wi-Fi Heatmaps.

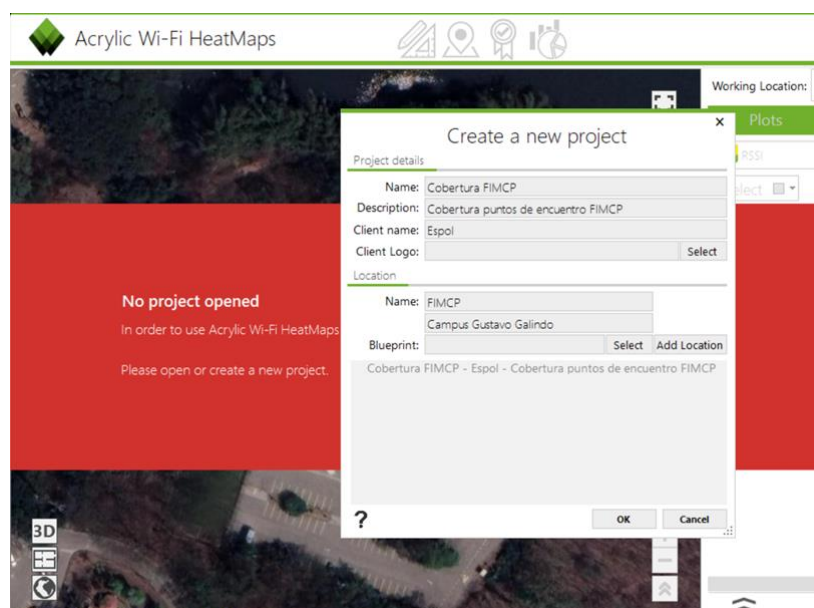
Como se muestra en la figura 2.3 mediante la recolección de datos tipo “. PCAP” los cuales son archivos de datos acerca del tráfico de red, el programa hace uso de capturas de wireshark y otros analizadores de red, de esta forma obtiene datos importantes sobre el área donde se están realizando los estudios de cobertura. Para esto también se debe ingresar el área a analizar mediante una captura satelital, haciendo uso de la herramienta Google Maps se puede obtener dicha referencia, el programa tiene la posibilidad de calibrar el terreno en base al plano ingresado. Se ingresan entonces los datos del terreno, su ubicación referencial y el plano del terreno de la zona sobre la cual se realiza el estudio de cobertura.

Cuando ya han sido tomados los valores de intensidad de señal recibida (RSSI) a través del programa Acrylic Wi-Fi Heatmaps a lo largo de cada uno de los distintos puntos ubicados en el mapa del campus Gustavo Galindo el software de diseño se encarga de realizar un estimado de la señal inalámbrica en cada uno de ellos con lo cual se logra tener un mapa de calor denotando los puntos en donde la intensidad de señal es mayor lo cual garantiza la conectividad de los distintos tótems ubicados a lo largo del campus. A continuación, se detalla el proceso para elaborar dichos mapas de calor.

Al ingresar los datos del área a estudiar se procede a realizar la calibración del mapa para que el software tenga una referencia de medida con respecto al plano ingresado, para esto se debe ingresar una captura satelital con la cual se compara internamente en el software, una vez calibrados se puede comenzar a tomar muestras por el sector recibiendo así paquetes con datos como intensidad de señal recibida, procesada esta información el software es capaz de devolver mapas de calor denotando así las zonas con mayor y menor cobertura de red Wi-Fi dependiendo de la ubicación donde se esté realizando el estudio de cobertura.

Figura 2.4

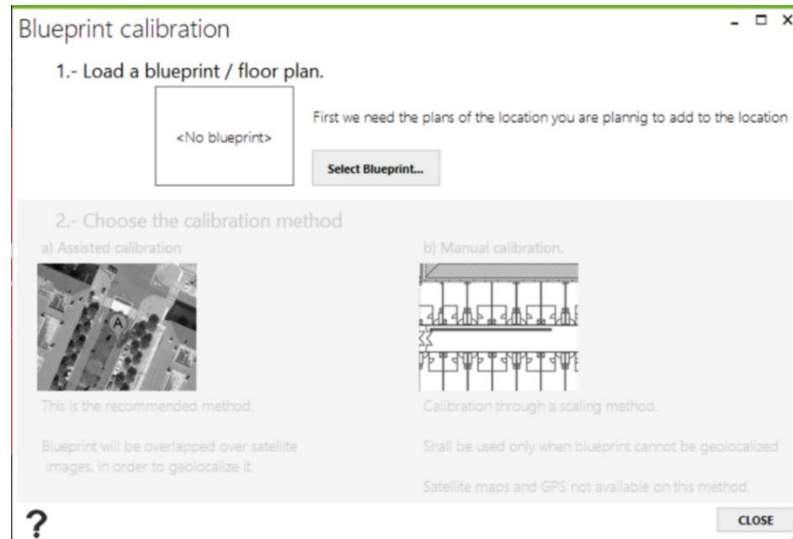
Ingreso de mapa del área a analizar.



Nota. La figura muestra el ingreso de planos de la zona a mapear, de acuerdo a esto se realizan las estimaciones necesarias del caso para los distintos puntos de acceso anteriormente ubicados.

Figura 2.5

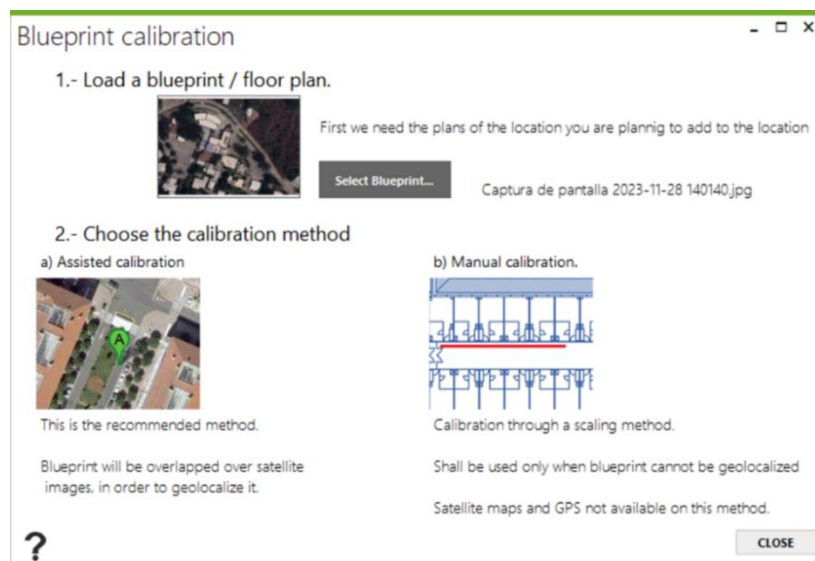
Calibración de planos en área a estudiar



Nota. La figura muestra el ingreso de los planos respectivos para el área de ubicación de los distintos puntos de encuentro a lo largo del campus Gustavo Galindo.

Figura 2.6

Calibración del mapa por guía satelital.

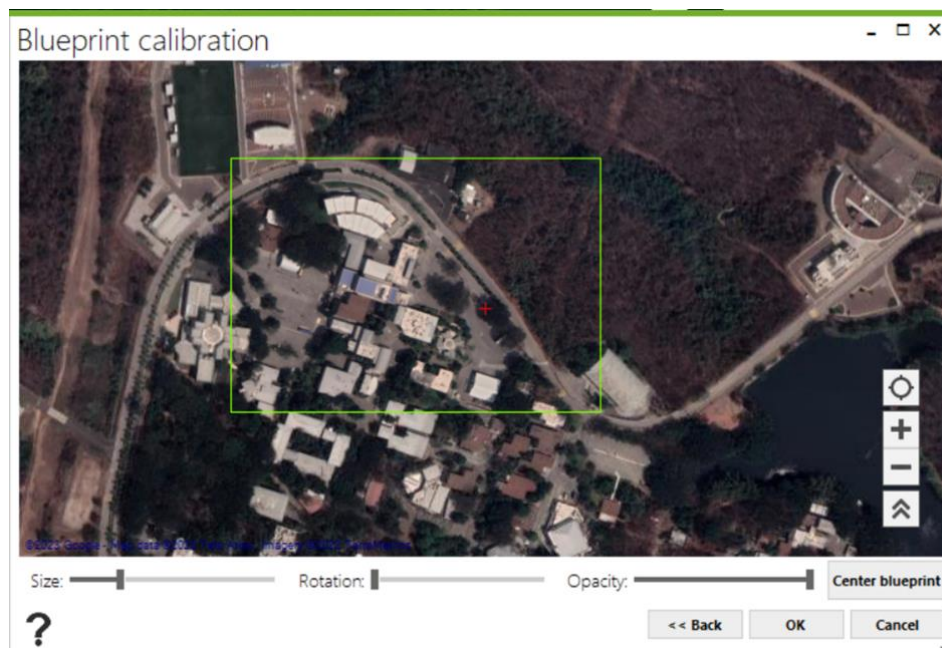


Nota. La figura muestra el ingreso de un mapa para su respectiva calibración.

Se establecen medidas de referencia ingresando una captura del terreno vía satélite y sobreponiéndolo con el mapa disponible dentro del software, como se muestra en la figura 2.7 al establecer semejanza entre ambos mapas el programa reconoce el terreno sobre el que está trabajando. Este proceso permite obtener un mapa calibrado, facilitando el recorrido para capturar datos del tráfico de la red. De esta forma, se puede generar un mapa de calor que identifique las zonas con mayor cobertura institucional. Es esencial realizar este procedimiento en cada uno de los puntos de encuentro designados por las facultades.

Figura 2.7

Superposición de mapas en software Acrylic Wi-Fi Heatmaps



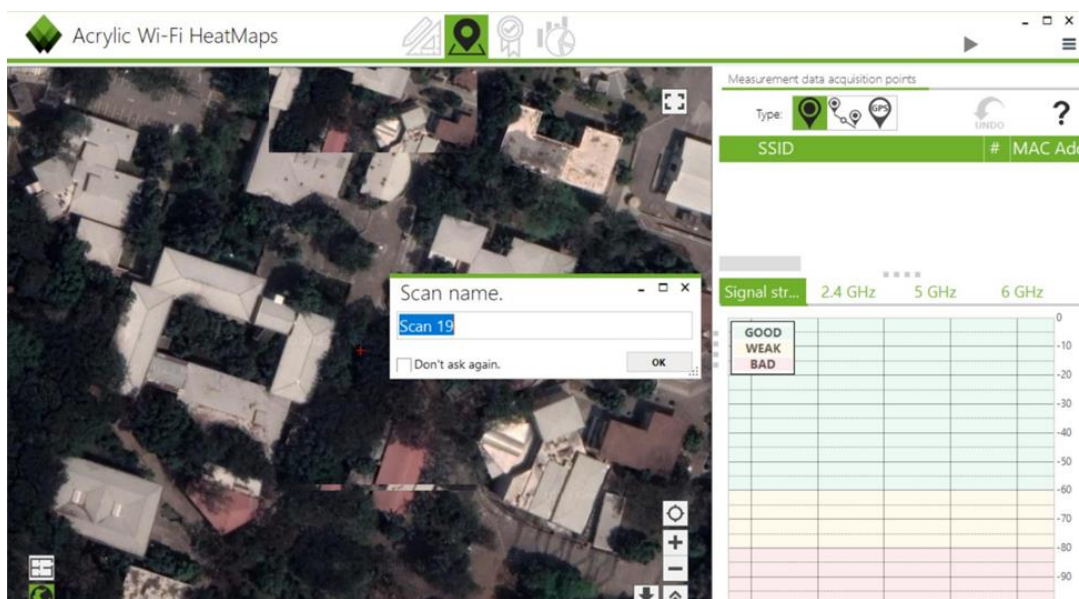
Nota. La figura muestra la superposición del mapa satelital del área a analizar con la información presente en el software de tal forma que se establezca una referencia para comenzar con el barrido y registros de muestras periódicas para el estudio de cobertura.

Cuando la calibración ha sido realizada de forma exitosa se dispondrá del mapa del área en donde se realizará el estudio de cobertura Wi-Fi, en este punto se registrará las muestras periódicamente mientras se desplaza por el área de interés, para esto es necesario realizar escaneos

periódicamente de manera que se abarque toda la zona de interés, a mayor número de escaneos la información de referencia para la creación de mapas de calor es más precisa, de esta forma se van ingresando los distintos escaneos progresivos, dando inicio al proyecto dentro del programa se pueden empezar a registrar las distintas muestras como se observa en la figura 2.8.

Figura 2.8

Escaneo en zona de interés

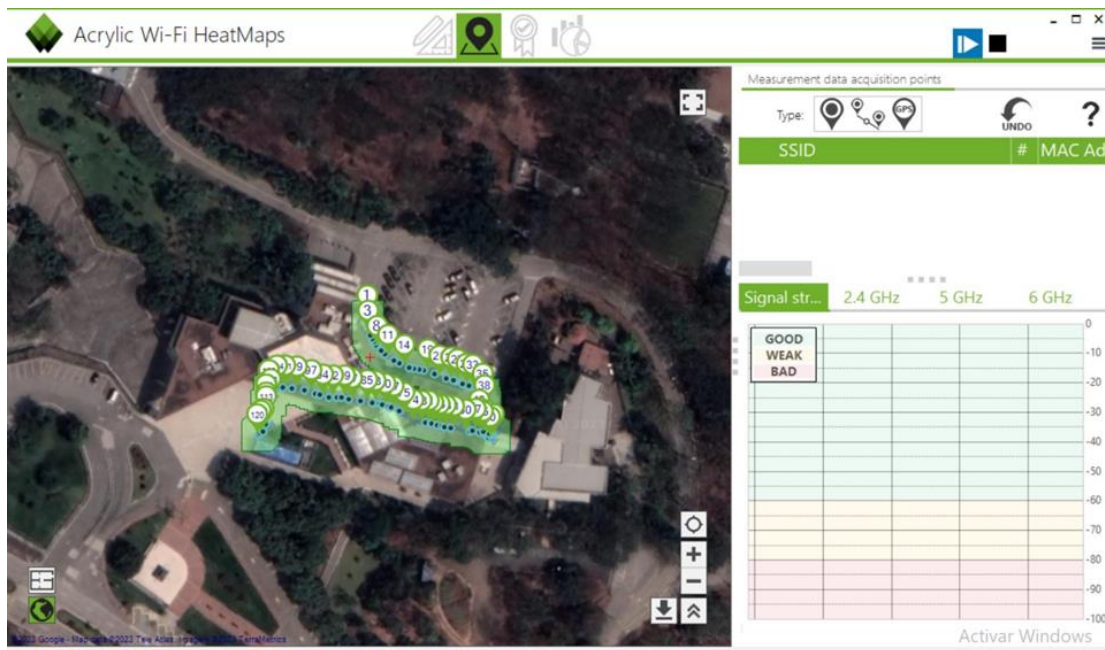


Nota. La figura muestra los distintos escaneos a realizar dependiendo de la ruta de movilización del equipo a medida que censa distintos niveles de RSSI.

Como se ilustra en la figura 2.9, es importante registrar la ruta durante el desplazamiento del usuario por el mapa. Este registro debe realizarse por el operador que maneja el software en el portátil, capturando así la trayectoria recorrida para el análisis posterior. De esta forma se irá analizando el tráfico de la red inalámbrica de forma pasiva, es decir; que el dispositivo estará en modo de “escucha” con lo cual analizará los paquetes Wi-Fi recibidos de tal forma que se pueda definir zonas con mayor y menor alcance de cobertura Wi-Fi.

Figura 2.9

Barrido de muestras en mapa dentro del software



Nota. La figura indica el barrido de muestras tomadas por escaneo en el programa, analizando el área de rectorado mediante la recopilación de datos de tráfico en la red se genera el mapeo de intensidad de señal recibida RSSI.

Durante un escaneo promedio se realizan entre 100 y 200 tomas puntuales de datos a lo largo del trayecto recorrido, es recomendable realizar varios escaneos para tener el mejor resultado posible, durante el desarrollo de este proyecto se han tomado entre 10 a 20 escaneos por área de interés para las distintas facultades y sitios estratégicos del campus Gustavo Galindo.

Cuando se realiza un número considerable de escaneos se puede empezar a generar la información correspondiente de forma gráfica mediante la herramienta de software. Adicional a la visualización de RSSI en el área de interés se puede notar las redes cercanas detectadas durante el trayecto, así como también el número de usuarios conectados a dichas redes en bandas de 2.4Ghz y 5Ghz. Las redes a ser analizadas se pueden seleccionar en conjunto o de forma individual para estudiar cada una de ellas.

Figura 2.10

Mapa de calor (RSSI) generado por Acrylic Wi-Fi Heatmaps.



Nota. La figura muestra el mapa de calor generado por el software dando a notar las zonas con mayor intensidad de señal y aquellas que no lo tienen. Se toman en cuenta las redes principales “ESPOL-Wi-Fi, Eduroam y ESPOL”.

Para ser utilizado de manera más eficiente se dispone de la opción de exportar estos datos a otras aplicaciones, en este caso al trabajar con referencias satelitales se pueden establecer comparaciones más exactas lo cual permite generar archivos tipo KMZ con la ubicación de dichas áreas, de esta forma es posible visualizar dichos datos en sitios como “Google Earth Pro”.

