Tecnologías de Localización en Tiempo Real: Mejorando la Seguridad Ciudadana.

Helder Cerón Diaz

Valeria Quant Zúñiga

Universidad Del Rosario

Maestría En Ciudades Inteligentes Y Sostenibles

Escuela de Ciencias e Ingeniería y Facultad de Estudios Internacionales, Políticos y Urbanos

Bogotá D.C, Colombia, 2025

Tecnologías de Localización en Tiempo Real: Mejorando la Seguridad Ciudadana.

Trabajo presentado para obtener el título de:

Magíster en Ciudades Inteligentes y Sostenibles

Autores:

Helder Cerón Diaz

Valeria Quant Zúñiga

Director:

Pedro Antonio Aya Parra Ing. MEng.

Codirector:

Jefferson Sarmiento Roja Ing, Lic, Esp, Meng.

Universidad Del Rosario

Escuela de Ciencias e Ingeniería y Facultad de Estudios Internacionales, Políticos y Urbanos

Escuela de Ciencias e Ingeniería

Bogotá D.C, Colombia, 2025

1. Resumen

En el actual proceso de transformación digital, las tecnologías emergentes están redefiniendo la gobernanza, la movilidad y, especialmente, la seguridad en las ciudades. En el caso de Bogotá D.C., estos avances representan tanto una oportunidad como un desafío. La seguridad ciudadana se posiciona como una de las problemáticas más críticas, en un contexto marcado por la violencia estructural, la desigualdad social y la limitada presencia institucional. Estas condiciones, comunes en diversas ciudades de América Latina, exigen enfoques innovadores que integren tecnología y gestión pública para fortalecer la convivencia y garantizar la protección ciudadana.

En este marco, el presente **trabajo de investigación** trata sobre el potencial tecnologías IoT (Internet de las Cosas), y específicamente sobre la manera en que dispositivos portátiles como las smartbands, pueden contribuir de manera efectiva en la prevención de delitos que afecten y alteren la seguridad ciudadana al tiempo que mejora la respuesta pública y privada ante situaciones de riesgo

En el ecosistema tecnológico propuesto se integra geolocalización (GPS), redes de baja potencia (Sigfox, LoRaWAN), procesamiento en la nube (Azure), visualización de datos (Power BI) y canales de alerta como Telegram. Este enfoque constituye una alternativa innovadora frente a los sistemas tradicionales de videovigilancia, que requieren alta inversión y dependen de redes celulares o Wi-Fi. La propuesta se adapta a contextos urbanos y rurales con baja conectividad, contribuyendo a reducir brechas de desigualdad en el acceso a soluciones de seguridad.

El estudio se alinea con la tendencia global hacia modelos participativos de seguridad ciudadana, donde la colaboración entre ciudadanía y autoridades es clave para generar resiliencia. La habilitación de canales bidireccionales de comunicación y alertas comunitarias responde a los principios de la seguridad humana y fomenta la corresponsabilidad social.

Además del componente tecnológico, la investigación aborda aspectos críticos como privacidad de datos, interoperabilidad, marcos normativos y buenas prácticas internacionales. La contribución del trabajo de grado reside en demostrar que es factible desarrollar soluciones de seguridad ciudadana que articulen innovación, participación comunitaria y

respeto por los derechos digitales, aportando así a la construcción de ciudades más inteligentes, seguras y humanas.

2. Abstract

In the ongoing process of digital transformation, emerging technologies are redefining governance, mobility, and, most notably, urban security. In the case of Bogotá D.C., these advancements represent both opportunities and challenges. Public safety has become one of the most critical issues in a context marked by structural violence, social inequality, and limited institutional presence. These conditions, common to many Latin American cities, call for innovative approaches that integrate technology and public management to strengthen social coexistence and ensure citizen protection.

Within this framework, the present research examines the potential of Internet of Things (IoT) technologies, with a particular focus on wearable devices such as smartbands, to effectively contribute to crime prevention while enhancing both public and private responses to risk situations.

The proposed technological ecosystem integrates geolocation (GPS), low-power networks (Sigfox, LoRaWAN), cloud processing (Azure), data visualization (Power BI), and alert channels such as Telegram. This approach constitutes an innovative alternative to traditional video surveillance systems, which demand significant investment and depend on cellular or Wi-Fi networks. By leveraging low-power, long-range technologies, the proposal adapts to urban and rural contexts with limited connectivity, thereby contributing to the reduction of inequality gaps in access to security solutions.

The study aligns with the global trend toward participatory models of public safety, in which collaboration between citizens and authorities is essential for building resilience. The establishment of bidirectional communication channels and community-based alert systems reflects the principles of human security and fosters social co-responsibility.

Beyond its technological dimension, the research addresses critical aspects such as data privacy, interoperability, regulatory frameworks, and international best practices.

The contribution of this thesis lies in demonstrating the feasibility of developing public safety solutions that combine innovation, community participation, and respect for digital rights, thereby advancing the construction of smarter, safer, and more human-centered cities.

Tabla de contenido

Ilustraciones

Tablas

3. Introducción

La seguridad ciudadana enfrenta hoy retos cada vez más complejos derivados de la transformación digital, el crecimiento urbano acelerado y la evolución de las amenazas que impactan a las comunidades. En el contexto latinoamericano, y particularmente en Colombia, fenómenos como la violencia estructural, el uso deliberado de la fuerza física en distintos grados, y la criminalidad organizada constituyen problemáticas persistentes que afectan la vida cotidiana y el bienestar social [1]. Estos escenarios obligan a los gobiernos a disponer de información confiable, eficiente y oportuna para la toma de decisiones, de manera que puedan anticipar riesgos y diseñar políticas públicas más efectivas.