Figura 2.11

Mapa de calor visualizado en aplicación “Google Earth”

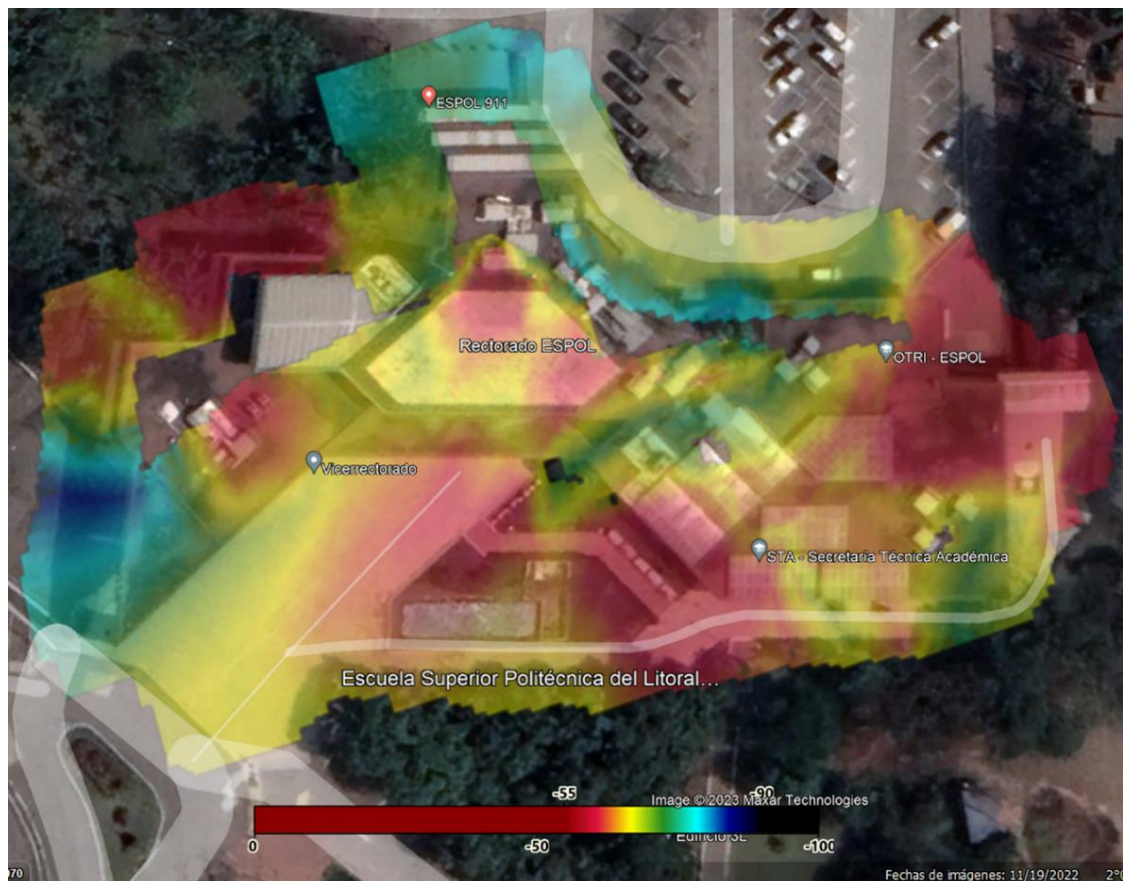


Nota. La figura muestra los datos RSSI en la aplicación Google Earth, de esta forma la visualización del área es más completa e interactiva.

Al tener la ubicación de las zonas de interés y el mapa de cobertura generado por el software Acrylic Wi-Fi Heatmaps se puede comenzar con el proceso de evaluación de mejores puntos de cobertura para la instalación de los equipos. De esta forma se tiene una referencia muy importante al momento de establecer los lugares de instalación de los distintos tótems de emergencia a lo largo del campus Gustavo Galindo. Como se puede observar en la figura 2.12 la variación del color en los mapas generados se basa en los límites definidos por el programa, en este caso se ha seteado un nivel máximo de -50dbm hasta un nivel mínimo de -100dbm como intensidad de señal recibida, un nivel por debajo de dichos límites se considera no adecuado o no confiable.

Figura 2.12

Rango de colores, intensidad máxima y mínima de señal recibida



Nota. La figura muestra el rango de colores en función de la intensidad de señal recibida RSSI, siendo las zonas rojas lugares con mayor intensidad y las azules las de menor (Makar Technologies, 2023).

2.4 Ubicación de los puntos de encuentro y zonas estratégicas – Equipo Etrex Garmin

Para la respectiva ubicación de cada uno de los puntos de encuentro y zonas estratégicas se debe mencionar el uso de un equipo para rastreo satelital de marca Etrex – Garmin.

Como se muestra en la figura 2.13, la coincidencia entre los datos de geolocalización del equipo Etrex – Garmin y los proporcionados por la aplicación móvil GPS 'TimeStamp' permite trabajar con todos estos datos de manera segura y eficiente. Esta correlación garantiza la fiabilidad y precisión necesarias para el análisis geoespacial del proyecto. Se irán ingresando las localizaciones de los puntos de encuentro en el mapa de calor generado para cada facultad.

Figura 2.13

Equipo de medición GPS Etrex.



Nota. La figura muestra la referencia GPS de uno de los varios puntos de encuentro (Celex) mapeados en el campus Gustavo Galindo.

Con las ubicaciones de los puntos de encuentro y el mapa de calor de las facultades en los cuales se encuentren estos mismos se puede realizar la evaluación de cobertura para cada uno de estos puntos, es importante mencionar que los puntos de encuentro son una medida tentativa, dependiendo del sector se pueden establecer nuevas posiciones de referencia para la instalación de los equipos a fin de asegurar su conectividad al estar en zonas de alta cobertura de red institucional.

Se realiza el mismo procedimiento para la ubicación de los puntos estratégicos visualizados en la figura 1.5.

Tabla 2.1

Localización de puntos de encuentro Campus Gustavo Galindo

Puntos de encuentro	Localización GPS
BIBLIOTECA	2°08'51.3"S 79°57'56.5"W
FADCOM	2°08'38.5"S 79°57'43.7"W
FIMCP 1 (Auditorio)	2°08'39.5"S 79°57'59.9"W
FIMCP 2 (Decanato)	2°08'40.6"S 79°57'58.1"W
FIMCP 3 (Parqueadero STEM)	2°08'37.8"S 79°57'58.4"W
UBEP 1 (Parqueadero)	2°08'33.5"S 79°58'01.8"W
UBEP 2 (Cancha Sintética)	2°08'36.0"S 79°58'03.3"W
I3LAB	2°08'47.1"S 79°57'53.9"W
FCSH 1 (Auditorio)	2°08'50.9"S 79°58'03.6"W
FCSH 2 (Edificio administrativo)	2°08'51.3"S 79°58'06.9"W
FIMCM 1 (Cancha Sintética)	2°08'48.8"S 79°57'47.9"W
FIMCM 2 (Ancla)	2°08'49.5"S 79°57'45.5"W
FIMCM 3 (Bloque 5G)	2°08'47.0"S 79°57'44.3"W
FIMCM 4 (Bloque 5H)	2°08'47.7"S 79°57'46.5"W
FCV	2°09'06.2"S 79°57'24.0"W
CELEX (Parqueadero)	2°08'54.1"S 79°58'04.0"W
FCNM 1 (Sweet & Coffee)	2°08'46.4"S 79°58'00.6"W
FCNM 2 (Laboratorios Química)	2°08'46.6"S 79°58'04.9"W
FICT (Decanato)	2°08'44.4"S 79°57'55.5"W
FIEC 1 (Parqueadero)	2°08'40.9"S 79°58'00.5"W
FIEC 2 (Fiec Vieja)	2°08'43.1"S 79°57'58.8"W
RECTORADO (Edificio principal)	2°08'51.9"S 79°57'52.9"W
RECTORADO 2 (Tesorería)	2°08'52.2"S 79°57'50.4"W

Nota. La tabla muestra la ubicación geográfica de los puntos de encuentro alrededor del campus Gustavo Galindo.

Como se aprecia en la tabla 2.1 se dispone de la ubicación de los puntos de encuentro para poder realizar el estudio correspondiente, se pueden visualizar de forma gráfica en la figura 1.4.

De esta forma se pueden ir asignando zonas donde dichos puntos de encuentro disponen de alta cobertura de red institucional con lo cual se asegura una buena comunicación con los equipos a utilizar para la ubicación de los respectivos tótems de emergencia.

Adicionalmente como se mencionó en la sección 1.2 se han agregado las ubicaciones de cada uno de los puntos estratégicos a lo largo del campus Gustavo Galindo. Los puntos estratégicos mencionados en la figura 1.5 han sido localizados como se muestra en la tabla 2.2.

Tabla 2.2

Localización de puntos estratégicos Campus Gustavo Galindo

Puntos Estratégicos	Localización GPS
Bosque Protector Prosperina	2°09'07.7"S 79°57'37.2"W
Mirador Bosque Protector Prosperina	2°09'20.3"S 79°57'45.4"W
Capilla	2°08'48.1"S 79°57'33.6"W
Cancha UBEP	2°08'34.5"S 79°58'04.8"W
Ciclo ruta 1 (Garita)	2°09'06.5"S 79°57'12.9"W
Ciclo ruta 2 (Tumbas)	2°09'00.6"S 79°57'33.8"W
Ciclo ruta 3	2°09'02.2"S 79°57'42.9"W
Guardería (Bloque 3G)	2°09'05.4"S 79°57'20.5"W
Coliseo Viejo	2°08'42.4"S 79°57'51.8"W
Glorieta (Residencia estudiantil)	2°09'12.5"S 79°57'24.0"W
Gimnasio Profesores	2°08'36.6"S 79°58'04.7"W
Estadio Deportivo	2°09'14.9"S 79°57'29.4"W
Paradero Rectorado	2°08'54.9"S 79°57'51.9"W
PARCON	2°08'45.1"S 79°56'54.7"W

Nota. La tabla muestra la localización de cada uno de los puntos estratégicos seleccionados para abarcar una mayor cobertura de respuesta ante posibles emergencias.

Capítulo 3

3 Identificación de mejor tecnología inalámbrica: ESP32 y Lora.

En este capítulo se analizará la mejor tecnología de comunicación inalámbrica en función de la ubicación de cada uno de los distintos puntos de encuentro de acuerdo al nivel de cobertura institucional presente en cada uno de ellos, es decir; para puntos con un nivel de intensidad de señal recibida moderado se utilizarán equipos ESP32 mientras que para los puntos con poca o cobertura nula se optará por otras tecnologías como por ejemplo Lora.

En base a los resultados obtenidos a través del estudio de cobertura realizado por medio del software “Acrylic Wi-Fi Heatmaps” se obtendrá una lista con los puntos que cuentan con un nivel óptimo de intensidad de señal recibida y los que no lo cumplen, dichos mapas de cobertura pueden ser visualizados en el apéndice A al final de este documento.

El estudio exhaustivo de la cobertura Wi-Fi realizado en los puntos de encuentro del campus Gustavo Galindo Velasco ha revelado un panorama mixto. La mayoría de las ubicaciones clave, como el Rectorado y la Biblioteca Central, mostraron una cobertura Wi-Fi adecuada, con mapas de calor indicando zonas de intensa señal idóneas para el funcionamiento de los tótems de emergencia. En contraste, áreas como CELEX y algunos sectores de la FCSH, FIEC y FIMCP, mostraron niveles de señal fluctuantes que sugieren la necesidad de una mejora infraestructural para garantizar la conectividad integral y el rendimiento óptimo del sistema ESPOL ALERT.

En particular, los puntos de encuentro dentro de FCSH y CELEX, pese a sus desafíos, están situados en lugares con alto flujo de tráfico estudiantil, resaltando la importancia de la ubicación estratégica para la instalación de los tótems. Además, la presencia de redes adicionales en la FIEC, como FIEC Wireless, proporciona una cobertura complementaria que favorece la comunicación en caso de emergencia, aunque se identificaron áreas susceptibles de mejora para alcanzar la cobertura deseada.

Estos hallazgos subrayan la viabilidad del proyecto en términos de infraestructura existente y resaltan oportunidades específicas para mejoras dirigidas. La implementación de tótems de emergencia no solo es factible desde una perspectiva tecnológica, sino que también es económicamente viable, aprovechando la red Wi-Fi actual y evitando inversiones significativas en nuevos equipos o servicios. Las recomendaciones resultantes de este estudio incluyen tanto la mejora de la cobertura Wi-Fi en áreas específicas como la instalación estratégica de tótems en puntos con alta densidad de población y tráfico, lo que fortalecerá la red de seguridad del campus y mejorará la capacidad de respuesta de ESPOL ALERT.

3.1 Comparativa de Cobertura Wi-Fi: Áreas Académicas vs. Espacios Abiertos

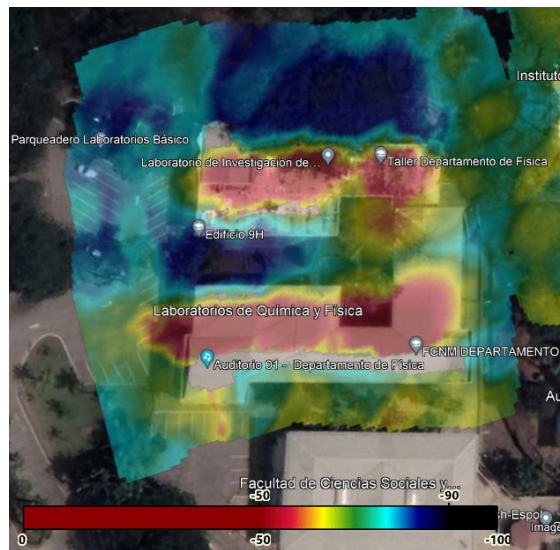
La investigación sobre la cobertura Wi-Fi en el campus Gustavo Galindo Velasco, destinada a la implementación de tótems de emergencia integrados al sistema ESPOL ALERT, demuestra la complejidad inherente a los entornos de señal dentro de un área geográfica y funcionalmente diversa como la de una institución educativa. En el terreno académico, las señales Wi-Fi se beneficiaron de la proximidad y la densidad de los puntos de acceso, a pesar de las interferencias potenciales de los materiales de construcción densos. Por el contrario, las áreas recreativas y al aire libre, aunque esenciales para el esparcimiento y la recreación estudiantil, presentaban un desafío más significativo debido a la dispersión y atenuación de señales causada por barreras naturales y construidas, así como por la mayor distancia de los puntos de acceso.

Este estudio sugiere que la variabilidad en la intensidad de la señal podría atribuirse no solo a la distancia física de los puntos de acceso, sino también a la interacción con la flora endémica y la topografía única del campus, que incluye zonas de bosque seco-tropical. Estos factores naturales, si bien enriquecen la biodiversidad y el valor estético del campus, pueden presentar desafíos significativos para la propagación de señales inalámbricas. La vegetación, en particular, puede tener un efecto de atenuación en la señal Wi-Fi, especialmente cuando está en su punto más

denso durante la estación de crecimiento. Como se puede observar en la figura 3.1 y 3.2 la señal Wi-Fi propagada en el aire tiene a perderse por fenómeno de absorción en el follaje de la vegetación.

Figura 3.1

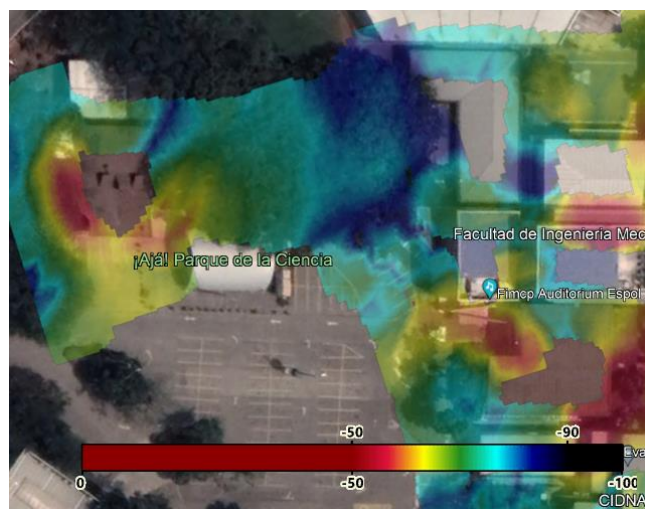
Pérdida de señal en áreas verdes



Nota. La figura muestra la pérdida de señal inalámbrica en áreas verdes. Aquellas zonas de color azul denotan la falta de cobertura de red institucional.

Figura 3.2

Pérdida de señal Wi-Fi en espacios abiertos.



Nota. La figura muestra la pérdida de señal inalámbrica en áreas verdes con vegetación.

Como se aprecia en la figura 3.2 la presencia de vegetación causa pérdida en la intensidad de señal recibida por lo que no se consideran espacios para trabajar con esta tecnología inalámbrica Wi-Fi. Además, el diseño arquitectónico y la disposición de los edificios, con una mezcla de estilos modernos y tradicionales, contribuyen a un patrón complejo de cobertura que requiere un enfoque meticuloso para el diseño y la distribución de la red Wi-Fi.

Para abordar estas complejidades y asegurar una cobertura de red homogénea y confiable, se plantea la necesidad de una estrategia de infraestructura de red que contemple la diversidad del entorno. Esto podría incluir la instalación de repetidores de señal en áreas clave, la optimización de la ubicación de los puntos de acceso existentes y la incorporación de tecnología capaz de traspasar las barreras naturales sin degradar la señal. Al mismo tiempo, se debe considerar la densidad de usuarios en diferentes momentos del día y en eventos específicos, lo que puede causar variaciones en la demanda de la red y, por ende, en la calidad de la conexión.

En definitiva, este análisis profundo y técnico subraya la importancia de una planificación detallada de la red Wi-Fi, que no solo considere las necesidades actuales, sino que también sea adaptable a los cambios futuros. El objetivo último es proporcionar una infraestructura de comunicación robusta que soporte de manera eficiente los tótems de emergencia y otros sistemas críticos para la seguridad y la funcionalidad del campus universitario.

3.2 Evaluación de Cobertura Wi-Fi en puntos de encuentro

En el análisis de cobertura Wi-Fi para implementar tótems de emergencia en la ESPOL, se observó que las zonas de alto tráfico como el Rectorado, Biblioteca Central y FICT poseen una señal de Wi-Fi potente y estable, adecuada para soportar sistemas críticos de comunicación en urgencia. Sin embargo, en áreas como CELEX y ciertos sectores de la FCSH, se identificaron fluctuaciones significativas en la intensidad de la señal, lo que subraya la necesidad de reevaluar

la infraestructura de red existente o la posible adición de puntos de acceso adicionales para fortalecer la señal en estos puntos clave.

En la FCNM, la presencia de cobertura adecuada en ciertas zonas contrasta con áreas donde la intensidad de la señal disminuye, resaltando la necesidad de una planificación detallada para la distribución espacial de los tótems.

Por otro lado, la FIEC presenta el desafío de gestionar múltiples redes solapadas, lo que requiere un enfoque integrado que optimice la señal y el tráfico de datos para evitar interferencias y garantizar una comunicación fluida y confiable.

En resumen, en zonas como UBEP, I3LAB, parqueadero de FIEC, Cancha FIMCM y parqueadero de FCNM el nivel de intensidad de señal recibida no es lo suficientemente bueno para asegurar el funcionamiento de algún equipo utilizando tecnología Wi-Fi, por lo tanto, se plantea otra tecnología inalámbrica para la conexión de los mismos a la red de tótems de emergencia.

Este análisis informa las decisiones sobre la ubicación de los tótems de emergencia y proporciona una hoja de ruta para mejorar la infraestructura de telecomunicaciones del campus, para lograr una red de seguridad y comunicación muy resiliente y adaptada a las necesidades de la comunidad universitaria. En base a los resultados obtenidos en el apéndice A se tienen los puntos dentro de zonas con alta cobertura de red institucional y puntos que no cuentan con niveles óptimos de intensidad de señal recibida que garanticen una conectividad fiable para los tótems mediante tecnología Wi-Fi.

3.2.1 Puntos de encuentro con cobertura óptima de red

Como se mencionó en la sección 3.2, mediante el estudio de cobertura a través del software (Acrylic Wi-Fi Heatmaps) se han identificado aquellos puntos dentro de zonas con cobertura de red institucional óptima para el uso de equipos que utilicen tecnología Wi-Fi para la transmisión

de alertas haciendo uso de equipos ESP32, dichos puntos pueden ser observados de manera general en la tabla 3.1.

Tabla 3.1

Puntos de encuentro en zonas con cobertura alta o moderada

Puntos de encuentro	Localización GPS
BIBLIOTECA	2°08'51.3"S 79°57'56.5"W
FADCOM	2°08'38.5"S 79°57'43.7"W
FIMCP 1 (Auditorio)	2°08'39.5"S 79°57'59.9"W
FIMCP 2 (Decanato)	2°08'40.6"S 79°57'58.1"W
FIMCP 3 (Parqueadero STEM)	2°08'37.8"S 79°57'58.4"W
FCSH 1 (Auditorio)	2°08'50.9"S 79°58'03.6"W
FCSH 2 (Edificio administrativo)	2°08'51.3"S 79°58'06.9"W
FIMCM 2 (Ancla)	2°08'49.5"S 79°57'45.5"W
FIMCM 3 (Bloque 5G)	2°08'47.0"S 79°57'44.3"W
FIMCM 4 (Bloque 5H)	2°08'47.7"S 79°57'46.5"W
FCV	2°09'06.2"S 79°57'24.0"W
CELEX (Parqueadero)	2°08'54.1"S 79°58'04.0"W
FCNM 1 (Sweet & Coffee)	2°08'46.4"S 79°58'00.6"W
FICT (Decanato)	2°08'44.4"S 79°57'55.5"W
FIEC 2 (Fiec Vieja)	2°08'43.1"S 79°57'58.8"W
RECTORADO (Edificio principal)	2°08'51.9"S 79°57'52.9"W
RECTORADO 2 (Tesorería)	2°08'52.2"S 79°57'50.4"W

Nota. La tabla muestra los puntos de encuentro en zonas de mediana y alta cobertura institucional.

Los puntos de encuentro mencionados en la tabla 3.1 se ubican dentro de zonas con rangos de cobertura óptimos para el uso de tecnología Wi-Fi a fin de poder utilizar dichos dispositivos para simular un botón de pánico el cual, al estar conectado a la red institucional será capaz de enviar una alerta en tiempo con la acción de dicho botón.

3.2.2 Puntos de encuentro sin cobertura óptima de red

De la misma forma, al analizar los resultados del estudio de cobertura detallados en el apéndice A se han detectado puntos de encuentro ubicados en zonas con baja cobertura de red

institucional, dichos niveles de intensidad de señal recibida no son óptimos para ser trabajados a través de tecnología Wi-Fi pues esto compromete la eficiencia del sistema ESPOL ALERT. Se propone la tecnología LoraWan para ser utilizada en cada uno de estos puntos detallados en la tabla 3.2.

Tabla 3.2

Puntos de encuentro en zonas con cobertura baja o nula

Puntos de encuentro	Localización GPS
UBEP 1 (Parqueadero)	2°08'33.5"S 79°58'01.8"W
UBEP 2 (Cancha Sintética)	2°08'36.0"S 79°58'03.3"W
FIMCM 1 (Cancha Sintética)	2°08'48.8"S 79°57'47.9"W
FCNM 2 (Laboratorios Química)	2°08'46.6"S 79°58'04.9"W
FIEC 1 (Parqueadero)	2°08'40.9"S 79°58'00.5"W
I3LAB	2°08'47.1"S 79°57'53.9"W

Nota. La tabla muestra los puntos de encuentro en zonas con cobertura de red institucional baja o nula.

3.3 Análisis de cobertura en zonas estratégicas

Como se detalló en la sección 1.2, además de los puntos de encuentro distribuidos por el campus Gustavo Galindo, es crucial incluir zonas estratégicas para ampliar la cobertura de respuesta ante emergencias.

Estos lugares adicionales se detallan en la tabla 2.2. Dado que la mayoría de estas áreas estratégicas carecen de cobertura de red institucional, se recomienda el uso de dispositivos LoRa. Sin embargo, algunos de estos puntos sí cuentan con cobertura de red institucional, lo que permite la implementación de tecnología Wi-Fi.

Para analizar los niveles de velocidad de red e intensidad de señal recibida en estos puntos se hizo uso de la aplicación “Wi-Fi Sweetspots” puesto que en la mayoría de dichos puntos no existen redes o en su defecto la señal es muy baja no se optó por utilizar un barrido de muestras

como en el caso de los puntos de encuentro, en su lugar se toman escaneos progresivos en los puntos específicos donde se planea instalar los tótems de emergencia, dichos puntos con alcance de cobertura de red institucional se observan en la figura 3.3.

Figura 3.3

Puntos estratégicos con cobertura alta o moderada

Spot Date	Speed	Signal
	SSID/BSSID	
Garita (Inicio Ciclovía) 24-01-17 10:36 AM	132.55 Mbps	-65 dBm
Guardería (Bloque 3G) 24-01-17 10:36 AM	123.57 Mbps	-61 dBm
Glorieta Residencias 24-01-17 10:36 AM	10.36 Mbps	-88 dBm
Paradero Rectorado 24-01-17 10:36 AM	17.24 Mbps	-77 dBm
Gym Profesores 24-01-17 10:36 AM	1.56 Mbps	-85 dBm
Coliseo Viejo 24-01-17 10:27 AM	13.56 Mbps	-90 dBm

Nota. La figura muestra el resultado del escaneo puntual en cada una de las zonas estratégicas con alcance de red institucional.

Como se observa en la figura 3.3 la aplicación muestra los niveles de intensidad de señal recibida y velocidad de datos promedio en cada uno de estos puntos con acceso a red institucional, aquellos marcados con visto verde poseen un nivel adecuado para trabajar con tecnología Wi-Fi por lo tanto de acuerdo a esta información se concluye que únicamente 3 puntos pueden ser trabajados con tecnología Wi-Fi al estar ubicados dentro de zonas con cobertura, estos puntos se visualizan en la tabla 3.3.

Tabla 3.3

Puntos estratégicos con cobertura alta o moderada

Puntos Estratégicos	Localización GPS
Ciclo ruta 1 (Garita)	2°09'06.5"S 79°57'12.9"W
Paradero Rectorado	2°08'54.9"S 79°57'51.9"W
Guardería (Bloque 3G)	2°08'45.1"S 79°56'54.7"W

Nota. La tabla muestra los puntos estratégicos con un nivel óptimo de intensidad de señal recibida, lo que los hace viables para trabajar con tecnología Wi-Fi mediante dispositivos ESP32.

Para el resto de los puntos estratégicos descritos en la tabla 2.2 se debe trabajar con tecnología Lora debido a la falta de conectividad a la red institucional, existen redes privadas las cuales no pueden ser utilizadas si se enfoca el desarrollo de este proyecto para el uso en el campus Gustavo Galindo, en dicho caso se requiere permisos de acceso para poder utilizar dichas redes privadas.

Tabla 3.4

Puntos estratégicos con cobertura deficiente o nula

Puntos Estratégicos	Localización GPS
Bosque Protector Prosperina	2°09'07.7"S 79°57'37.2"W
Mirador Bosque Protector Prosperina	2°09'20.3"S 79°57'45.4"W
Capilla	2°08'48.1"S 79°57'33.6"W
Cancha UBEP	2°08'34.5"S 79°58'04.8"W
Ciclo ruta 2 (Tumbas)	2°09'00.6"S 79°57'33.8"W
Ciclo ruta 3	2°09'02.2"S 79°57'42.9"W
Coliseo Viejo	2°08'42.4"S 79°57'51.8"W
Glorieta (Residencia estudiantil)	2°09'12.5"S 79°57'24.0"W
Gimnasio Profesores	2°08'36.6"S 79°58'04.7"W
Estadio Deportivo	2°09'14.9"S 79°57'29.4"W
PARCON	2°08'45.1"S 79°56'54.7"W

Nota. La tabla muestra los puntos estratégicos con cobertura de red institucional deficiente.

3.4 Implementación del ESP32 en la Red de Tótems de Emergencia

Según la información gráfica obtenida en los mapas de calor se pueden descartar puntos fuera de las zonas de cobertura y trabajar solo con los que, si cumplen cierto nivel de RSSI, en este caso se podrán utilizar dispositivos ESP32 para enviar un mensaje de emergencia a un servidor en línea notificando inmediatamente al personal encargado de seguridad, quien accederá a dichas notificaciones.

El ESP32 es un microcontrolador de bajo costo y bajo consumo energético, pero con alto rendimiento. Se destaca por su capacidad de conectividad inalámbrica, incorporando Wi-Fi y Bluetooth, lo cual lo convierte en una opción ideal para aplicaciones de Internet de las Cosas (IoT). Además, el ESP32 ofrece un amplio rango de funcionalidades como interfaces GPIO, soporte para una variedad de sensores, y capacidades de procesamiento de señales digitales. Es un potente procesador de doble núcleo Tensilica Xtensa LX6 que opera hasta 240 MHz, y un diseño de bajo consumo energético que optimiza la vida útil de la batería en dispositivos portátiles. Además, ofrece gran adaptabilidad mediante soporte para protocolos de comunicación y una amplia gama de GPIO. Su amplia aceptación en la comunidad de desarrolladores se ve reforzada por su compatibilidad con diversos entornos de programación, como Arduino IDE y ESP-IDF de Espressif, facilitando así su integración en una variedad de proyectos. [11]

El ESP32 es un elemento clave en el proyecto de ESPOL para mejorar su infraestructura de seguridad y respuesta a emergencias, contribuyendo significativamente con su robusta conectividad que garantiza una comunicación constante y fiable, crucial para enviar alertas de emergencia. Su adaptabilidad lo hace ideal para el entorno dinámico de un campus universitario, permitiendo su integración con una variedad de sensores y sistemas. La eficiencia en costos y energía del ESP32 lo posiciona como una solución sostenible y económica para implementar tecnologías avanzadas en el campus.

3.4.1 Configuración y Programación del ESP32 para Conectividad Wi-Fi

Para programar el ESP32, se instala inicialmente un entorno de desarrollo integrado (IDE), optando por el Arduino IDE por su compatibilidad y accesibilidad. Este IDE se descarga desde la página oficial de Arduino y se siguen las instrucciones de instalación específicas para el sistema operativo utilizado. Posteriormente, se añaden soportes para el ESP32 en el Arduino IDE, proceso que implica ingresar la URL de la tarjeta de gestión de placas de Espressif Systems en las preferencias del IDE.

Una vez configurado el Arduino IDE, se procede a preparar el ESP32 para la programación. El dispositivo se conecta a la computadora mediante un cable micro USB, seleccionando luego en el Arduino IDE el modelo específico del ESP32 y el puerto adecuado. Dependiendo del sistema operativo, es necesario instalar drivers específicos para que la computadora reconozca correctamente el ESP32, asegurando una comunicación fluida entre el IDE y el microcontrolador.

[12]

Para validar la correcta configuración del entorno de desarrollo, se realiza una prueba de programación cargando y subiendo al ESP32 al programa de ejemplo "Blink". Tras la carga exitosa del programa, se observará el parpadeo del LED integrado en el ESP32, indicando una programación exitosa. Se enfrentan algunos problemas durante este proceso, que se resuelven verificando la funcionalidad del cable USB, asegurando la correcta selección del modelo de ESP32 en el IDE y, en algunos casos, reinstalando los drivers o cambiando el puerto USB.

Para la conexión del ESP32 a la red Wi-Fi de ESPOL, se desarrolla un código específico que maneja la conexión y autenticación Wi-Fi. Este proceso comienza con la inclusión de la biblioteca 'Wi-Fi.h' y la definición de las credenciales de la red Wi-Fi. En la función 'setup()', se inicia la comunicación serial y la conexión Wi-Fi. Un bucle while se utiliza para esperar hasta que el ESP32 se conecte a la red, y una vez conectado, el programa imprime la dirección IP asignada

al ESP32. Este código es esencial para asegurar una conexión efectiva y se adapta para incluir funcionalidades adicionales, como la integración con otros sistemas en el campus de ESPOL. La resolución de problemas durante este proceso implica la verificación de la selección correcta del modelo de ESP32 en el IDE, la funcionalidad del cable USB, y en algunos casos, la reinstalación de drivers o el cambio del puerto USB.

3.4.2 Estrategias de Seguridad y Protección de Datos para el ESP32 en la Red ESPOL

Para asegurar la conexión Wi-Fi del ESP32 en el proyecto de ESPOL, se utilizan protocolos de seguridad robustos como WPA o WPA2, proporcionando una capa de seguridad esencial contra accesos no autorizados. Se mantiene actualizado tanto el firmware del ESP32 como el software del router Wi-Fi, incorporando las últimas mejoras de seguridad. Durante la transmisión de datos a través de Internet, se emplea la encriptación SSL/TLS para proteger la información, especialmente los datos sensibles. Además, se validaron correctamente los certificados de los servidores al usar SSL/TLS, previniendo ataques man-in-the-middle y asegurando una comunicación segura y protegida.

En el manejo de credenciales y datos sensibles en el ESP32, se evita almacenar estas credenciales directamente en el código. En su lugar, se utilizan métodos de almacenamiento seguro como EEPROM o preferencias. También se previene la exposición de datos sensibles en la consola serial, especialmente en ambientes de producción. Para reforzar la seguridad en la red, se conecta el ESP32 a una red Wi-Fi segregada, específicamente diseñada para dispositivos IoT, limitando así el acceso a la red principal y reduciendo el riesgo de ataques. Se implementan firewalls y listas de control de acceso para controlar la interacción de dispositivos con el ESP32 en la red, fortaleciendo la seguridad general del sistema.

Para garantizar la seguridad y el correcto funcionamiento del ESP32 en la red de ESPOL, se mantiene constantemente actualizado el software, incluyendo las bibliotecas y el entorno de

desarrollo, para incorporar las últimas mejoras y correcciones de seguridad. Se realiza un seguimiento y auditoría periódicos del comportamiento del ESP32 en la red, lo que es clave para identificar y responder a cualquier actividad sospechosa. Estas prácticas de actualización y mantenimiento resultan fundamentales para proteger tanto el dispositivo como los datos que se manejan, contribuyendo a una integración segura y eficiente dentro de la infraestructura de red de ESPOL. [13] [14]

3.4.3 Transmisión de alertas de emergencia desde el ESP32 a ESPOL ALERT

Para la implementación del envío de datos desde un ESP32 al sistema ESPOL ALERT, concretamente para la función de un botón de pánico en un tótem, se utiliza un código que emplea protocolos HTTP/HTTPS para comunicarse con la API del sistema ESPOL ALERT. El código desarrollado es el siguiente (ver apéndice B).

El código desarrollado para integrar el ESP32 con el sistema ESPOL ALERT sigue un proceso claro y bien estructurado. Inicialmente, se establece una conexión del ESP32 con la red Wi-Fi de ESPOL, un paso fundamental para permitir la comunicación con el sistema central de alertas. Luego, se implementa un mecanismo para detectar la activación del botón de pánico, un elemento crucial del sistema, cuyo funcionamiento varía según la configuración específica del hardware de cada tótem.

Cuando el botón de pánico es presionado, el ESP32 ejecuta un comando para enviar una alerta al sistema ESPOL ALERT. Esta acción se lleva a cabo mediante una petición HTTP POST a la API del sistema, enviando un mensaje en formato JSON que contiene los detalles de la alerta. Tras el envío, el ESP32 recibe una respuesta del servidor de ESPOL ALERT, que puede ser una confirmación de la recepción de la alerta o información adicional.

Este proceso de envío y recepción de datos resulta crucial para garantizar que las alertas de emergencia sean comunicadas y gestionadas eficazmente por el sistema. Es importante destacar

que el código utilizado es un ejemplo y tiene que ser adaptado a las especificaciones técnicas de la API de ESPOL ALERT y a las características específicas del hardware del ESP32. Además, siempre se consideran aspectos importantes de seguridad, como la encriptación de las comunicaciones y la autenticación adecuada de los dispositivos, para asegurar la integridad y la confidencialidad de la información transmitida. [15]

3.4.4 Configuración de la Infraestructura en la Nube para Gestión de alertas de Tótems

La selección de un servidor en la nube resulta fundamental en el proyecto de tótems de emergencia en ESPOL para garantizar una recolección y procesamiento eficientes de datos. Se opta por servicios como AWS, Google Cloud Platform o Microsoft Azure, considerando su escalabilidad, confiabilidad y amplio rango de herramientas analíticas. La configuración del servidor implica la creación de una instancia en la nube que se adecuaba a las necesidades específicas del proyecto, con un enfoque particular en la configuración de seguridad para proteger tanto la red como los datos. [16]

Se instalan y configuran softwares esenciales como servidores de base de datos y aplicaciones, elementos cruciales para el procesamiento y almacenamiento de los datos recopilados de los tótems. El manejo y almacenamiento de los datos generados por los tótems de emergencia se llevan a cabo en este servidor en la nube, donde servicios de base de datos proporcionan un almacenamiento seguro y adaptable. La selección del tipo de base de datos se basa en la estructura y los requisitos específicos de los datos de emergencia.

Para permitir análisis y respuestas inmediatas a las alertas de los tótems, se implementan herramientas de procesamiento en tiempo real, como AWS Lambda. La seguridad de los datos es una prioridad máxima, aplicándose medidas como la encriptación durante el tránsito y el almacenamiento, y estableciéndose políticas de acceso rigurosas para mantener la confidencialidad e integridad de la información. [17]

Esta infraestructura en la nube, robusta y segura, se convierte en un componente vital para el éxito de los tótems de emergencia en ESPOL, asegurando un manejo efectivo y protegido de los datos y siendo esencial para la eficacia del sistema ESPOL ALERT en situaciones críticas.

3.5 Implementación de Lora en la red de Tótems de Emergencia

Al no disponer de una buena intensidad de señal recibida para todos los puntos de encuentro a lo largo del campus Gustavo Galindo se propone el uso de la tecnología Lora para comunicar aquellos puntos de interés fuera de zonas de cobertura o con intensidad de señal baja o nula como se nota en la tabla 3.2.

Lora es una tecnología de comunicación inalámbrica desarrollada por SemTech. Tiene su propia técnica de modulación CSS (Chirp Spread Spectrum) en la cual los datos son transmitidos codificando su información en variaciones de frecuencia a lo largo del tiempo. Además, funciona en varias bandas de frecuencia dependiendo de la zona geográfica donde se encuentre operando (Para el caso de América se utiliza una frecuencia de 915Mhz). [25]

Lora proporciona largas distancia de transmisión lo cual es útil para añadir puntos de interés adicionales a medida que se implementa el proyecto ESPOL ALERT. Zonas como el mirador del bosque protector o senderos a lo largo del campus en donde no existe cobertura de red institucional pueden ser trabajados con esta tecnología. Al tratarse de dispositivos que requieren ser activados una sola vez para el envío de emergencias lo más recomendable es utilizar una configuración de dispositivos clase A como se mencionó en la sección 1.4.4, es decir que no se encuentren en estado activo todo el tiempo sino únicamente cuando se requiera hacer el envío de un mensaje de alerta al activar el botón de pánico, para esto se realizan configuraciones en el entorno de desarrollo para definir un “SLEEP MODE” o modo de reposo una vez que se haya activado el tótem de emergencia para reportar un siniestro, dicha configuración puede ser observada de forma general en el apéndice C.