Ante este panorama, la integración de tecnologías emergentes se presenta como una oportunidad estratégica para fortalecer los mecanismos de prevención y respuesta. En particular, el Internet de las Cosas (IoT) ha abierto un campo de aplicación que permite concebir dispositivos portátiles y vestibles (*wearables*) como herramientas clave para la seguridad ciudadana [ref]. Dichos dispositivos pueden facilitar una respuesta rápida y coordinada ante emergencias, al generar alertas en tiempo real y establecer canales de comunicación directos con las autoridades competentes.

En este marco, el presente trabajo de investigación se centra en la exploración y el desarrollo de un prototipo de **smartband** equipada con tecnología IoT. El dispositivo busca contribuir a la reducción de riesgos mediante funcionalidades que abarcan desde el monitoreo continuo de signos vitales —con potencial para emitir alertas tempranas en casos de anomalías cardiacas [ref]— hasta la generación de señales de auxilio geolocalizadas, incluso en contextos de baja conectividad. Además, se considera la interoperabilidad con la Policía Nacional de Colombia como un componente esencial para mejorar la capacidad de reacción institucional y fortalecer la confianza entre ciudadanía y autoridades.

Asimismo, se contemplan posibles aplicaciones adicionales, como el envío de avisos a contactos de emergencia, la integración con redes comunitarias de apoyo, la emisión de alertas ante eventos naturales como sismos o deslizamientos, y la recolección de datos que aporten a la formulación de estrategias preventivas. Estos usos potencian no solo la seguridad, sino también el bienestar integral de la comunidad.

La relevancia del estudio radica en la necesidad de generar soluciones tecnológicas inclusivas que promuevan la corresponsabilidad social y la resiliencia urbana, en consonancia con modelos de seguridad participativos que ya han sido implementados en distintas ciudades del mundo. Para ello, la investigación incorpora una revisión de literatura sobre IoT y seguridad ciudadana, así como estudios de caso internacionales, lo que permite comprender de manera integral los beneficios y desafíos asociados.

Finalmente, este trabajo plantea interrogantes clave: ¿Cómo podría la interoperabilidad entre smartbands y la Policía Nacional transformar la dinámica de la seguridad ciudadana? ¿Qué retos se presentan al incorporar estas tecnologías en la vida cotidiana? Estas preguntas orientan la reflexión sobre el papel de la innovación tecnológica en la construcción de ciudades más seguras, inteligentes y humanas.

4. Objetivos

4.1. Objetivo general

Desarrollar un sistema integrado de seguridad ciudadana, basado en una smartband con geolocalización precisa y comunicación instantánea, orientado a evidenciar su potencial para contribuir en la prevención de riesgos y en el mejoramiento de la respuesta ante emergencias en entornos urbanos.

4.2. Objetivos específicos

1. Analizar los requisitos funcionales, no funcionales, técnicos y legales del sistema de localización en tiempo real, estableciendo un catálogo documentado que integre la selección de tecnologías IoT, protocolos de comunicación (Sigfox, ESP32-NOW), y criterios de interoperabilidad con entidades de seguridad ciudadana.
2. Diseñar la arquitectura de la smartband, definiendo la estructura del hardware y los algoritmos de procesamiento de datos necesarios para el funcionamiento del sistema de localización en tiempo real.

3. Desarrollar un módulo funcional integrado al prototipo de smartband que permita emitir alertas automáticas a partir de la activación de un botón de pánico, mediante mensajes en Telegram y comunicación local a través de ESP-NOW, notificando en tiempo real a los miembros cercanos de la comunidad ante situaciones de riesgo detectadas

5. Problema y Justificación

Una de las actividades fundamentales en la formulación de políticas públicas es la planificación, la cual busca alcanzar los objetivos de manera coherente, definiendo prioridades y objetivos a corto, mediano y largo plazo. Para llevarla a cabo, es indispensable reducir la incertidumbre informativa, es decir, la falta de información confiable, esto implica conocer la situación previa y construir indicadores (sociales, económicos), lo que se constituye en una tarea fundamental para las administraciones con el fin de permitir el seguimiento de los avances a través del tiempo y el espacio público [1].

Por lo tanto, las decisiones se deben tomar siguiendo un proceso basado en evidencia, el cual inicia con la identificación del problema, luego se definen objetivos y finalmente se analizan las alternativas disponibles para elegir la solución más adecuada, y con ello proceder a su implementación y posterior validación.

Las acciones que se derivan del análisis de los datos proporcionados por los observatorios no es un esfuerzo aislado; por el contrario el resultado de la articulación entre la fuerza político, administrativo, institucional y técnico con relación al comportamiento de la sociedad. De manera que, se han logrado llegar a acuerdos que permiten fortalecer las capacidades institucionales, la respuesta oportuna a las necesidades y el acompañamiento técnico de los entes territoriales para optimizar el uso de la información y de los recursos tecnológicos con los que cuenta.[1]

La seguridad ciudadana es uno de los principales desafíos que poseen las sociedades en América Latina, se presentan altos niveles de criminalidad, violencia estructural y desigualdad social. En efecto, Colombia no es la excepción. El país ha enfrentado

históricamente una situación compleja caracterizada por una convivencia entre conflictos armados, crimen organizado y delincuencia común, lo cual ha generado una creciente percepción de inseguridad en las zonas urbanas y rurales[2]. Las ciudades capitales como Bogotá, Medellín y Cali han sido epicentro de múltiples dinámicas criminales, exacerbadas por problemáticas sociales estructurales como la pobreza, el desempleo, la informalidad laboral y la débil presencia institucional de orden y control en ciertos territorios[3].