Posee un bajo consumo de energía por lo que es eficiente para el uso de baterías durante largos periodos de tiempo lo cual a su vez es importante para mantener activo el sistema de alerta, los costos de los módulos son reducidos haciendo que el desarrollo de este tipo de proyectos sea accesible además de presentar una alta penetración a los obstáculos en zonas con alto follaje y vegetación abundante lo cual es importante para mantener comunicación sin interrupción. Adicionalmente las redes LoraWan pueden ser configuradas de tal forma que la información transmitida sea segura y privada con lo cual no se compromete el sistema de emergencias al estar expuesta a terceros, dependiendo del módulo LORA utilizado se tienen distintas configuraciones posibles para la encriptación de datos.

El uso de la tecnología Lora es esencial para conectar todos los puntos que carecen de cobertura institucional, al ser fácil de implementar y escalables se pueden adaptar a varias aplicaciones y entornos dependiendo de la necesidad del usuario.

3.5.1 Estrategias de Seguridad y Protección de Datos para Lora en la Red ESPOL

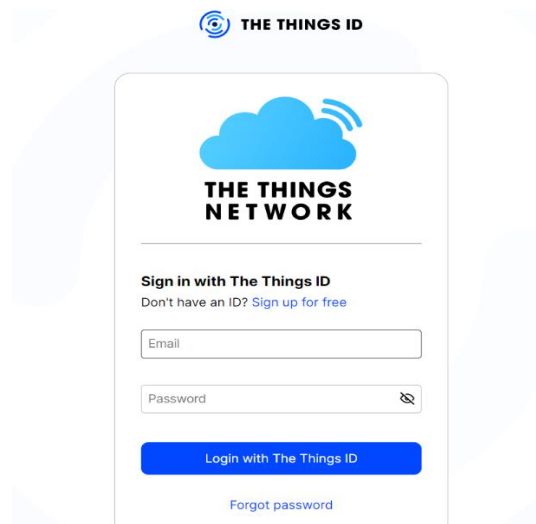
Lora cuenta con varias estrategias de seguridad para proteger los datos enviados hacia los módulos receptores o hacia un servidor central. LoraWan utiliza cifrado AES-128 (Advanced Encryption Standard) para encriptar la información entre nodos y servidores de red [24], estos dispositivos son autenticados y autorizados antes de enviar o recibir información, en algunos módulos Lora será necesario configurar esta autenticación cada vez que se encienda el módulo, en tal caso se debe revisar el datasheet del dispositivo Lora a utilizar (TTGO, RYLR896, etc).

Al utilizar claves criptográficas únicas para cada dispositivo se ofrece una capa adicional de seguridad, sin embargo, al momento de registrar los gateways y nodos en un servidor de red como TTN (The Things Network) también se generan claves para cada uno de ellos con lo cual al registrarse únicamente pueden ser accesibles por el servidor autorizado, para esto se hace intercambio de claves de sesión y autenticación con claves únicas. Dado que este proyecto está

enfocado a un sistema de emergencia el uso de un servidor en TTN para la visualización de los datos es una opción viable dado que permite monitorear y gestionar los dispositivos agregados a la red sean estos nodos (equipos terminales) o puertas de enlace (Gateways) con lo cual se permite responder e identificar accesos no autorizados.

Figura 3.4

Plataforma TTN (*The Things Network*)



Nota. La figura muestra el inicio de sesión en TTN para la creación de proyectos utilizando la tecnología LoraWan.

3.5.2 Transmisión de alertas de Emergencia desde dispositivos Lora a ESPOL ALERT

Como se mencionó en la sección 1.5.4 Lora hace uso de varios dispositivos intermedios para procesar la información recolectada por los nodos o equipos terminales de tal forma que puedan ser visualizados en un servidor de aplicación para posteriormente trabajar con la información transmitida. Como se observa en la figura 1.9 se hace uso de 4 componentes principales los cuales son:

nodos o equipos terminales. Encargados de recolectar la información a transmitir a través de la red Lora, en este caso al ser un botón de pánico para reportar emergencias se pueden utilizar

placas específicas que disponen de este para la activación y reporte del siniestro (Pycom, Dragino Lora IoT, RAK Wireless WisNode Button, etc) o a su vez utilizar placas adicionales como Arduino o ESP32 los cuales se encargarán de simular la acción de encendido de dicho botón de pánico para activar la señal de emergencia. El tipo de data a enviar para reportar la emergencia puede ser un mensaje de texto en formato HTTP.

Puerta de enlace (Gateway). El objetivo de la puerta de enlace es reenviar los paquetes recibidos por los nodos (botones de pánico) de modo que se disponga de información útil que puede procesarse en el servidor de red, las puertas de enlace no procesan directamente la información, pues los nodos usan formato JSON u otro dependiendo del dispositivo final para enviar datos a la nube. Hay microcontroladores programados que trabajan con nodos sin programación previa de forma que se conectan a la puerta de enlace directamente.

Se puede crear un gateway propio utilizando un microordenador Raspberry Pi más algún módulo RAK Lora o a su vez utilizar puertas de enlace previamente desarrolladas y comercializadas. Existen varias opciones para puertas de enlace, se deben tener en cuenta el número de nodos permitidos y temas como la potencia de sensibilidad de transmisión/recepción y el alcance.

Servidor de red. El servidor de red recoge la información proporcionada por los nodos, los cuales a su vez envían estos datos a un gateway y posteriormente al servidor de red en la nube, puede utilizarse dispositivos físicos como una Raspberri Pi para simular un servidor local, sin embargo, esta opción podría traer limitaciones, a su vez se puede utilizar servidores en internet para guardar y administrar los dispositivos que se utilizan en la red como TTN. Al utilizar TTN se deben registrar los nodos y gateways respectivamente definiendo datos importantes como EUI (identificación ID de cada dispositivo) y claves de seguridad para evitar posibles ingresos no autorizados, todo esto es configurado en el servidor en la red.

Se pueden registrar varios dispositivos como microcontroladores diseñados a través de chips (Arduino, ESP32, ESP8266, etc) que dispongan de transceivers Lora. Adicionalmente se dispone de dispositivos “Plug & Play” los cuales cuentan con la parte de la programación previamente realizada de tal forma que se pueden utilizar para comunicarse directamente con los gateway dependiendo del tipo de dispositivo que admitan estos mismos.

Servidor de aplicación. Cuando se dispone de la información en el servidor de red se utiliza un servidor de aplicación para poder visualizar esta data, se utilizan protocolos como MQTT o HTTP dependiendo de la aplicación que se desea desarrollar o utilizar, en el caso del botón de pánico, la función del servidor de aplicación es comunicarse con el servidor de red a través del intercambio de mensajes JSON de tal forma que la información específica dentro de este formato pueda ser utilizada en una interfaz gráfica o más interactiva para quien recibe la información. Al usar TTN (The Things Network) se dispone de un servidor de aplicaciones que proporciona herramientas para gestionar los datos recibidos y crear una aplicación capaz de mostrar en tiempo real un mensaje de emergencia dependiendo del dispositivo accionado para reportar siniestros al sistema ESPOL ALERT. Sin embargo, no es el único servidor disponible, existen otras opciones como ChirpStack, Node-Red, Google Cloud Iot Core, entre otros.

3.6 Análisis de Costos para la Implementación Tecnológica

Desarrollar un análisis de costos para la implementación de tótems de emergencia en el campus ESPOL utilizando tecnología ESP32 y LoRaWAN implica una evaluación integral desde la perspectiva de un ingeniero en telecomunicaciones. El hardware incluye no solo los tótems físicos sino también módulos LoRaWAN, antenas y gateways, todos cuidadosamente seleccionados por su capacidad para funcionar en el entorno específico del campus. Estos dispositivos deben ser lo suficientemente sensibles y robustos para manejar las variaciones de señal causadas por la topografía y la vegetación del campus.

El software es igualmente crucial, ya que debe ser capaz de codificar y decodificar mensajes eficientemente, gestionar la red y asegurar la interoperabilidad con sistemas ya existentes. La seguridad cibernética es una consideración primordial para proteger la red de amenazas digitales.

3.6.1 Costos de implementación para ESP32

La inversión en un sistema basado en ESP32 se justifica tanto por su costo inicial accesible como por los bajos costos operativos, además de los significativos beneficios a largo plazo en términos de eficiencia, seguridad y capacidad de adaptación. El ESP32, con su flexibilidad, bajo consumo y amplio soporte comunitario, proporciona una excelente relación coste-beneficio para proyectos de IoT. Esto es especialmente relevante en aplicaciones de seguridad y automatización como los tótems de emergencia en tu proyecto.[20]

Desde la perspectiva operativa, el ESP32 tiene un consumo de corriente de aproximadamente 80mA durante la operación normal, operando en un voltaje de 3.3V DC (rango de 2.7 a 3.6V) [19]. La gestión de la alimentación es crucial, requiriendo un circuito de filtrado de energía para reducir el ruido y proteger el microcontrolador de fluctuaciones de voltaje y picos de corriente. Además, el ESP32 se puede programar utilizando Arduino IDE y otros entornos de desarrollo como MicroPython, lo que implica costos asociados al desarrollo de software y posibles licencias de software o herramientas de desarrollo.[21] [22]

En cuanto a los costos de mantenimiento, la optimización del inventario es fundamental para evitar pedidos duplicados y mejorar la logística, lo que puede conducir a ahorros significativos. Adoptar un enfoque preventivo y predictivo centrado en los modos de fallo es esencial para reducir los costos a largo plazo. Implementar técnicas de monitorización de la condición y una comunicación asertiva son cruciales para justificar los costos de mantenimiento.

Además, los costos relacionados con el reemplazo de componentes y reparaciones pueden variar según la frecuencia de uso y las condiciones de operación del ESP32. [23]

Los costos de implementación incluyen la adquisición de hardware, como placas de desarrollo ESP32 disponibles a precios accesibles, por ejemplo, el ESP-WROOM-32 ESP32 ESP-32S Development Board el cual más costo de envío está en \$37.33. [23] A esto se suman los costos de componentes adicionales como sensores, actuadores y módulos de comunicación, así como los costos asociados al desarrollo de software específico para el proyecto. También se deben considerar los costos de mano de obra y expertise para el desarrollo, implementación y mantenimiento del sistema.

La implementación de un sistema basado en ESP32 puede conducir a innovaciones que posicionen a la institución a la vanguardia de la tecnología, lo cual es beneficioso tanto desde una perspectiva educativa como de imagen institucional. La eficiencia operativa, la seguridad mejorada y la adaptabilidad a las necesidades futuras proporcionan un sólido retorno de la inversión a largo plazo, justificando así la inversión en el sistema.

De acuerdo a los resultados obtenidos se tiene un total de 17 puntos de encuentro y 3 puntos estratégicos con cobertura de red adecuada para hacer uso de dispositivos ESP32, como se aprecia en la tabla 3.5. Considerando valores un poco por encima del promedio en el mercado actual existente el costo para la implementación de estos puntos es:

Tabla 3.5

Costo inicial implementación ESP32

Equipo	Marca	Proveedor	Precio Unitario	Precio total
ESP32 x20	HiLetgo ESP-WROOM-32 ESP32 ESP-32D	Amazon	\$10.00	\$200 + \$27.34 (importación)

Botón pulsador (Paquete de 100)	DAOKI 100Pcs Tact Button Switch 2 Pin DIP 6x6x5mm	Amazon	\$0.05	\$5 + \$27.06 (Importación)
Protoboard x37	MB-102 830 Ties Breadboard Protoboard	Ali baba	\$0.60	\$22.20 + \$137.08 (Importación)
Caja de paso x20	Caja Para Proyectos Abs 130x170x55mm Diy Caja Plastica Ploma	Innovatech	\$9.35	\$187
Batería de litio x20	PKCELL 18650 3.7V 6700mAh Rechargeable Lithium Battery (ICR18650)	PKCELL	\$6.00	\$120 + Importación
Juego Jumpers x 40	Cable Jumper 40 Pines 20cm Para Protoboard Arduino Dupont	Mercado libre o Tiendas Electrónicas	\$1.75	3 packs a \$5.25
<u>COSTO TOTAL</u>				<u>\$730.93</u>

Nota. La tabla muestra el coste inicial de los dispositivos a utilizarse con tecnología Wi-Fi mediante el uso de equipos ESP32.

Como se nota en la tabla 3.5 se consideran los equipos necesarios para la implementación de tótems de emergencia a través de tecnología Wifi haciendo uso de dispositivos ESP32, no se considera el costo del servidor en red que se utiliza puesto que este depende de la proyección y dimensionamiento del proyecto a implementar. Al requerir del uso de protoboards tanto para el ESP32 como para Lora se puede realizar una compra en conjunto ahorrando costes de importación (se utilizan 37 en total).

3.6.2 Costos de implementación para LoraWan

La instalación y configuración de los tótems y la red LoRaWAN deben ser meticulosas, tomando en cuenta la topografía del campus y los obstáculos que pueden influir en la propagación de la señal. El mantenimiento es un factor continuo que involucra la revisión y actualización

periódica de equipos y software, así como un monitoreo constante del sistema para identificar y solucionar problemas de manera proactiva. Este trabajo será considerado en horas/hombre más adelante.

En términos de costos frente a beneficios, la implementación de LoRaWAN para tótems de emergencia representa una inversión inicial significativa, pero los costos operacionales son comparativamente bajos. Los beneficios se extienden más allá de la seguridad mejorada y la reducción del tiempo de respuesta en emergencias, incluyendo la adaptabilidad a tecnologías futuras y las necesidades cambiantes de la universidad. La evaluación de costos debe ser flexible, considerando la expansión futura de la red, el ciclo de vida de los dispositivos y la evolución de las necesidades de conectividad.

De acuerdo a los resultados obtenidos se tiene un total de 17 puntos (6 puntos de encuentro y 11 puntos estratégicos) a ser implementados con tecnología LoraWan, al trabajar con módulos Lora RAK811 o RAK5205 se hace necesaria la implementación de un botón adicional que ejecute la acción de botón de pánico para él envío de alertas, afortunadamente estos módulos permiten la conexión de dispositivos externos a través de sus pines de propósito general GPIO, de esta forma se debe configurar el dispositivo final para reconocer la activación de dichos botones para enviar un mensaje de alerta. Sin embargo, el RAK5205 está mayormente enfocado para aplicaciones de monitoreo y rastreo, al no desear este consumo constante de energía se opta por el RAK811 para ser configurado como un dispositivo clase A, eficiente en cuanto a consumo de energía.

Tabla 3.6

Costo inicial implementación LoraWan

Equipo	Marca	Proveedor	Precio Unitario	Precio total
(RAK811 + antenna SMA + IPX) x17	RAK Wireless RAK811 Módulo Breakout LPWAN	MAKER STORE	\$20.26	\$344.42

Caja de paso x 17	Caja Para Proyectos Abs 130x170x55mm Diy Caja Plastica Ploma	Innovatech	\$9.35	\$158.95
Batería de litio x17	PKCELL 18650 3.7V 6700mAh Rechargeable Lithium Battery (ICR18650)	PKCELL	\$6.00	\$102 + Importación
Puerta de enlace RAK2287 LPWAN	Módulo concentrador RAK2287 LPWAN mini-pcie basado en Semtech SX1302 IoT Gateway Equipment LoRaWAN con Chip GPS ZOE-M8Q RAK2287	AliExpress	\$149.97	\$149.97
COSTO TOTAL				\$755.34

Nota. La tabla muestra los costos iniciales para la implementación de tótems de emergencia considerando tecnología LoraWan.

3.6.3 Costo total implementación tótems de emergencia

En conjunto, al implementarse ambas tecnologías se debe considerar la estructura física de los tótems de emergencia, se debe considerar las horas hombre trabajadas para el mantenimiento de cada uno de los dispositivos instalados, según las estimaciones del caso se planifica un tiempo de mantenimiento de 1 a 2 horas para los distintos dispositivos, el coste estimado de horas hombre se plantea en \$25 por lo cual considerando un tiempo planificado de 2 horas se tiene un total de \$1850. Además, cada tótem tiene un costo de \$1105.00, considerando los 37 puntos en total se tendría una inversión inicial de \$40885.00 debido a esto se tiene las siguientes consideraciones:

Tabla 3.7

Costo total implementación tótems de emergencia

Tipo de inversión	Precio total
Implementación ESP32	\$790.93

Implementación LoraWan	\$755.34
Infraestructura física tótems de emergencia	\$40885.00
Horas hombre trabajadas	\$1850
COSTO TOTAL	\$44281.27

Nota. La tabla muestra el costo estimado inicial de la implementación del proyecto tomando en cuenta factores como la infraestructura física de los tótems de emergencia, tecnologías utilizadas y el costo de horas hombre trabajadas para los dispositivos.

Capítulo 4

4 Conclusiones y recomendaciones

4.1 Conclusiones

- **Estudio de Cobertura y Selección Tecnológica:** El estudio realizado para la cobertura y selección tecnológica ha identificado que las tecnologías inalámbricas Wi-Fi y LoRaWAN son las más adecuadas para los tótems de emergencia en el Campus Gustavo Galindo Velasco. La integración del ESP32 en este contexto cumple eficazmente con los requisitos de conectividad del sistema ESPOL ALERT. Esta elección tecnológica no solo responde al objetivo general del proyecto, sino que también asegura una implementación efectiva y una respuesta ágil en situaciones de emergencia
- **Evaluación de Zonas Estratégicas:** La evaluación de las zonas estratégicas fue un proceso que implicó una clasificación detallada basada en la topografía, vegetación y cobertura de red institucional. Este análisis meticuloso permitió definir de manera precisa los puntos más idóneos para la ubicación de los tótems de emergencia. Esta clasificación y selección de zonas estratégicas se alinea directamente con uno de los objetivos específicos del proyecto, garantizando una cobertura de respuesta y comunicación óptima en situaciones de emergencia. Este enfoque estratégico y metódico subraya la importancia de una planificación detallada y un diseño de red inalámbrica que se adapte a las características únicas del campus.
- **Análisis Presupuestario y Viabilidad Económica:** El análisis presupuestario realizado ha sido minucioso y detallado, enfocándose en la identificación de los dispositivos esenciales para asegurar una conectividad efectiva de los tótems de emergencia. Este análisis ha demostrado no solo la viabilidad económica de implementar el sistema ESPOL ALERT en el campus, sino que también resalta su alineación con el tercer objetivo específico del proyecto. Este enfoque garantiza que la inversión necesaria para la implementación del

sistema se ajusta a los parámetros financieros previstos, asegurando una implementación eficiente y sostenible a largo plazo.

- **Mejora en la Seguridad y la Capacidad de Respuesta:** La implementación de los tótems de emergencia, siguiendo las recomendaciones del estudio, representa un avance significativo en la seguridad y capacidad de respuesta del campus ante emergencias. Este enfoque responde directamente al objetivo principal del proyecto, demostrando el impacto tangible y práctico que tendrá en la mejora de los protocolos de seguridad y eficiencia en la gestión de situaciones críticas en el campus.

4.2 Recomendaciones

- Es importante considerar que, durante la implementación de dispositivos que requieren conexión a Internet, la Escuela Superior Politécnica del Litoral (ESPOL) utiliza el protocolo 802.11x para la autenticación de usuarios. Este protocolo garantiza un proceso de conexión seguro y confiable, esencial para la efectiva operatividad de los equipos en la red institucional.
- Para optimizar los costos del proyecto durante la fase de implementación, se prioriza el uso de la infraestructura de red existente. Sin embargo, en situaciones donde la señal Wi-Fi es insuficientemente fuerte o la cobertura es inadecuada debido a la escasez de puntos de acceso, se recurre a la tecnología LoRa como una solución alternativa. Esta tecnología se destaca por su capacidad para proporcionar conectividad en áreas con limitaciones de infraestructura de red, garantizando así una implementación eficiente y efectiva.
- El estudio de cobertura institucional se ha llevado a cabo en base a las configuraciones actuales implementadas por GTS. Esto implica que cualquier modificación futura, ya sea ajustes en los puntos de acceso existentes o la implementación de nuevos puntos, requerirá la realización de un estudio de cobertura adicional. Por tanto, es importante destacar que

los resultados y conclusiones del estudio actual son aplicables únicamente a la infraestructura de red tal como está configurada hasta la fecha de este informe.

REFERENCIAS

- [1] J. Jones. (1991, Mayo 10). Networks (2nd ed.) [Online]. Disponible en: <http://www.atm.comApéndices>
- [2] Feredación de Enseñanza de CC.OO de Andalucía, «La conectividad Inalámbrica: un enfoque para el alumno,» ISSN:1989-4023, Andalucía, 2010.
- [3] Feredación de Enseñanza de CC.OO de Andalucía, «La conectividad Inalámbrica: un enfoque para el alumno,» ISSN:1989-4023, Andalucía, 2010.
- [4] CISCO, «¿Qué es Wi-Fi?,» CISCO, 2021. [En línea]. Available: https://www.cisco.com/c/es_mx/products/wireless/what-is-Wi-Fi.html. [Último acceso: 2023].
- [5] LoRa Alliance, «LoRaWAN What is it?,» San Ramon CA, 2015.
- [6] CAT SENSORS, «TECNOLOGÍA LORA Y LORAWAN,» 2020. [En línea]. Available: <https://www.catsensors.com/es/lorawan/tecnologia-lora-y-lorawan>. [Último acceso: 2023]
- [7] Semtech Corporation , «LoRa Modulation Basic,» 2015.
- [8] G. M. Carrión, «Desarrollo De Una Pasarela LORA y evaluación de prestaciones,» Valencia, Departamento de Comunicaciones, 2017, p. 10.
- [9] P.C. Yáñez, «ESTUDIO DE LOS CANALES CON DESVANECIMIENTO SOBRE REDES FIJAS Y MÓVILES EN SISTEMAS DE RADIO COMUNICACIÓN», 2009
- [10] O.G. Barrera, «Contaminación ambiental por ondas electromagnéticas no ionizantes producto de tecnologías inalámbricas en ambientes al aire libre,» MUTIS, Facultad de Ciencias Naturales e Ingeniería de la UJTL, 2018.
- [11] Polaridad.es, "Todo lo que necesitas saber sobre el ESP32: un microcontrolador versátil," polaridad.es. Disponible en: <https://www.polaridad.es/todo-sobre-el-esp32/>

- [12] J. Beunza, "ESP32 conexión via Wi-Fi," Juanjo Beunza, 25 junio 2020. Disponible en: <https://www.juanjobeunza.com/esp32-Wi-Fi/>.
- [13] Espressif Systems, "Wi-Fi Security - ESP32," ESP-IDF Programming Guide. Disponible en: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/Wi-Fi.html>.
- [14] ElectroSoftCloud, "Seguridad en tu ESP32 con ESP-Now," electrosoftcloud.com. Disponible en: <https://www.electrosoftcloud.com/seguridad-en-tu-esp32-con-esp-now/>.
- [15] Microcontrollers Lab, "ESP32 Rest API Web Server GET and POST Examples with Postman API," microcontrollerslab.com. Disponible en: <https://microcontrollerslab.com/esp32-rest-api-web-server-get-post-examples-postman-api/>.
- [16] AWS Cloud Operations & Migrations Blog, "Alarms, incident management, and remediation in the cloud with Amazon CloudWatch," aws.amazon.com. Disponible en: <https://aws.amazon.com/blogs/mt/alarms-incident-management-and-remediation-in-the-cloud-with-amazon-cloudwatch/>.
- [17] InfoQ, "A Comprehensive Guide to Building Event-Driven Architecture on Azure, AWS, and Google Cloud," www.infoq.com. Disponible en: <https://www.infoq.com/articles/event-driven-architecture-azure-aws-google/>.
- [18] Polaridad.es, "Alimentación del ESP32: todo lo que debes saber," Polaridad.es. [En línea]. Disponible en: <https://www.polaridad.es/alimentacion-del-esp32-todo-lo-que-debes-saber/>. [Accedido: 12-ene-2024].
- [19] RobotUNO, "Preguntas frecuentes ESP32," www.robotuno.com. [En línea]. Disponible en: <https://www.robotuno.com/preguntas-frecuentes-esp32/>. [Accedido: 16-ene-2024].
- [20] Acortes Software, "Tutorial ESP32," www.acortes.co. [En línea]. Disponible en: <https://www.acortes.co/tutorial-esp32/>. [Accedido: 14-ene-2024].

[21] Industrial Shields, "Industrial ESP32 PLC - Product Range ideal for Internet of Things," www.industrialshields.com. [En línea]. Disponible en: <https://www.industrialshields.com/industrial-esp32-plc-product-range-ideal-for-internet-of-things>. [Accedido: 14-ene-2024].

[22] Infraspak Blog, "Guía de costes de mantenimiento: cómo calcular y cómo reducir," blog.infraspak.com. [En línea]. Disponible en: <https://blog.infraspak.com/es/costes-de-mantenimiento/>. [Accedido: 16-ene-2024].

[23] Amazon.com, "ESP-WROOM-32 ESP32 ESP-32S Development Board 2.4GHz Dual-Mode Wi-Fi + Bluetooth Dual Cores Microcontroller Processor Integrated with Antenna RF AMP Filter AP STA Compatible with Arduino IDE (3PCS)," www.amazon.com [En línea]. Disponible en: <https://www.amazon.com/ESP-WROOM-32-Development-Bluetooth-Microcontroller-Compatible/dp/B0718T232Z>. [Accedido: 16-ene-2024].

[24] N. C. Romero, "Mejora de la seguridad en redes LoRaWAN," Tesis de Grado, Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación, https://wpa.ugr.es/~jorgenavarro/thesis/2019_TFG_NataliaChinchillaRomero.pdf. [Accedido: 20-ene-2024].

[25] S. Sabas, "Haciendo IOT Con Lora: Capitulo 2.- tipos y clases de nodos," Medium, <https://medium.com/beelan/haciendo-iot-con-lora-capitulo-2-tipos-y-clases-de-nodos-3856aba0e5be> [Accedido: 20-ene-2024].

[26] Maker Store, "RAK Wireless RAK811 Módulo Breakout LPWAN," www.maker-store.es. [En línea]. Disponible en: <https://maker-store.es/home-automation/industrial-automation/lora-iot-sensoren/3296/rak-wireless-rak811-modulo-breakout-lpwan> [Accedido: 21-ene-2024].

[27] AliExpress, "Módulo concentrador RAK2287 LPWAN mini-pcie basado en Semtech SX1302 IoT Gateway Equipment LoRaWAN con Chip GPS ZOE-M8Q RAK2287,"

es.aliexpress.com. [En línea]. Disponible en: <https://es.aliexpress.com/i/1005002609853629.html> [Accedido: 21-ene-2024].

[28] Pkcell, “PKCELL 18650 3.7V 6700mAh Rechargeable Lithium Battery Pack with PCM and Connector Supplier,” www.batterypkcell.com [En línea]. Disponible en: <https://www.batterypkcell.com/pkcell-18650-3-7v-6700mah-rechargeable-lithium-battery-pack-product/> [Accedido: 21-ene-2024].

[29] Mercado libre, “Caja Para Proyectos Abs 130x170x55mm Diy Caja Plastica Ploma,” www.mercadolibre.com [En línea]. Disponible en: https://articulo.mercadolibre.com.ec/MEC-517973669-caja-para-proyectos-abs-130x170x55mm-diy-caja-plastica-ploma-JM#position=18&search_layout=stack&type=item&tracking_id=f3e5a4eb-8140-4848-b261-254cd60fc1bc [Accedido: 21-ene-2024].

[30] Alibaba, “MB-102 830 Ties Breadboard Protoboard,” www.alibaba.com [En línea]. Disponible en: https://www.alibaba.com/product-detail/MB-102-830-Ties-Breadboard-Protoboard_1600465472991.html?spm=a2700.7735675.0.0.6e91twfOtwfOua [Accedido: 21-ene-2024].

APÉNDICES

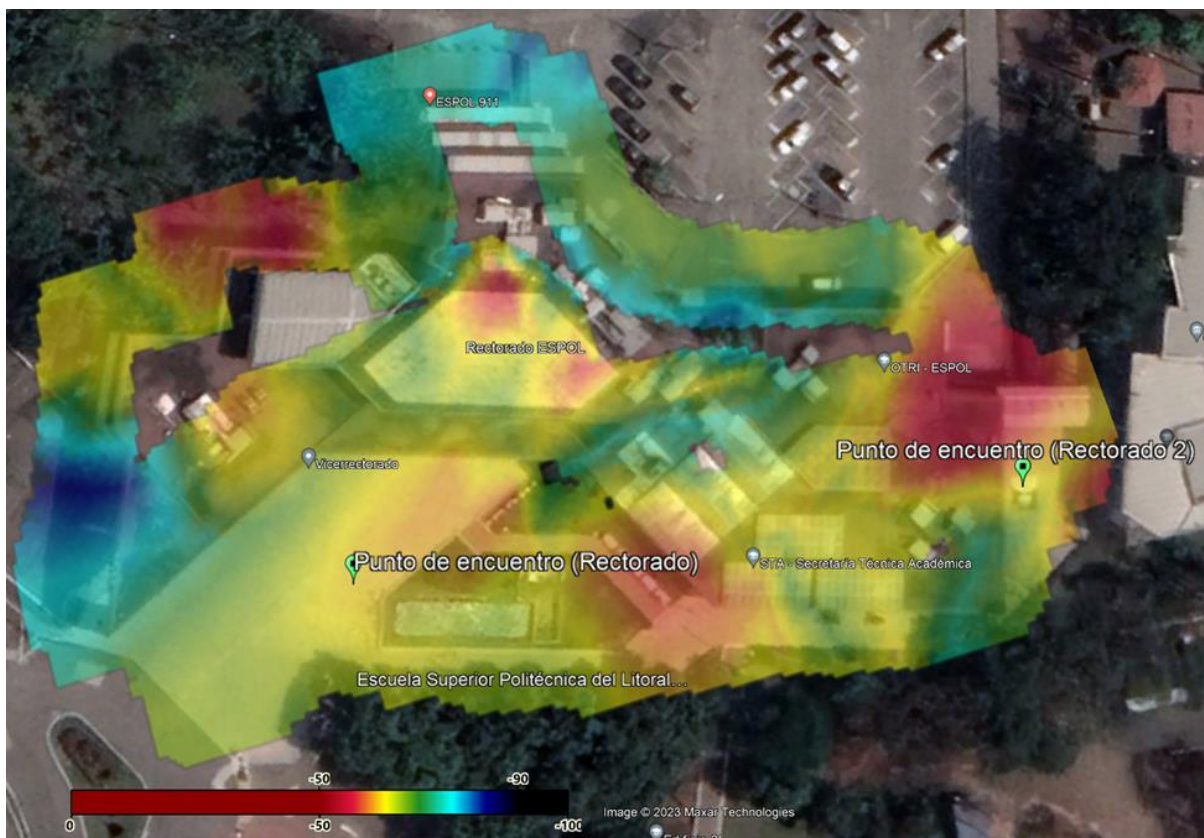
Apéndice A. Mapas de cobertura

En esta sección se ingresarán los distintos mapas de cobertura obtenidos a través del software “Acrylic Wi-Fi Heatmaps”. Los distintos puntos de encuentro mencionados en la tabla 2.1 han sido añadidos en sus respectivas zonas para notar de manera visual si dichos puntos se encuentran o no en zonas con intensidad de señal recibida fuerte de tal forma que pueda ser seleccionado como un punto tentativo de instalación para los tótems de emergencia.

A.1 Puntos de encuentro Rectorado

Figura A1

Mapa de cobertura Rectorado

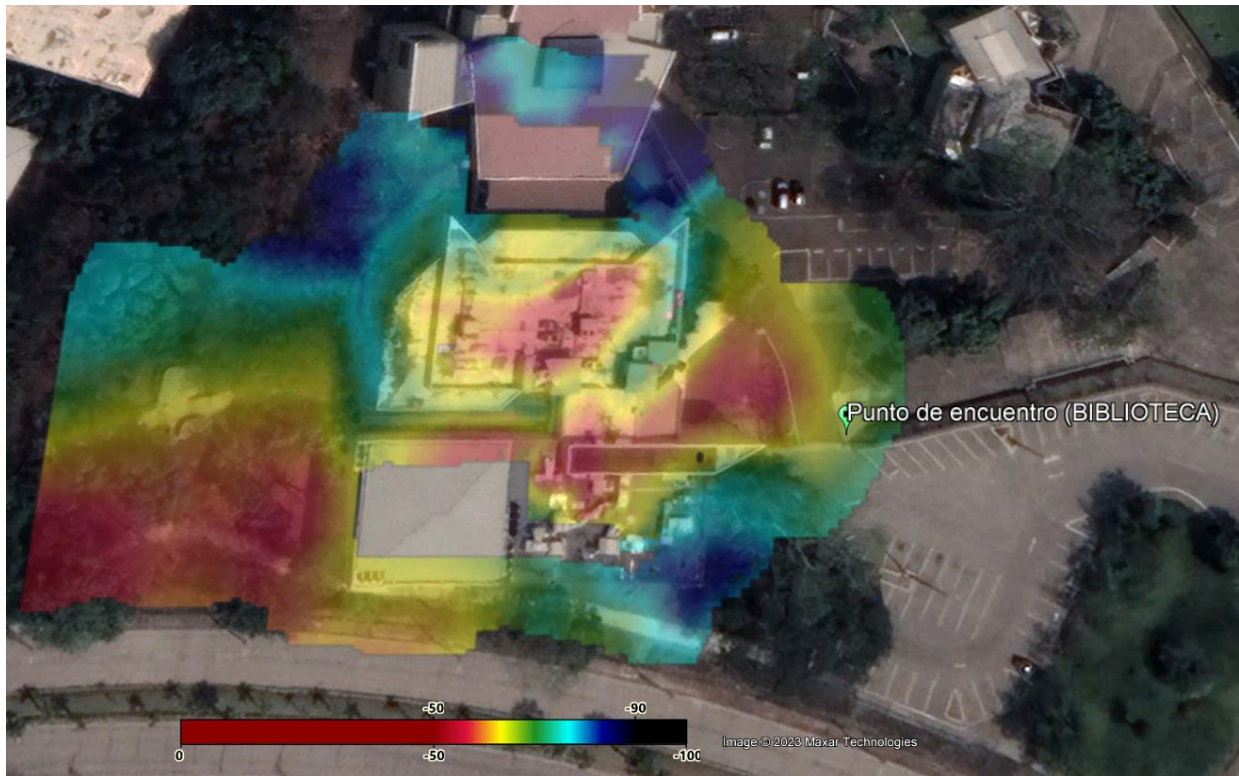


Nota. La figura muestra los puntos de encuentro ubicados en el área de rectorado. Ambos puntos se encuentran dentro de una zona con alto nivel de potencia recibida por lo cual son aptos para la ubicación de tótems de emergencia.

A.2 Puntos de encuentro CIB

Figura A2

Mapa de cobertura CIB



Nota. La figura muestra el punto de encuentro ubicado en el área de biblioteca central.

Dicho punto se encuentra dentro de una zona con alta intensidad de potencia recibida (RSSI) por lo cual dicho punto de encuentro es óptimo para la ubicación de un tótem de emergencia.

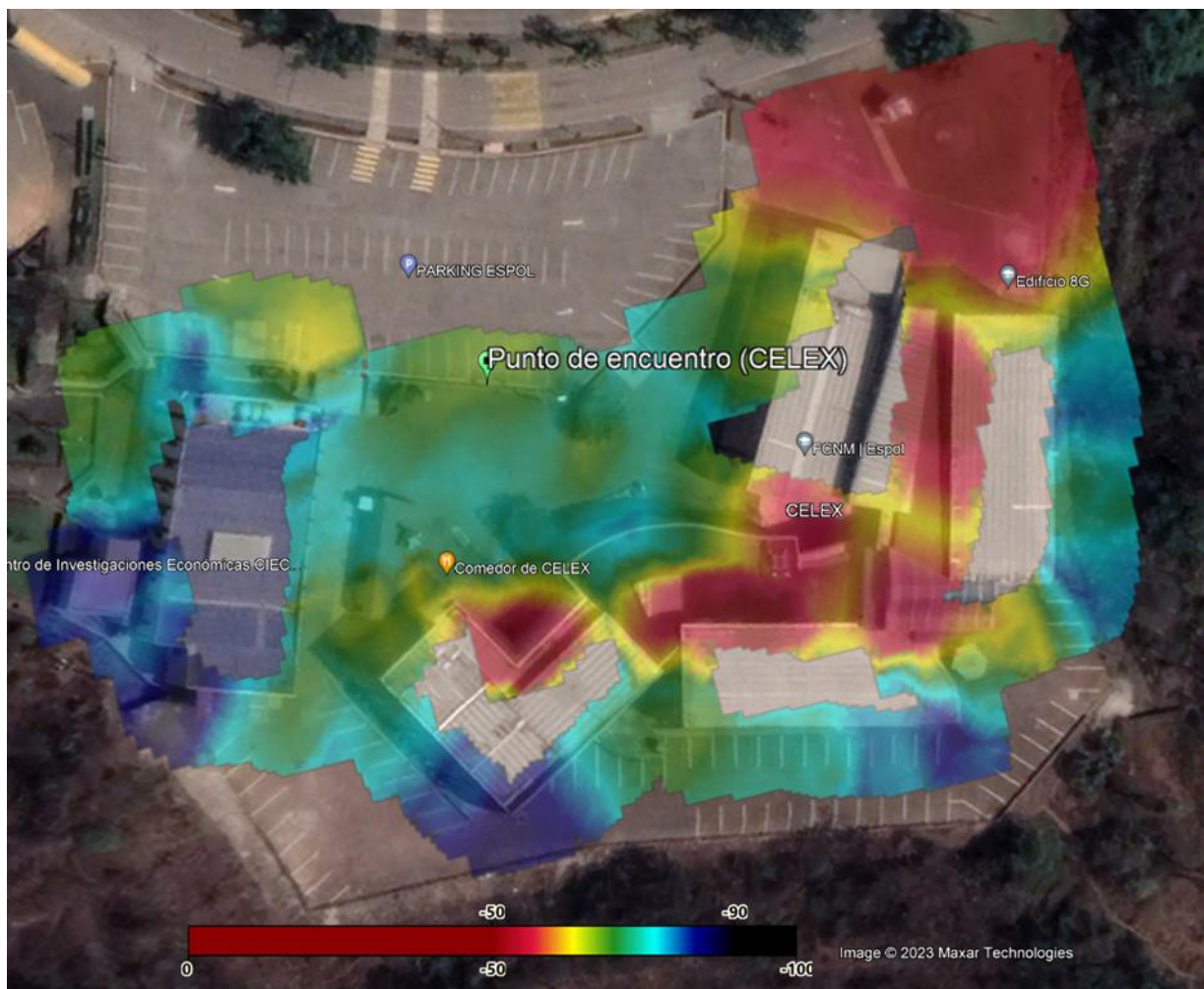
Sin embargo, existe un área extensa de alta intensidad de señal por lo cual el dispositivo podría ser ubicado estratégicamente a lo largo de esta zona. Si se nota detenidamente, en la zona del ingreso posterior a la biblioteca subiendo por las escaleras existe una buena intensidad de señal debido a la instalación de repetidores de red, debido a esto es posible la ubicación de un tótem en dicha zona al haber alta densidad de tráfico estudiantil.