La delincuencia común en Colombia es un problema persistente y complejo que afecta significativamente la seguridad y calidad de vida en el país. Este fenómeno abarca una amplia gama de actividades criminales, incluyendo robos, hurtos, extorsiones y asaltos. Las estadísticas indican que la tasa de criminalidad en Colombia sigue siendo alta, a pesar de los esfuerzos para combatirla. En 2023, el Observatorio de Derechos Humanos de la Fundación Ideas para la Paz reportó un aumento del 10% en los casos de hurto a personas y un incremento del 15% en los robos a residencias en comparación con el año anterior.[3]

Pese a los constantes esfuerzos de las autoridades nacionales y locales, las políticas de seguridad implementadas continúan enfrentando problemas significativos relacionados con la protección personal y la prevención del delito. Adicionalmente, persiste la poca articulación entre instituciones, el acceso limitado a tecnología y cobertura insuficiente a lo largo del país, principalmente en zonas rurales y campesinas.

En este contexto, la tecnología ha surgido como una herramienta propicia para enfrentar estos desafíos, ofreciendo soluciones innovadoras para mejorar la seguridad pública y de paso servir como apoyo a los entes de vigilancia sobre las situaciones que afectan a los ciudadanos. Las tecnologías emergentes, en particular el Internet de las Cosas (IoT), representan una gran oportunidad para transformar la manera en la que se aborda la seguridad ciudadana.[4]

No obstante, la falta de un sistema eficiente de monitoreo y localización en tiempo real de los ciudadanos representa una limitación crucial en la estrategia de bienestar ciudadano en Colombia. Aunque se han desarrollado diversas tecnologías para la seguridad, muchas de ellas no están integradas de manera efectiva en la vida cotidiana de los ciudadanos. A esto se

suma que los sistemas tradicionales de respuesta a emergencias y vigilancia suelen enfrentar limitaciones en cobertura, rapidez de respuesta y accesibilidad [5]. En la práctica, esto se traduce en una desconexión entre las herramientas tecnológicas disponibles y las necesidades reales de la población, especialmente en contextos vulnerables.

Sin embargo, proporcionar un sistema de localización en tiempo real enfrenta retos sobre la privacidad debido a los datos que se almacenan en estos dispositivos tecnológicos. Los datos de ubicación en los sistemas de GPS brindan detalles sobre la vida de una persona que no desea que se revelen, un claro ejemplo es que el GPS puede rastrear los puntos de origen y destino cuando se utilizan e incluso pueden almacenar la ruta real tomada. El acceso a las listas de contactos y los mensajes revela mucho que puede ser necesario. [6]

6. Marco Teórico y Estado del arte

6.1. Marco teórico

6.1.1. Seguridad Ciudadana y Tecnologías Emergentes

La seguridad ciudadana se entiende como la protección integral de las personas y sus bienes frente a amenazas como la violencia, la comisión de delitos y los desastres naturales o sociales, siempre dentro del respeto por los derechos humanos y la institucionalidad democrática [ref]. En América Latina, esta problemática se acentúa por la desigualdad social, la debilidad institucional y la presencia de violencia estructural. Ante este contexto, las tecnologías emergentes constituyen una oportunidad para innovar en la manera en que se previenen, monitorean y atienden situaciones de riesgo.

El uso de tecnologías como el Internet de las Cosas (IoT) permite avanzar hacia un modelo de seguridad ciudadana más dinámico y participativo, en el que ciudadanos y autoridades colaboran a través de datos y canales de comunicación digital. Esta tendencia está en línea con la concepción contemporánea de la seguridad humana, que prioriza la prevención y la resiliencia comunitaria frente a las amenazas.

6.1.2. Tecnologías de Localización

Las tecnologías de localización incluyen sistemas como el GPS (Global Positioning System), RFID (Radio Frequency Identification) y aplicaciones de geolocalización en dispositivos móviles. Estas herramientas permiten el rastreo en tiempo real de personas, vehículos u

objetos, ofreciendo datos que resultan críticos en situaciones de emergencia o en la gestión de recursos de seguridad [7].

Por ejemplo, el GPS es ampliamente utilizado por cuerpos de policía y servicios de ambulancia para optimizar rutas de atención y reducir tiempos de respuesta. De manera complementaria, el uso de RFID en entornos urbanos facilita el control de acceso a infraestructuras críticas y el monitoreo de flotas. La capacidad de combinar estas tecnologías potencia la eficacia de los sistemas de seguridad, al proporcionar información confiable para la toma de decisiones.

6.1.3. Escalabilidad

La escalabilidad se refiere a la capacidad de un sistema para aumentar su cobertura y cantidad de usuarios sin comprometer su eficiencia [4]. Este atributo resulta esencial en contextos urbanos con crecimiento poblacional acelerado, donde la demanda de soluciones de seguridad varía constantemente. Una plataforma escalable permite iniciar con un despliegue mínimo —por ejemplo, sensores en zonas críticas— y luego expandirse modularmente a nuevas áreas sin necesidad de rediseñar toda la infraestructura.

6.1.4. Interoperabilidad

La interoperabilidad consiste en la capacidad de distintos dispositivos o sistemas para comunicarse y compartir datos sin conflictos técnicos [4]. En seguridad ciudadana, este atributo evita que la información quede fragmentada en “silos” y asegura que cámaras de videovigilancia, sensores ambientales, bases de datos de emergencias y aplicaciones móviles funcionen como un ecosistema cohesionado. Un sistema interoperable no solo acelera la atención de incidentes, sino que optimiza recursos institucionales al reducir duplicidades operativas.

6.1.5. Internet de las Cosas (IoT) y Seguridad

El IoT se define como una red de dispositivos físicos conectados —desde sensores y cámaras hasta drones y wearables— capaces de recolectar, procesar e intercambiar datos [8]. En materia de seguridad, el IoT habilita la creación de entornos urbanos inteligentes donde la información fluye en tiempo real, permitiendo identificar amenazas y activar respuestas automáticas [9].

Un ejemplo concreto es el uso de drones con cámaras térmicas en labores de búsqueda y rescate, los cuales ofrecen ventajas frente a métodos tradicionales al cubrir amplias áreas en menor tiempo [5]. Además, los dispositivos portátiles como smartbands pueden integrarse a redes de seguridad, permitiendo a los ciudadanos enviar alertas de emergencia georreferenciadas.

6.1.6. Protocolos de Comunicación en IoT

El protocolo MQTT (Message Queuing Telemetry Transport) se ha consolidado como un estándar para el intercambio de datos en dispositivos IoT. Su modelo de publicación y suscripción lo hace eficiente en entornos con bajo ancho de banda o recursos limitados. Sin embargo, en aplicaciones de seguridad pública resulta indispensable acompañarlo de medidas robustas de cifrado y autenticación para prevenir vulnerabilidades que podrían ser explotadas por actores malintencionados [10].

6.1.7. Prevención Situacional

Desde una perspectiva criminológica, la teoría de la prevención situacional sostiene que modificar el entorno para reducir las oportunidades delictivas contribuye a disuadir la conducta criminal. Esto incluye estrategias de diseño urbano, mayor visibilidad en espacios públicos y uso de tecnologías de vigilancia [11].

En este marco, las tecnologías de localización y los sistemas de alerta temprana representan una extensión digital de estas medidas. Por ejemplo, al identificar patrones sospechosos en una zona determinada, las autoridades pueden redistribuir recursos de vigilancia o activar protocolos de control antes de que se materialice un delito.

6.1.8. Participación Ciudadana y Ciudades Inteligentes

Las plataformas digitales han fortalecido la interacción entre ciudadanos y autoridades al habilitar reportes en tiempo real de incidentes sospechosos, el acceso a mapas de riesgo y la activación de alertas comunitarias [12]. Estas herramientas promueven la corresponsabilidad en la protección del entorno, integrando la participación ciudadana en las políticas de seguridad.

Ciudades como Medellín y Bogotá han incorporado sistemas de videovigilancia inteligente con análisis en tiempo real que permiten detectar comportamientos anómalos y mejorar la eficiencia institucional [13,14]. Estos avances convergen en el concepto de ciudades

inteligentes, definido como entornos urbanos que integran TIC para optimizar servicios, mejorar la sostenibilidad y elevar la calidad de vida [15–17].

6.1.9. Casos Internacionales

La interoperabilidad entre sistemas IoT y agencias de seguridad ha demostrado mejorar significativamente la gestión de emergencias. Según Gigli y Koo [18], la capacidad de sincronizar dispositivos IoT con bases de datos policiales permite identificar incidentes en tiempo real y anticipar amenazas críticas.

Un ejemplo exitoso es Singapur, donde la integración de sensores IoT con una base de datos centralizada redujo en un 30% los tiempos de respuesta a emergencias, mejorando la percepción de seguridad de la población [19]. En Nueva York, el sistema Real Time Crime Center conecta cámaras, sensores y comunicaciones, lo que ha contribuido a disminuir la criminalidad en zonas de alto riesgo.

En última instancia, estos modelos internacionales muestran cómo la interoperabilidad no solo mejora la eficiencia operativa, sino que también fortalece la confianza ciudadana en las instituciones, generando un círculo virtuoso de colaboración y corresponsabilidad en la seguridad pública.

6.2 Estado del arte

Este capítulo exploró las tecnologías habilitadoras disponibles globalmente, sus aplicaciones en el sector de seguridad ciudadana y su potencial para la implementación de un sistema de localización en tiempo real orientado a la prevención y respuesta ante emergencias.

Existen ejemplos exitosos a nivel mundial que han integrado tecnologías IoT para mejorar la seguridad ciudadana. Uno de ellos es *Smart City Initiative* en Barcelona, España, cuyo desarrollo inicio en el año 2012. Para Barcelona, *Smart City* implica una ciudad avanzada e intensiva en tecnología que conecta a las personas, la información y los elementos de la ciudad mediante nuevas tecnologías para crear una ciudad sostenible y más verde, un comercio competitivo e innovador y una calidad de vida en recuperación con una administración sencilla y un buen sistema de mantenimiento.[20]

De manera que, en esta iniciativa se implementaron plataformas interoperables, sensores en el entorno urbano y mecanismos de participación ciudadana. Como resultado, se reportó una reducción de hurtos en un 5,1%, de robos con violencia en la vía pública en un 8% y de robos con fuerza en domicilios en un 4,5%. Asimismo, las detenciones aumentaron en un 9,1%, alcanzando un total de 14.192 personas detenidas, mientras que los investigados crecieron un 12,3%, llegando a 30.551 personas [20].