Al ser una zona con factor de riesgo de accidente debido a la presencia de escalones, en este tipo de situaciones el disponer de una respuesta inmediata ante cualquier tipo de emergencia es importante para tener un tiempo de reacción adecuado en este tipo de situaciones.

A.3 Puntos de encuentro CELEX

Figura A3

Mapa de cobertura CELEX



Nota. La figura muestra los puntos de encuentro ubicados en el área de CELEX.

De acuerdo al mapa de calor visualizado en la figura A3, el punto de encuentro está ubicado en una zona con intensidad de señal recibida moderada, sin embargo, las zonas con mayor intensidad de señal recibida se encuentran en los pasillos del edificio 8G y Celex por lo cual dichas

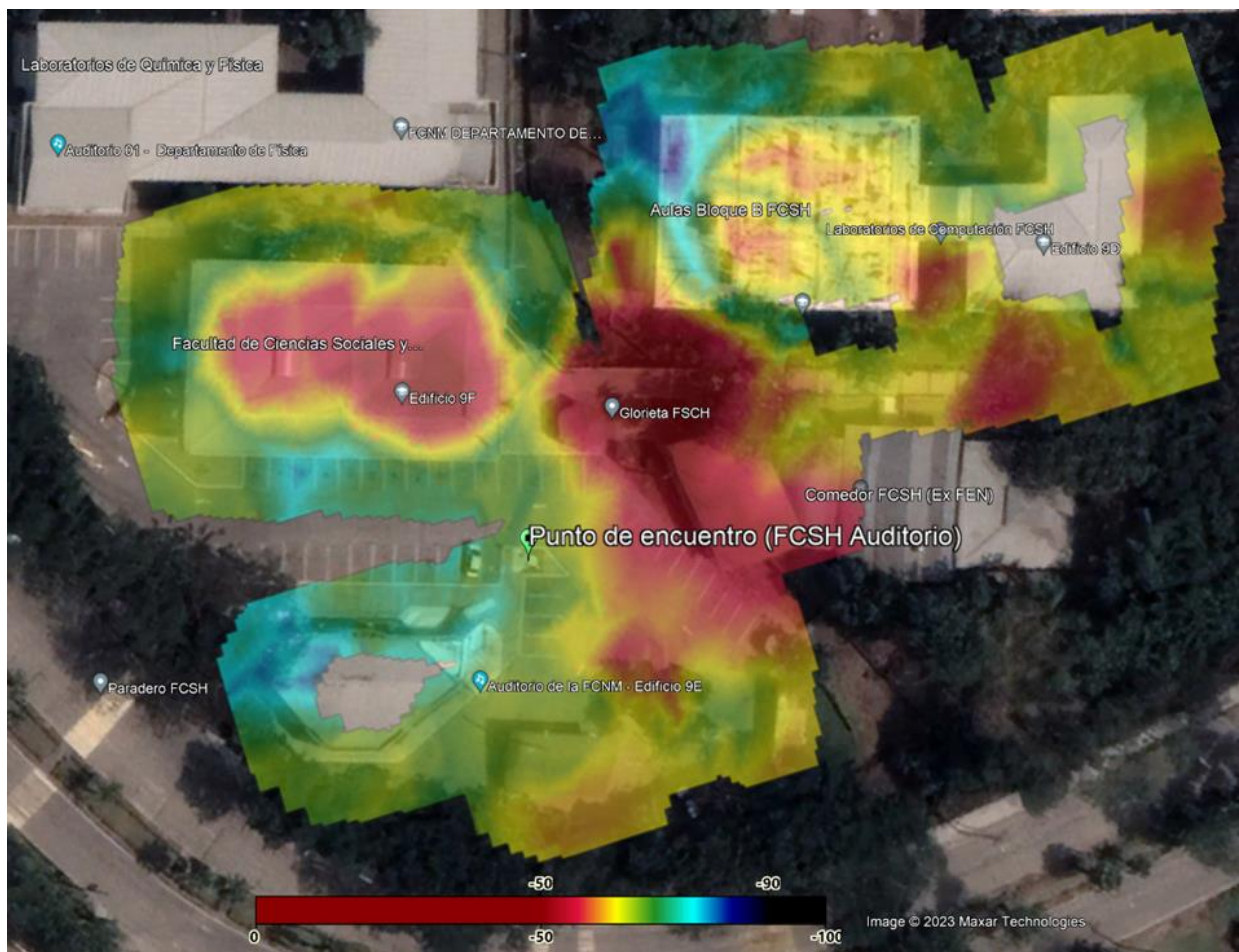
zonas son más recomendables para la instalación de un tótem de emergencia al ser zonas con alta densidad de tráfico estudiantil.

A.4 Puntos de encuentro FCSH

Para la facultad FCSH se tienen los mapas de cobertura correspondientes al edificio administrativo y aulas alrededor del bloque 9F. Analizando cada uno se tienen los siguientes mapas de cobertura.

Figura A4.1

Mapa de cobertura FCSH



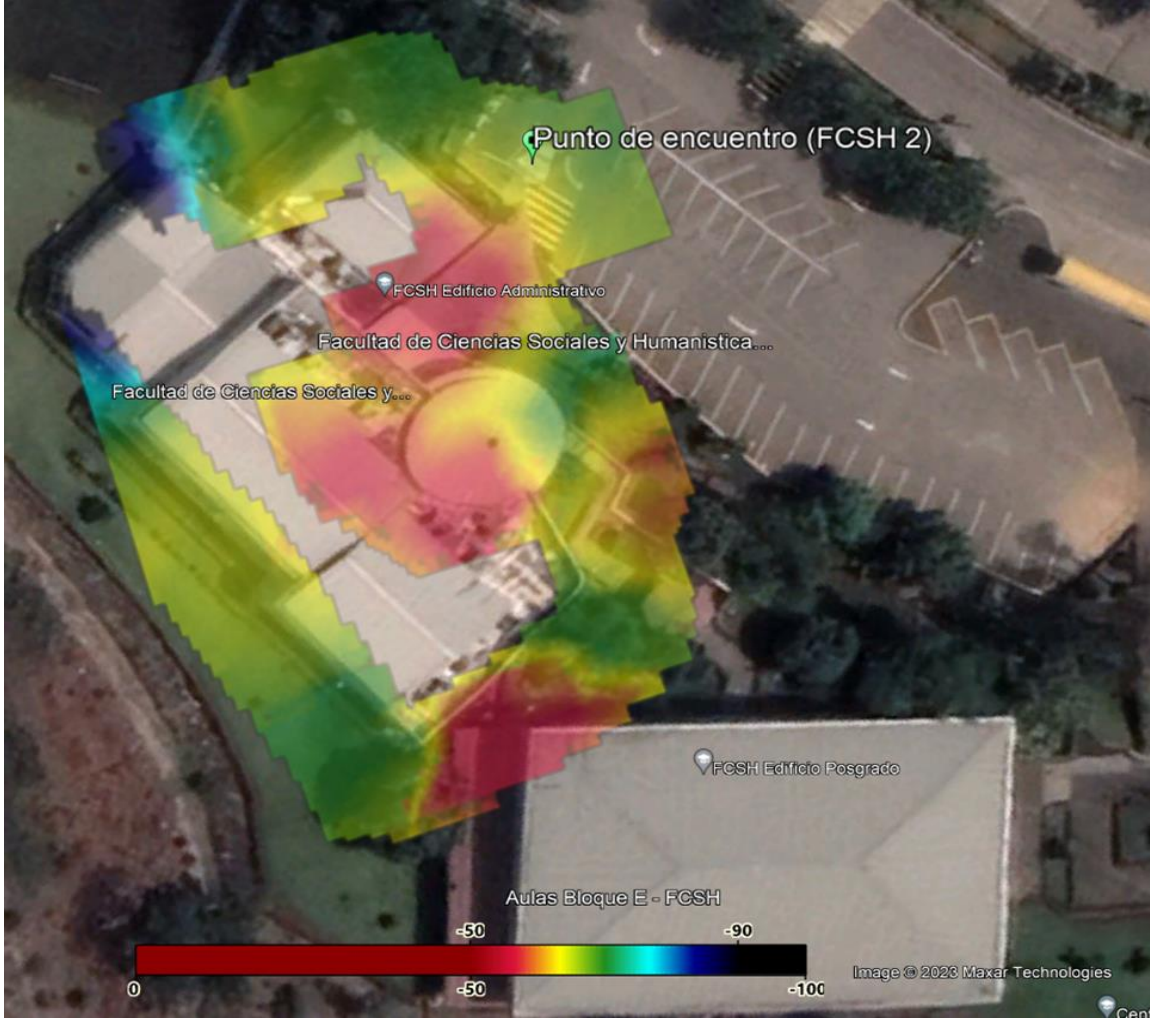
Nota. La figura muestra los puntos de encuentro ubicados en el área de FCSH.

El punto de encuentro ubicado a la salida del auditorio se encuentra en una zona con nivel de intensidad de señal recibida moderada. El área de comedores y glorieta de FCSH presentan

mayor intensidad de señal recibida donde podría ubicarse un tótem de emergencia considerando también el tráfico estudiantil en dichas zonas. Cabe mencionar que existe un alto nivel de intensidad de señal recibida en el área del comedor por lo que se disponen de varias zonas con buena cobertura de red para la instalación de equipos que trabajen con tecnología Wi-Fi, al haber zonas cercanas con una intensidad moderada no se presentaría problemas al momento de enlazar dichos equipos a una red institucional, de cualquier forma, estas áreas con buena intensidad de señal son óptimas para la ubicación de tótems de emergencia.

Figura A4.2

Mapa de cobertura FCSH (Edificio administrativo)



Nota. La figura muestra el punto de encuentro ubicado en el edificio administrativo de la FCSH.

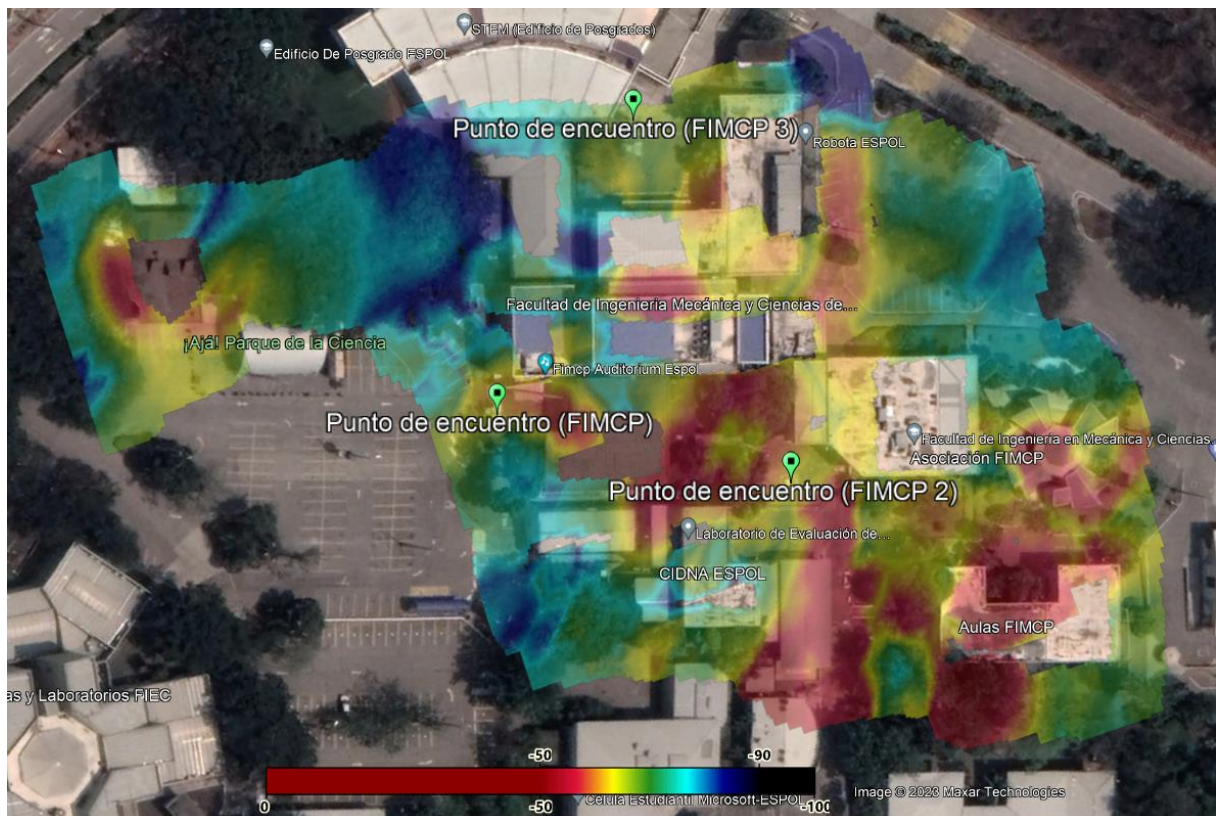
De acuerdo al mapa de calor visualizado en la figura A4.2 se observa el punto de encuentro dentro de una zona con intensidad de señal recibida moderada por lo cual puede ser un lugar tentativo de instalación para un tótem de emergencia.

Al tratarse del edificio administrativo de la FCSH el tráfico estudiantil en esta zona no es tan denso como en otros sectores del campus, sin embargo, al haber presencia de buena intensidad de señal recibida es viable para la instalación de tótems mediante el uso de tecnología Wi-Fi para el envío de alertas al sistema ESPOL ALERT.

A.5 Puntos de encuentro FIMCP

Figura A5

Mapa de cobertura FIMCP



Nota. La figura muestra los puntos de encuentro ubicados en el área de FIMCP.

El mapa de cobertura indica los 3 puntos de encuentro a lo largo de la facultad FIMCP como se observa en la figura A5. Al encontrarse dentro de un rango moderado de intensidad de

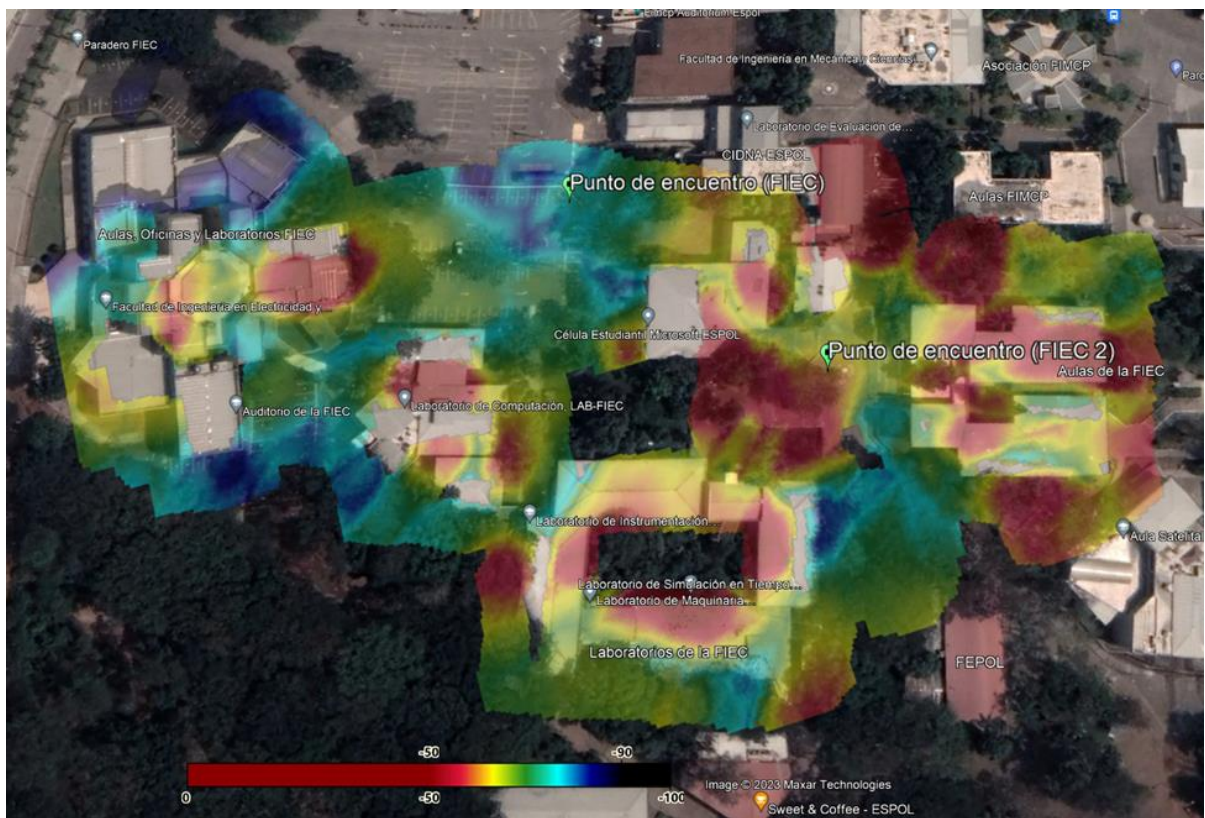
señal recibida todos los puntos en dicha zona son óptimos para ser elegidos como puntos de instalación para los respectivos tótems de emergencia mediante el uso de tecnología Wi-Fi para el reporte de emergencias.

A.6 Puntos de encuentro FIEC

Para el caso de FIEC se tienen 2 mapas de calor existentes, al disponer de redes adicionales en la facultad FIEC, se ingresará entonces el resultado del mapa de cobertura para las redes de interés (ESPOL, ESPOL Wi-Fi & Eduroam) como también las redes propias de FIEC (Fiec, Fiec Wireless) las cuales suplen de cobertura en ciertas áreas del edificio 11A satisfaciendo la demanda de conectividad en dicha zona.

Figura A6.1

Mapa de cobertura FIEC (Redes ESPOL, ESPOL Wi-Fi & Eduroam)



Nota. La figura muestra los puntos de encuentro ubicados en el área de FIEC, en este caso se analizan las redes “ESPOL, ESPOL Wi-Fi y Eduroam”.

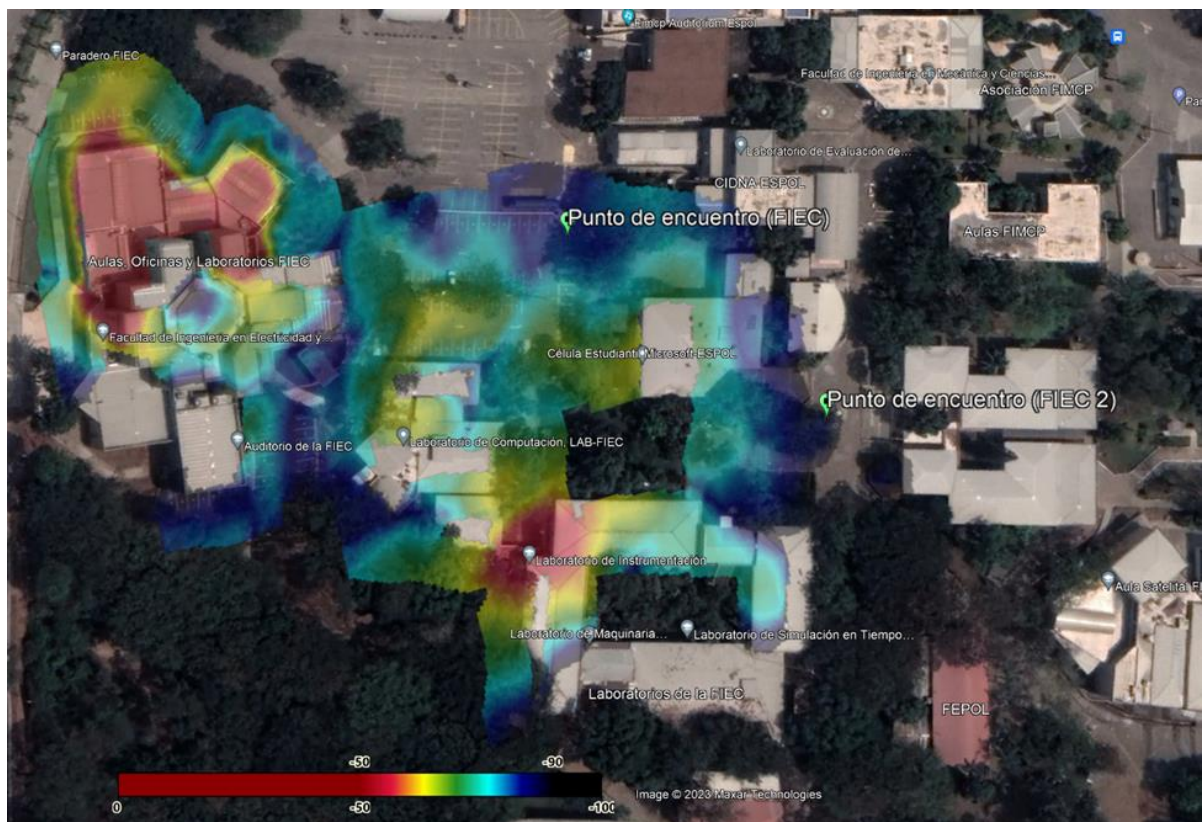
Como se puede observar en la figura A6.1 el punto de encuentro “FIEC” se encuentra en una zona con intensidad de señal recibida deficiente por lo cual no es óptimo para la ubicación de un tótem de emergencia.

Por otro lado, el punto de encuentro “FIEC 2” se encuentra dentro de una zona con intensidad de señal recibida moderada motivo por el cual solo este punto es elegible para la ubicación de algún equipo a trabajar con tecnología Wi-Fi en su respectivo tótem de emergencia.

Se puede notar el fenómeno de absorción para la señal Wi-Fi en algunos puntos con alto follaje de vegetación motivo por el cual se debe considerar al momento de realizar la instalación de los tótems de emergencia en los puntos de encuentro ubicados alrededor de esta área.

Figura A6.2

Mapa de Cobertura FIEC (Redes FIEC & FIEC Wireless)



Nota. La figura muestra los puntos de encuentro ubicados en el área de FIEC bajo la cobertura de las redes FIEC & FIEC Wireless.

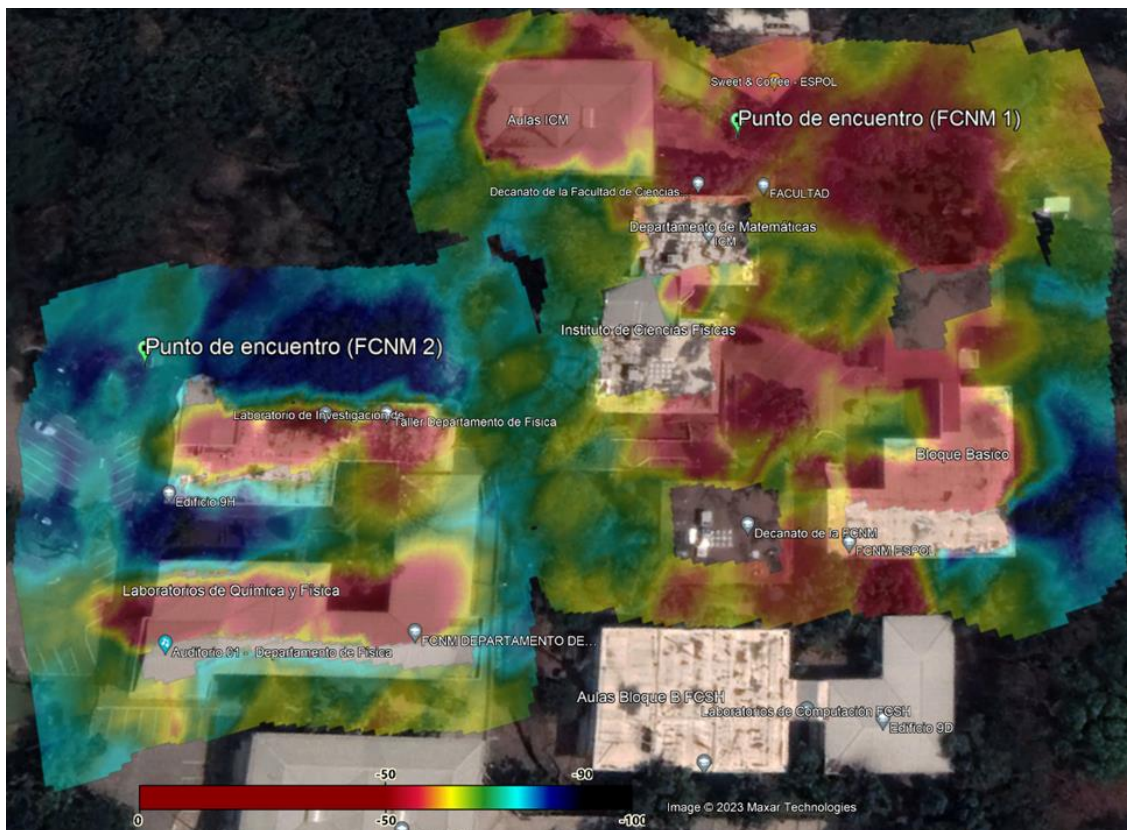
De acuerdo al mapa de calor observado en la figura A6.2 ninguno de los 2 puntos de encuentro se ubican dentro una zona con intensidad de señal recibida alta por lo cual quedan descartados para trabajar con estas redes, si se compara con la figura A6.1 estas redes propias de FIEC proporcionan cobertura adicional que las otras redes no brindan sobre todo para el edificio 11A.

En caso de trabajar con estas redes únicamente un área de los laboratorios de FIEC es óptima para la instalación de tótems de emergencia con tecnología Wi-Fi a través del uso de dispositivos ESP32. Por ende, no es recomendable el uso de estas redes si se toman en consideración la ubicación tentativa de los tótems en los puntos de encuentro en esta área.

A.7 Puntos de encuentro FCNM

Figura A7

Mapa de Cobertura FCNM



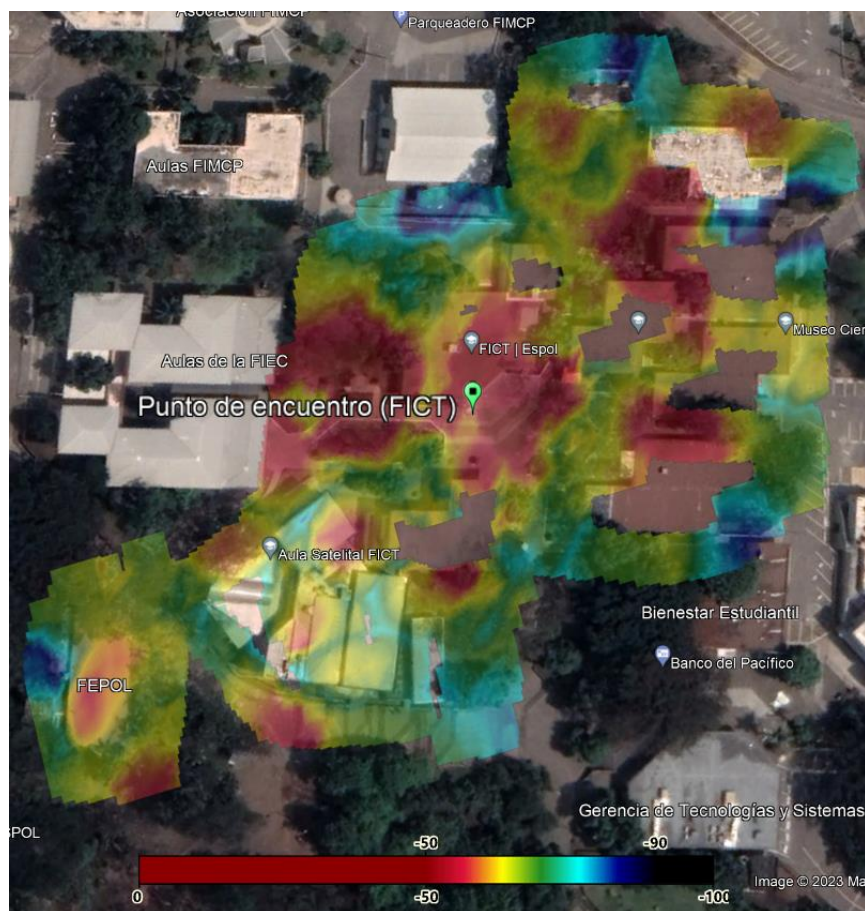
Nota. La figura muestra los puntos de encuentro ubicados en el área de FCNM.

Como se observa en la figura A7 el punto de encuentro “FCNM 1” se encuentra dentro de una zona con alta intensidad de señal recibida, considerando el tráfico de estudiantes en dicha zona debido al establecimiento “Sweet & Coffe” es un buen punto para la ubicación de un tótem de emergencia mediante el uso de tecnología Wi-Fi. Por otro lado, el punto de encuentro “FCNM 2” se halla ubicado en una zona con baja intensidad de señal recibida esto debido a la lejanía con el edificio principal de laboratorios en donde se encuentran ubicados los puntos de acceso y además por el efecto de la vegetación sobre la intensidad de señal recibida en dicho punto, debido a esto este no es apto para utilizar tecnología Wi-Fi para el envío de emergencias.

A.8 Puntos de encuentro FICT

Figura A8

Mapa de Cobertura FICT



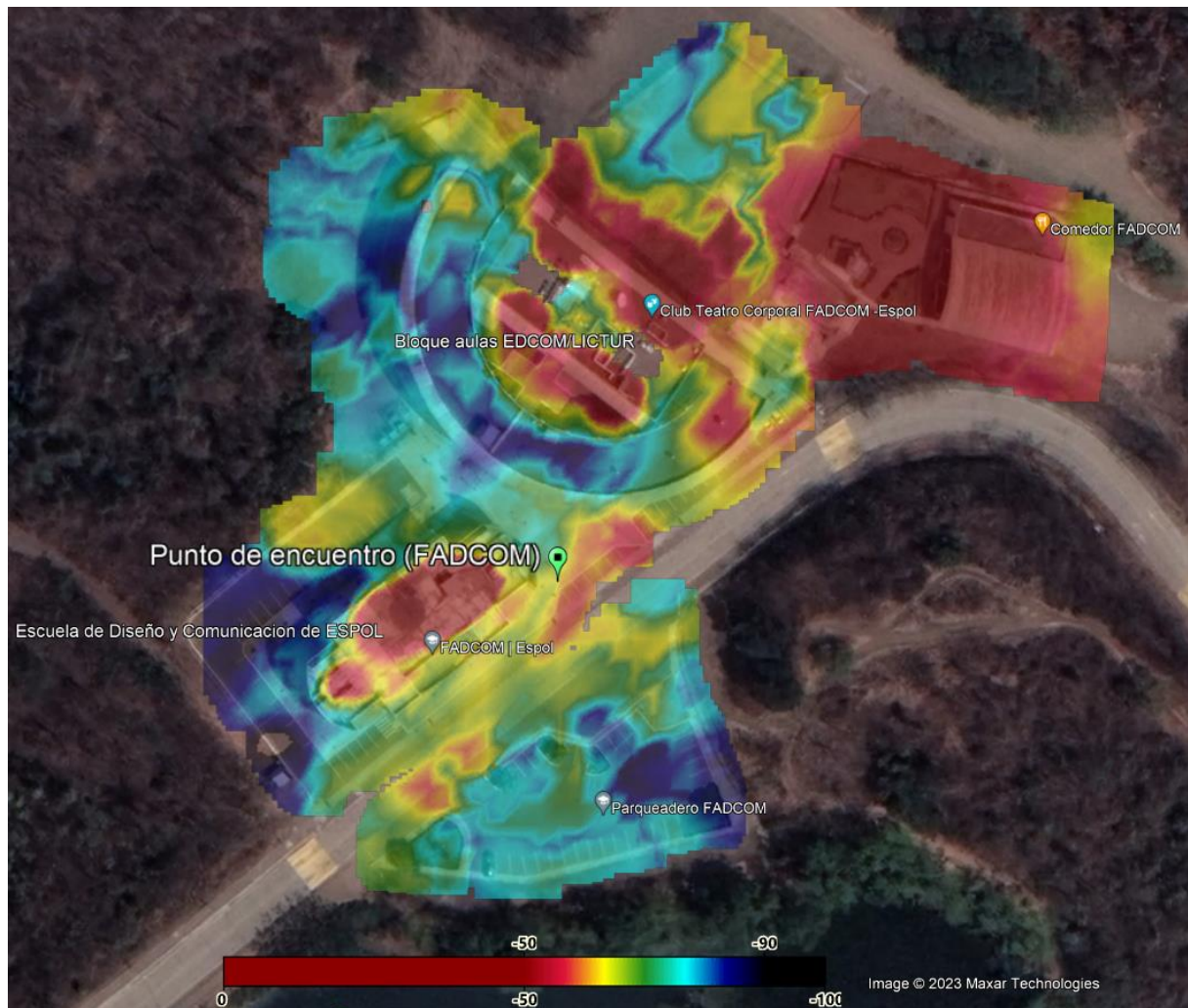
Nota. La figura muestra los puntos de encuentro ubicados en el área de FICT.

El punto de encuentro ubicado en la parte exterior del edificio principal de la FICT se encuentra en una zona con alta intensidad de señal recibida por lo cual es un lugar óptimo para la instalación de un tótem de emergencia. Además, la presencia de un repetidor en el área verde cercana permite un mayor rango de cobertura de red institucional en caso de instalación de tótems adicionales.

A.9 Puntos de encuentro FADCOM

Figura A9

Mapa de Cobertura FADCOM



Nota. La figura muestra el punto de encuentro ubicado en el área de FADCOM.

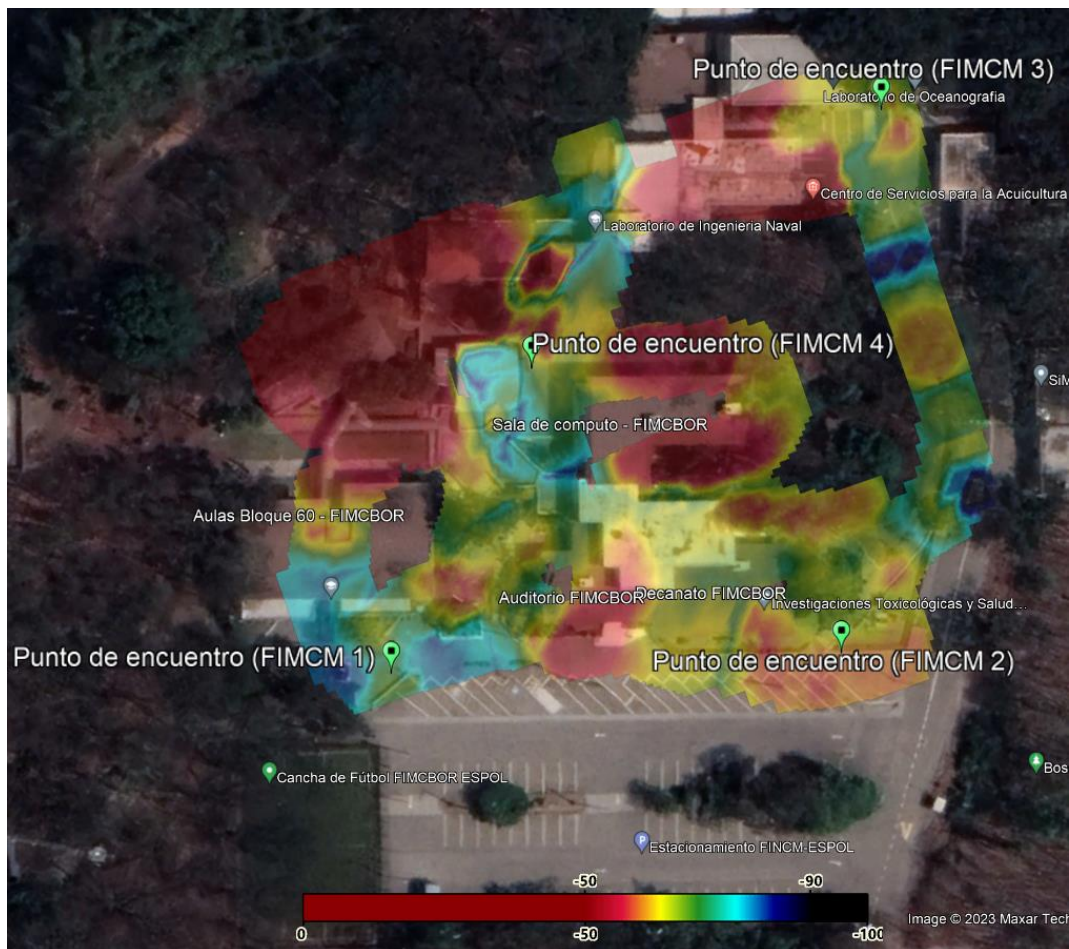
En base al mapa de cobertura visualizado en la figura A9, el punto de encuentro se ubica en una zona con intensidad de señal recibida moderada por lo cual es un lugar tentativo para la instalación de un tótem de emergencia utilizando tecnología Wi-Fi para el envío de alertas.