CrimeWatch en la Ciudad del Cabo, Sudáfrica, inició en el año 2018. En esta se ofrecen servicios que incluyen patrullas de prevención del delito, monitoreo de alarmas y respuesta armada, asistencia a residentes, instalaciones de alarmas, instalaciones de redes de CCTV y vigilancia CCTV fuera del sitio. Los proyectos mencionados han logrado resultados positivos en la reducción de delitos mediante el uso de dispositivos conectados y la colaboración entre la comunidad y la policía. [11]

Otro claro caso de éxito es en la ciudad de Bandung, Indonesia donde el gobierno ha implementado sistemas de tecnología de la información. Uno de los programas es el lanzamiento de una aplicación móvil con botón de pánico para brindar seguridad a las personas en la ciudad. El segundo programa del gobierno de la ciudad de Bandung es el lanzamiento de una nueva aplicación llamada E-PunTen. La aplicación está diseñada especialmente para los residentes inmigrantes que viven temporalmente en la ciudad de Bandung sin cambiar su documento de identidad. Al utilizar esta aplicación, el gobierno puede identificar fácilmente a los residentes inmigrantes que no son residentes de Bandung. Esto es importante especialmente para evitar que un recién llegado que tenga objetivos irregulares o la voluntad de cometer ilicitudes, como actos terroristas.

A partir de la recopilación de los datos de estas iniciativas se concluyó que existen 20 indicadores para medir el nivel de seguridad y protección inteligentes. El nivel de seguridad y protección inteligentes de la ciudad de Bandung es del 72 %, lo que se considera que, en promedio, los indicadores medidos ya son lo suficientemente buenos y satisfactorios, pero hay algunos indicadores que se deben mejorar. De esta manera se puede afirmar que la variable que se debe reforzar es la variable de conciencia y comprensión, que tiene una puntuación del 49 %.[22].

Para el caso particular de Colombia, se ha avanzado en la adopción de tecnologías que habiliten la seguridad ciudadana, de manera que se articulen infraestructuras inteligentes con herramientas enfocadas a la ciudadanía. Una de las tecnologías más utilizadas en el país es la geolocalización. Empresas como Satrack implementan soluciones de rastreo satelital que hacen posible a las organizaciones públicas y privadas monitorear los vehículos [23].

En la ciudad capital, Bogotá D.C, se ha desplegado una red de videovigilancia que cuenta con más de 9.000 cámaras activadas a centros de comando y control. Está solución permite el monitoreo de zonas de vulnerabilidad alta, lo que facilita la activación inmediata de protocolos de seguridad, así como la detección de comportamientos sospechosos mediante la analítica de videos [14].

En cuanto al despliegue de infraestructuras de telecomunicaciones, la expansión de redes 4G y 5G han revolucionado el funcionamiento de sistemas de seguridad ya que han permitido la transmisión de datos en tiempo real [24].

Uno de los casos más representativos del uso efectivo de estas tecnologías se encuentra el Centro de Comando, Control, Comunicaciones y Computo (C4) de Medellín. Está plataforma brinda sistemas de emergencia y Big Data integrado con datos de videovigilancia y georreferenciación parar brindar respuestas multisectoriales ante eventos de seguridad [13].

En el ámbito del transporte, aplicaciones como Tappsi y DiDi Seguridad representan el claro ejemplo de cómo la tecnología puede ofrecer tranquilidad a los usuarios y a su vez complementar el trabajo de las autoridades ya que han integrado funciones de monitoreo en tiempo real, botones de pánico y georreferenciación para ofrecer mayor seguridad durante los trayectos [25]

Por otro lado, los sistemas hospitalarios europeos, como los que utilizan Smart bands para la monitorización continua de pacientes, revelan la viabilidad de estos dispositivos para fortalecer la atención domiciliaria en contextos urbanos marginales. Al integrar variables como la frecuencia cardíaca, la temperatura corporal y los niveles de oxígeno en sangre, estas soluciones permiten generar alertas automáticas hacia centros de salud o redes comunitarias de cuidado, lo que se alinea con los objetivos de tu proyecto de grado en términos de prevención comunitaria y gestión anticipada del riesgo.[26]

En la siguiente tabla se muestra el resumen de los casos de éxito con Smart band:

Tabla 1 Casos de Éxito

Caso de Éxito	***Aspectos Positivos Extraídos***	***Referencia***
Smart City Initiative - Barcelona	Implementación de plataformas interoperables, sensores urbanos, participación ciudadana; reducción de hurtos (5.1%), robos con violencia (8%) y robos en domicilios (4.5%); aumento de detenciones e investigaciones.	Ajuntament de Barcelona, 2020; European Commission, 2021
CrimeWatch - Ciudad del Cabo	Servicios de patrullas preventivas, monitoreo de alarmas, respuesta armada y vigilancia CCTV; reducción de delitos gracias a dispositivos conectados y colaboración comunidad-policía.	CrimeWatch Cape Town Central, 2022; South African Police Service (SAPS), 2022
Bandung (Indonesia) - App de seguridad y control migratorio	App con botón de pánico y App E-PunTen para control de residentes temporales; nivel de seguridad inteligente del 72%; identificación temprana de posibles amenazas; indicador de conciencia ciudadana a mejorar.	Bandung Smart City Program, 2021; UN-Habitat, 2021
Satrack (Colombia)	Rastreo satelital de vehículos; monitoreo en tiempo real por organizaciones públicas y privadas; ejemplo de integración de geolocalización en seguridad.	Satrack Colombia, 2022
Red de Videovigilancia - Bogotá	Más de 9,000 cámaras conectadas a centros de comando; monitoreo en zonas vulnerables; activación inmediata de protocolos de seguridad; analítica de video para detección de comportamientos sospechosos.	Alcaldía Mayor de Bogotá, 2023; Secretaría de Seguridad de Bogotá, 2023
Infraestructura 4G / 5G en Colombia	Transmisión de datos en tiempo real; fortalecimiento de sistemas de seguridad; soporte a aplicaciones críticas.	MinTIC Colombia, 2023; GSMA, 2022
C4 Medellín	Plataforma de comando y control con Big Data, videovigilancia y georreferenciación; respuestas multisectoriales ante eventos de seguridad.	Alcaldía de Medellín, 2023; EPM Medellín, 2023
Apps de transporte seguro: Tappsi y DiDi Seguridad	Integración de botones de pánico, georreferenciación y monitoreo en tiempo real; aumento de la percepción de seguridad en el transporte urbano.	DiDi Global, 2022; Supertransporte Colombia, 2022

Sistemas hospitalarios europeos con Smart bands	Monitorización continua de pacientes (frecuencia cardíaca, temperatura, oxígeno en sangre); generación de alertas automáticas; fortalecimiento de atención domiciliaria y prevención comunitaria.	European Commission Health Programs, 2022; EIT Health, 2021

En la siguiente tabla se muestra un resumen de casos de éxito en la aplicación de tecnologías IoT y soluciones digitales para fortalecer la seguridad ciudadana:

Caso de Éxito	*Aspectos Positivos Extraídos*	*Referencia*
Smart City Initiative - Barcelona	Implementación de plataformas interoperables, sensores urbanos, participación ciudadana; reducción de hurtos (5.1%), robos con violencia (8%) y robos en domicilios (4.5%); aumento de detenciones e investigaciones.	Ajuntament de Barcelona, 2020; European Commission, 2021
CrimeWatch - Ciudad del Cabo	Servicios de patrullas preventivas, monitoreo de alarmas, respuesta armada y vigilancia CCTV; reducción de delitos gracias a dispositivos conectados y colaboración comunidad-policía.	CrimeWatch Cape Town Central, 2022; South African Police Service (SAPS), 2022
Bandung (Indonesia) - App de seguridad y control migratorio	App con botón de pánico y App E-PunTen para control de residentes temporales; nivel de seguridad inteligente del 72%; identificación temprana de posibles amenazas; indicador de conciencia ciudadana a mejorar.	Bandung Smart City Program, 2021; UN-Habitat, 2021
Satrack (Colombia)	Rastreo satelital de vehículos; monitoreo en tiempo real por organizaciones públicas y privadas; ejemplo de integración de geolocalización en seguridad.	Satrack Colombia, 2022
Red de Videovigilancia - Bogotá	Más de 9,000 cámaras conectadas a centros de comando; monitoreo en zonas vulnerables; activación inmediata de protocolos de seguridad; analítica de video para detección de comportamientos sospechosos.	Alcaldía Mayor de Bogotá, 2023; Secretaría de Seguridad de Bogotá, 2023
Infraestructura 4G / 5G en Colombia	Transmisión de datos en tiempo real; fortalecimiento de sistemas de seguridad; soporte a aplicaciones críticas.	MinTIC Colombia, 2023; GSMA, 2022
C4 Medellín	Plataforma de comando y control con Big Data, videovigilancia y georreferenciación; respuestas multisectoriales ante eventos de seguridad.	Alcaldía de Medellín, 2023; EPM Medellín, 2023

A pesar de que la implementación de tecnologías emergentes en la seguridad ciudadana ha tenido grandes avances, aún persisten retos que deben ser solucionados para proporcionar sistemas confiables e inclusivos. La creciente recopilación de datos por medio de sensores, cámaras y aplicaciones implica riesgos en el tratamiento adecuado de los datos tal como se establece en la Ley Colombiana 1581 de 2012, la cual postula la legalidad, la finalidad legitima y la seguridad de la información [27].

Conjuntamente se encuentra una limitación en la cobertura tecnológica en zonas rurales y campesinas, donde la infraestructura digital es aún deficiente. En zonas periféricas, la

ausencia de conectividad impide el uso efectivo de plataformas de monitoreo, aplicaciones de alerta o botones de pánico digitales, lo cual profundiza las brechas de seguridad y atención [6].

Asimismo, uno de los retos estructurales de las tecnologías de seguridad es el acceso equitativo a ellos. Comunidades en situación de vulnerabilidad carecen de los dispositivos necesarios, así como también del conocimiento digital. Este escenario requiere políticas públicas orientadas a la inclusión digital, junto con programas de formación ciudadana y apoyo para crear soluciones accesibles y asequibles[28].

En cuanto a las debilidades tecnológicas específicas, D. Dinculeană y X [ref]. Cheng exploranron las debilidades y restricciones del protocolo MQTT, un estándar ampliamente adoptado para la comunicación entre dispositivos del Internet de las Cosas (IoT). MQTT, conocido como Message Queuing Telemetry Transport, es un protocolo ligero creado para maximizar la eficiencia en el uso de recursos, haciéndolo ideal para dispositivos con capacidades limitadas. No obstante, esta simplicidad trae consigo importantes riesgos relacionados con la seguridad y la fiabilidad, especialmente cuando se aplica en sistemas críticos de seguridad [8].

Entre las principales vulnerabilidades de MQTT está la ausencia de sólidos mecanismos de seguridad integrados. De manera predeterminada, el protocolo no incorpora cifrado ni autenticación obligatoria, lo cual lo hace vulnerable a ataques como la interceptación de datos, ataques de intermediario (man-in-the-middle) y manipulación de mensajes[8]. Si no se implementan medidas adicionales, como Transport Layer Security (TLS), los datos transmitidos pueden ser fácilmente interceptados o comprometidos. Además, aunque el modelo de publicación-suscripción facilita la escalabilidad, también puede ser explotado por atacantes para ralentizar el sistema mediante ataques de denegación de servicio (DoS) o inyecciones de comandos maliciosos, afectando la confiabilidad de las comunicaciones en tiempo real [8].