Sin embargo, existen otras zonas con mayor intensidad y donde hay mayor flujo de estudiantes como por ejemplo el sector de pasillos y comedor destacando una intensidad todavía mayor a la existente en el punto de encuentro “FADCOM”, de este modo se disponen de varios puntos tentativos para la instalación de tótems de emergencia.

A.10 Puntos de encuentro FIMCM

Figura A10

Mapa de Cobertura FIMCM



Nota. La figura muestra los puntos de encuentro ubicados en el área de FIMCM.

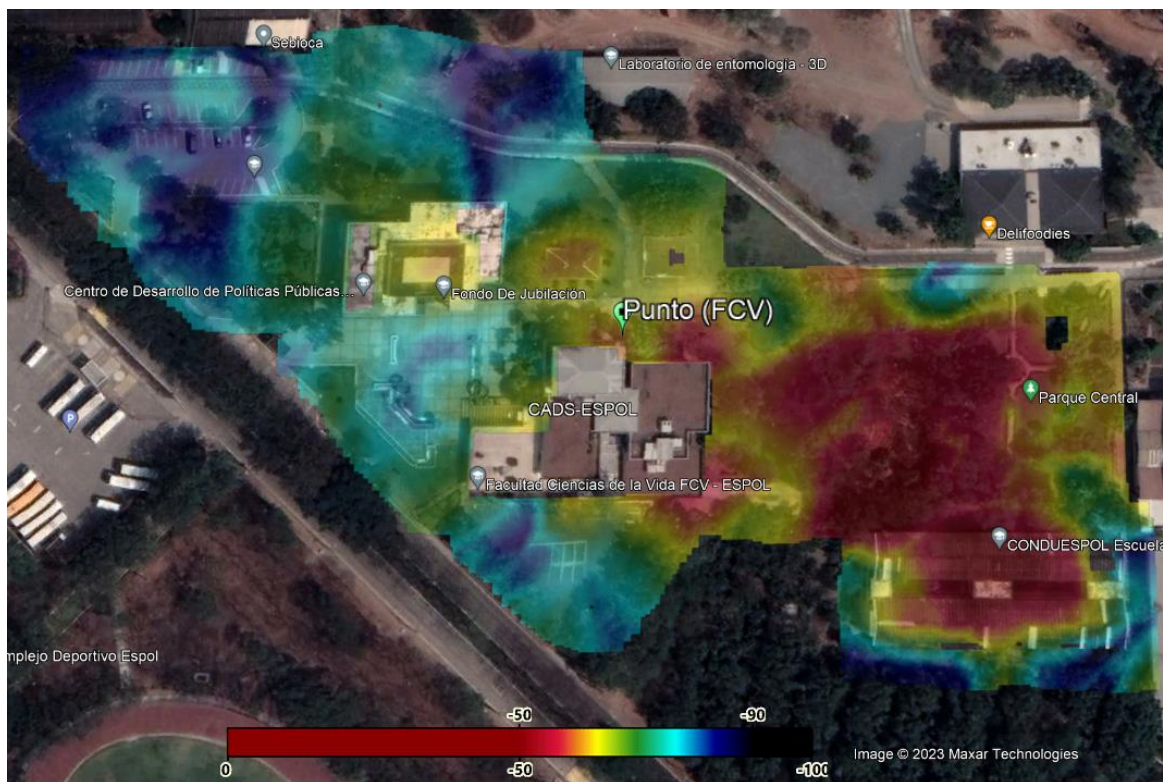
Como se observa en la figura A10 únicamente el punto de encuentro “FIMCM 1” y “FIMCM 4” están ubicados en una zona con baja intensidad de señal recibida mientras que el resto de los puntos “FIMCM 2” y “FIMCM 3” se encuentran ubicados en áreas con intensidad de señal recibida moderada haciéndolos puntos tentativos de instalación para los tótems de emergencia.

A.11 Punto de interés FCV

Para FCV no se dispone de puntos de encuentro, sin embargo, se analiza toda la zona al pertenecer a una facultad importante dentro del campus.

Figura A11

Mapa de Cobertura FCV



Nota. La figura muestra el punto de interés ubicado en el área de FCV.

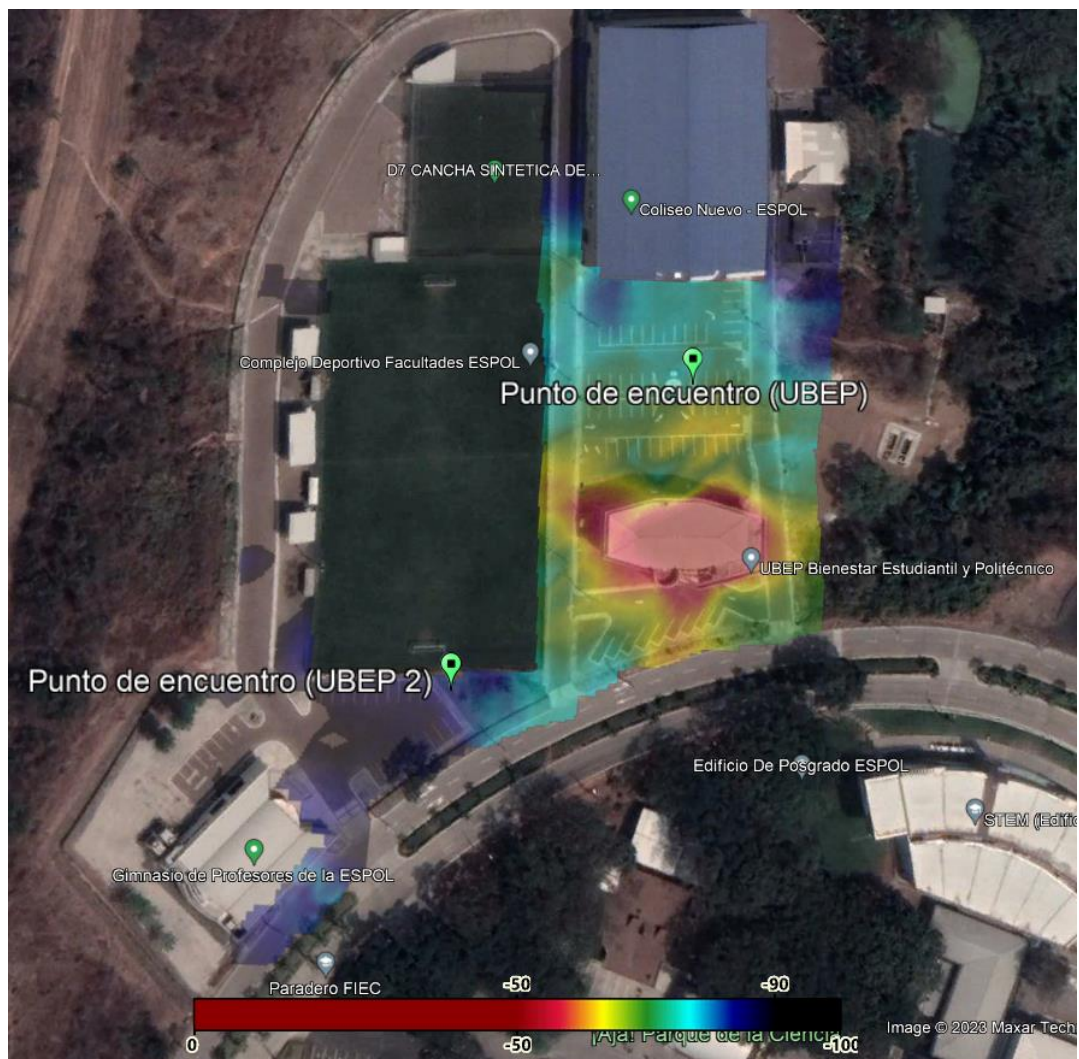
En base al mapa de cobertura visualizado en la figura A11 se observa el punto de interés seleccionado como lugar tentativo de instalación para un tótem de emergencia en dicha área considerando el nivel de intensidad recibida, la ubicación del edificio principal y el tráfico estudiantil presente en dicha zona.

Cabe mencionar la presencia de alta intensidad de señal recibida en el edificio principal de “Conduespol” debido a la instalación de un repetidor de señal en esa área, de esta forma en caso de ser necesario se tiene la garantía de una comunicación fiable para la instalación de tótems en estas áreas verdes con un tráfico de estudiantes moderado al tratarse de un área verde, a diferencia de las demás áreas verdes en el campus únicamente debido a la presencia de un repetidor de señal Wi-Fi se puede tomar en cuenta esta ubicación.

A.12 Puntos de encuentro UBEP

Figura A12

Mapa de Cobertura UBEP



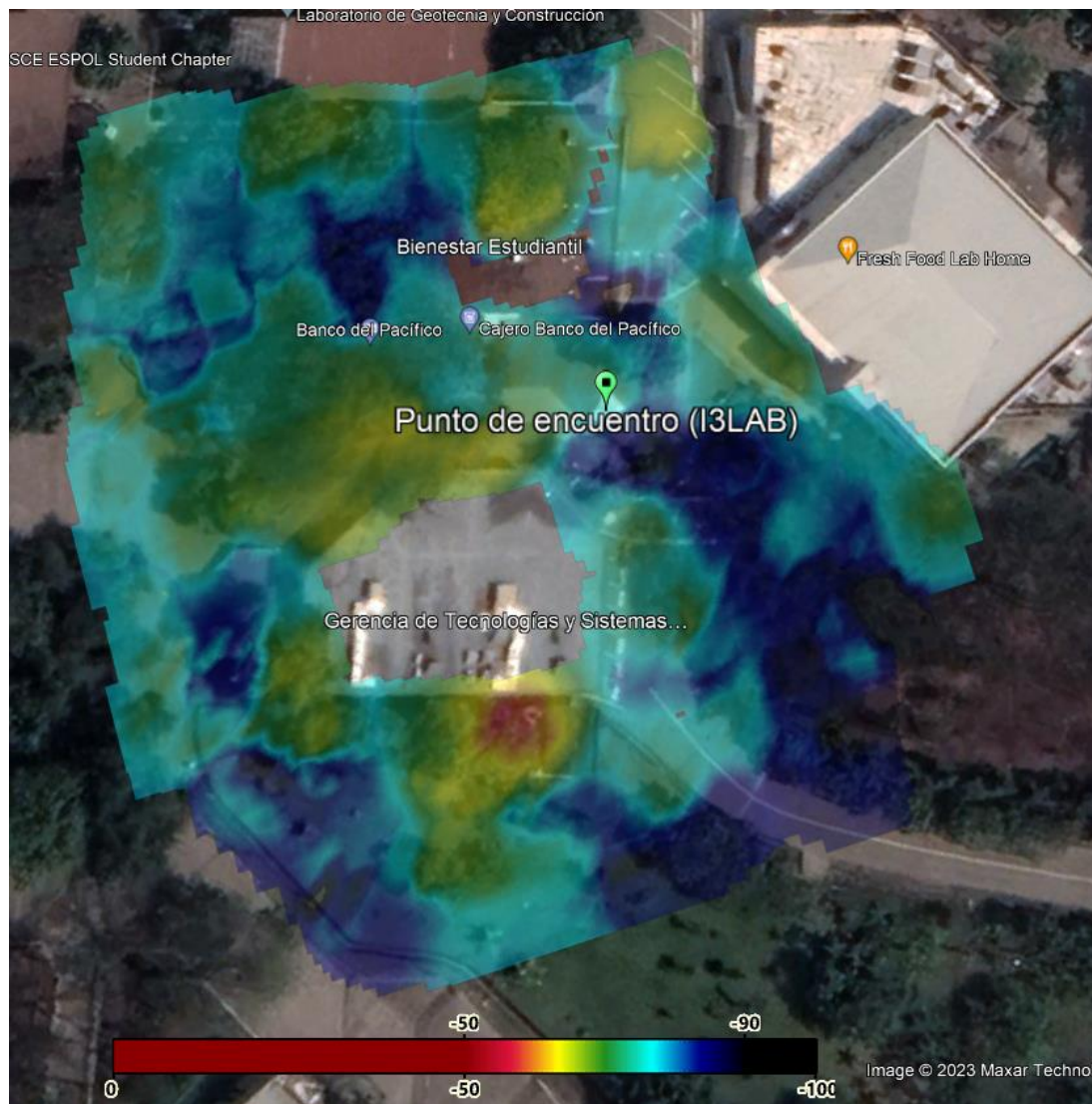
Nota. La figura muestra los puntos de encuentro ubicados en el área de UBEP.

En base al mapa de cobertura visualizado en la figura A12 se puede observar una mayor intensidad de señal recibida para el edificio principal donde se encuentran ubicados los Access Points, se nota como ambos puntos de encuentro se ubican en zonas con baja intensidad de señal recibida lo cual no garantiza una comunicación fiable ante situaciones de emergencia mediante el uso de tecnología Wi-Fi.

A.13 Puntos de encuentro I3LAB

Figura A13

Mapa de Cobertura I3LAB



Nota. La figura muestra el punto de encuentro ubicado en el área de I3LAB.

Como se puede observar en la figura A13 el punto de encuentro está ubicado en una zona con intensidad de señal recibida baja, no obstante, hay zonas con mayor intensidad por lo cual este podría ser reubicado dependiendo del caso.

Apéndice B. Código base para programar la conexión del ESP32 a la red Wi-Fi

```
#include <Wi-Fi.h>

// Reemplazar con las credenciales de la red Wi-Fi de ESPOL
const char* ssid = "Nombre_Red_Wi-Fi";
const char* password = "Contraseña";

void setup() {
  // Iniciar la comunicación serial
  Serial.begin(115200);

  // Iniciar la conexión a la red Wi-Fi
  Wi-Fi.begin(ssid, password);

  // Esperar hasta que se establezca la conexión
  while (Wi-Fi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }

  // Una vez conectado, imprimir la dirección IP asignada
  Serial.println("Conectado a la red Wi-Fi");
  Serial.print("Dirección IP: ");
  Serial.println(Wi-Fi.localIP());
}

void loop() {
  // Aquí se puede agregar lógica adicional si se requiere
}
```

Código base para envío de datos desde un ESP32 al sistema ESPOL ALERT

```
#include <Wi-Fi.h>
#include <HTTPClient.h>

const char* ssid = "Nombre_Red_Wi-Fi";
const char* password = "Contraseña";
const char* serverUrl = "http://direccion_api_ESPOL_ALERT.com/alerta";

Wi-FiClient client;
HTTPClient http;

void setup() {
  Serial.begin(115200);

  // Conectar a Wi-Fi
  Wi-Fi.begin(ssid, password);
  while (Wi-Fi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Conectando a la red Wi-Fi...");
  }
  Serial.println("Conectado a la red Wi-Fi");
}

void loop() {
  // Supongamos que esto se activa cuando se presiona un botón
  if (botonDePanicoPresionado()) {
    enviaralerta();
  }
}

void enviaralerta() {
```

```
http.begin(client, serverUrl);
http.addHeader("Content-Type", "application/json");

// Suponiendo que enviamos un paquete JSON con un mensaje de alerta, el mensaje debe ser
editado dependiendo de la ubicación del tótem, al ser activado se presentará esta información.
int httpResponseCode = http.POST("{\"alerta\": \"emergencia\"}");

if (httpResponseCode > 0) {
  String response = http.getString();
  Serial.println(httpResponseCode);
  Serial.println(response);
} else {
  Serial.print("Error en el envío: ");
  Serial.println(httpResponseCode);
}

http.end();
}

bool botonDePanicoPresionado() {
  // Aquí se debería implementar la lógica para detectar cuando se presiona el botón de pánico
  // Por ejemplo, leer un pin GPIO (pin de propósito general)
  return digitalRead(BOTON_PANICO_PIN) == HIGH;
}
```

Apéndice C: Código base para el envío de emergencias mediante Lora

```
#include <RH_RF95.h> // Incluye la biblioteca RadioHead para LoRa
#include <SPI.h> //Se define la comunicación Serial Peripheral Interface
#include <LowPower.h> // Incluye la biblioteca LowPower para gestionar el modo de sueño

//Proceden a definirse los pines para la selección del chip, el reseteo e interrupción del módulo

#define RFM95_CS 10 // Pin del chip select del módulo LoRa
#define RFM95_RST 9 // Pin de reset del módulo LoRa
#define RFM95_INT 2 // Pin de interrupción del módulo LoRa

RH_RF95 rf95(RFM95_CS, RFM95_INT); // Inicializa el objeto LoRa

const int buttonPin = 7; // Pin del botón de pánico (Puede ser otro si se requiere)
int buttonState = 0; // Variable para almacenar el estado del botón

void setup() {
  Serial.begin(9600); //Se define una tasa de 9600 Baudios por defecto
  pinMode(POWER_SWITCH, INPUT_PULLUP); // Configura el pin del botón como entrada con
  resistencia pull-up

  if (!rf95.init()) {
    Serial.println("LoRa initialization failed!");
    while (1);
  }
  Serial.println("LoRa initialization OK!");
}

void loop() {
  buttonState = digitalRead(buttonPin); // Lee el estado del botón de pánico
  if (buttonState == LOW) { // Si el botón está presionado procede a enviar la alerta
```

```
    sendMessage("Emergencia: Necesito ayuda! Ubicación:UBICACIÓN DEL TÓTEM");  
// Envía un mensaje de emergencia  
    delay(500); // Evita el rebote del botón  
}  
//Si se requieren realizar implementaciones adicionales pueden configurarse en esta sección  
// Pasa al modo de sueño para ahorrar energía en la batería  
goToSleep();  
}  
  
void sendMessage(String message) {  
    Serial.println("Enviando mensaje: " + message);  
    rf95.send((uint8_t*)message.c_str(), message.length()); // Envía el mensaje de emergencia  
    rf95.waitPacketSent(); // Espera a que el mensaje sea enviado  
    Serial.println("Mensaje enviado correctamente.");  
}  
  
void goToSleep() {  
    Serial.println("Entrando en modo de sueño...");  
    LowPower.powerDown(SLEEP_FOREVER); // Entra en modo de sueño hasta ser activado  
nuevamente  
    Serial.println("Despertando del modo de sueño...");  
}
```