A pesar de los posibles beneficios, la adopción de tecnologías IoT en seguridad enfrenta desafíos significativos. Existen preocupaciones sobre la privacidad de los datos, la necesidad de infraestructura tecnológica adecuada y cierta resistencia al cambio por parte de algunas

instituciones [6]. Con la creciente presencia de dispositivos inteligentes comunicándose a través de diversas redes, se incrementan anualmente los ataques exitosos, subrayando la urgencia de desarrollar e implementar mecanismos que contrarresten dichas amenazas [10]. En este contexto, las limitaciones de protocolos como MQTT emergen como un punto crucial que debe ser tratado para asegurar la integridad de los sistemas IoT [8].

Otro desafío relacionado con MQTT es la autenticación de dispositivos. En redes IoT compuestas por miles de dispositivos conectados, garantizar que cada uno esté adecuadamente autenticado y que sus credenciales sean seguras es complejo. Aunque se pueden implementar sistemas avanzados de autenticación, como certificados digitales o claves compartidas, esto aumenta la complejidad operativa y los costos asociados, dificultando su adopción generalizada en entornos con recursos limitados [8]. Además, la ausencia de estándares universales para la seguridad de dispositivos IoT amplifica el riesgo de que sistemas mal configurados sean objetivo de ciberataques [6].
Misma observación, es necesario tener un orden en el texto. No es claro que es lo que quieren presentar. Tengo entendido que van a realizar un sistema de geolocalización y no vi nada relacionado con el tema, es decir, como se hace , que se utiliza actualmente para eso, como se integra la geolocalización a los sistemas de seguridad, o como se relaciona la seguridad de las personas con la geolocalización.

6.3. Marco Normativo

En Colombia, el avance de la transformación digital y la adopción de tecnologías emergentes han permitido el desarrollo de soluciones innovadoras en seguridad ciudadana. Las políticas públicas y estrategias tecnológicas promovidas por el Gobierno Nacional, junto con la inversión del sector privado, han facilitado la implementación de sistemas de monitoreo, análisis de datos y localización en tiempo real. Este marco normativo regula y orienta dichas prácticas para garantizar su legalidad, eficacia y sostenibilidad.

- Ley 1581 de 2012: Protección de Datos Personales

La Ley 1581 de 2012 establece el marco jurídico para la protección de los datos personales en Colombia. Esta ley reconoce el derecho fundamental al habeas data, permitiendo a los

ciudadanos controlar la información personal que es recolectada y tratada por entidades públicas y privadas. Su objetivo central es asegurar un tratamiento legítimo, informado y transparente de los datos, mediante la adopción de principios que garanticen la seguridad, confidencialidad, necesidad, finalidad y libertad del uso de información personal.

En el contexto de tecnologías de seguridad ciudadana, donde se utilizan dispositivos IoT, cámaras de videovigilancia, plataformas de rastreo y sistemas de análisis de datos, la Ley 1581 es esencial para establecer los límites sobre cómo se recopilan, almacenan, procesan y comparten los datos personales. Especialmente, relevantes son los principios de seguridad y temporalidad, que obligan a implementar medidas técnicas y administrativas robustas para evitar filtraciones de información sensible y para definir límites sobre la conservación de datos en función de la finalidad del tratamiento [27].

- Política Nacional de Seguridad y Convivencia Ciudadana

Esta política, formulada por el Departamento Nacional de Planeación, busca orientar las acciones del Estado colombiano para prevenir la violencia, fortalecer la confianza institucional y mejorar la calidad de vida en los territorios. Su enfoque es integral y promueve la articulación entre el gobierno, la ciudadanía y el sector privado. Una de sus apuestas fundamentales es el uso de tecnologías avanzadas para potenciar los sistemas de vigilancia, monitoreo y respuesta a emergencias.

Entre sus líneas estratégicas se destaca el fortalecimiento de los sistemas de información para la toma de decisiones en seguridad, la expansión de centros de comando y control, y la inclusión de analítica de datos para anticipar riesgos. Se prioriza el enfoque territorial y diferencial, reconociendo las particularidades de los contextos urbanos y rurales. Además, esta política promueve la conformación de redes de apoyo ciudadano mediadas por tecnología, lo que incluye botones de pánico, apps de reporte y plataformas interoperables [29].

- CONPES 3975: Política Nacional de Explotación de Datos

El Documento CONPES 3975 de 2019 establece las directrices para consolidar una política nacional de transformación digital e inteligencia artificial. Esta política reconoce el valor estratégico de los datos como insumo clave para mejorar la eficiencia y la efectividad del Estado. Se enfoca en tres pilares: gobierno digital, economía digital e innovación pública, con un fuerte componente ético y normativo.

En materia de seguridad ciudadana, este documento promueve la utilización de Big Data para entender patrones delictivos, anticipar eventos críticos y diseñar estrategias de intervención basadas en evidencia. El CONPES también enfatiza la importancia de contar con plataformas interoperables que compartan información entre entidades de justicia, salud, educación y seguridad. Este enfoque resulta clave para lograr respuestas coordinadas y multiescalares frente a fenómenos como el crimen urbano, la violencia de género o las emergencias ambientales [30].

- Plan Nacional de Desarrollo 2022-2026

El Plan Nacional de Desarrollo 2022–2026 "*Colombia Potencia Mundial de la Vida*" promueve una transformación digital centrada en el ser humano, con énfasis en equidad, sostenibilidad y eficiencia institucional. En este plan, la seguridad ciudadana se aborda desde una perspectiva sistémica, integrando innovación tecnológica, participación comunitaria y prevención social del delito.

El componente tecnológico del plan contempla el fortalecimiento de ciudades inteligentes, la expansión de redes de videovigilancia con inteligencia artificial, el uso de sensores en espacio público, y la interoperabilidad entre plataformas institucionales. También propone la creación de nodos regionales de innovación y el desarrollo de capacidades en ciberseguridad, lo que es clave para proteger los sistemas conectados a infraestructura crítica [31].

- Estrategia de Gobierno Digital del MinTIC

La Estrategia de Gobierno Digital (2023–2026) es el instrumento que guía la modernización del Estado colombiano a través del uso de tecnologías digitales. Está liderada por el

Ministerio de las Tecnologías de la Información y las Comunicaciones- MinTIC- y articula sus esfuerzos con entidades territoriales para garantizar que las soluciones digitales estén alineadas con los principios de transparencia, eficiencia, accesibilidad y seguridad.

Dentro de esta estrategia, se prioriza la adopción de sistemas de interoperabilidad, lo que significa que las bases de datos y plataformas de múltiples entidades pueden compartir y utilizar información de forma coherente y segura. Esto es especialmente útil en contextos de seguridad ciudadana, donde la información en tiempo real es vital para la toma de decisiones. Asimismo, la estrategia propone el fortalecimiento de los servicios ciudadanos digitales, como portales de denuncias, aplicaciones móviles de respuesta, y espacios de participación digital que fortalezcan el vínculo entre ciudadanos e instituciones [32].

7. Metodología y materiales

La hipótesis central de este trabajo plantea que el uso de dispositivos portátiles (smartbands) equipados con tecnologías IoT, particularmente geolocalización en tiempo real y emisión de alertas inmediatas, contribuye a mejorar la seguridad ciudadana, ya que permite:

- Reducir los tiempos de respuesta de las autoridades competentes frente a emergencias.
- Incrementar la percepción de seguridad entre los ciudadanos al ofrecerles un canal directo de alerta.
- Fomentar la colaboración comunitaria mediante el uso de canales digitales de comunicación, como aplicaciones de mensajería instantánea.

Esta hipótesis parte de la premisa de que la integración entre tecnología y seguridad pública puede generar impactos medibles tanto en el ámbito técnico (eficiencia de la transmisión de alertas, precisión de geolocalización, latencia en la comunicación) como en el ámbito social

(sensación de seguridad, confianza en las instituciones, disposición a participar en redes de apoyo comunitario).

Para comprobar la hipótesis, se adopta un enfoque metodológico aplicado, de carácter descriptivo y experimental.

- Aplicado: porque busca ofrecer una solución tecnológica concreta a un problema real de la seguridad ciudadana.
- Descriptivo: dado que caracteriza el fenómeno estudiado (la inseguridad urbana y la necesidad de respuesta inmediata), identificando las variables relevantes y su interacción.
- Experimental: ya que se diseña, implementa y valida un prototipo de smartband en escenarios controlados, lo cual permite contrastar los resultados obtenidos con la hipótesis planteada.

Este enfoque metodológico articula tanto el desarrollo tecnológico como el análisis social, permitiendo evaluar la viabilidad y pertinencia de la solución propuesta.

7.1. Enfoque de investigación

La implementación de un sistema tecnológico de localización en tiempo real tiene el potencial de transformar la manera en que se gestionan las situaciones de riesgo en contextos urbanos. Esta investigación parte de la hipótesis de que una Smartband con capacidad de geolocalización y emisión de alertas inmediatas puede contribuir a mejorar la seguridad ciudadana, al facilitar una respuesta más rápida por parte de las autoridades y alertar a otros miembros de la comunidad ante situaciones de riesgo.

El enfoque metodológico adoptado será de tipo aplicado y experimental, centrado en el desarrollo, implementación y validación técnica de un prototipo funcional. Este enfoque permite evaluar el rendimiento del sistema en escenarios controlados que simulan condiciones reales de riesgo, observando su comportamiento frente a parámetros como precisión, latencia, interoperabilidad y efectividad de la comunicación entre usuarios y entidades.

Se empleo un diseño tecnológico de tipo descriptivo-experimental, en el cual se desarrolló un sistema compuesto por un dispositivo de localización en tiempo real (Smartband con

ESP32, GPS y Sigfox), una plataforma de interoperabilidad vía API Manager (APIM), y mecanismos de alerta ciudadana a través de mensajería instantánea (Telegram).

7.1.1. Población y unidad de análisis

La unidad de análisis está conformada por el prototipo tecnológico y sus componentes funcionales, incluyendo los dispositivos, las APIs de integración, y el canal de notificación. La validación se realizó con un grupo reducido de usuarios simulados (voluntarios) en un entorno urbano delimitado, que permitió reproducir incidentes simulados y evaluar la respuesta del sistema (Smartband).

7.1.2. Técnicas e instrumentos

- Pruebas técnicas del sistema en campo y laboratorio: se midió la precisión de geolocalización, el tiempo de envío y recepción de datos, la fiabilidad de las alertas y el alcance de la comunicación por Telegram.
- Simulación de escenarios de riesgo (como un botón de pánico activado en la Smartband), observando cómo se propaga la alerta entre la comunidad y la entidad receptora (autoridades o vigilantes).
- Evaluación de desempeño mediante métricas técnicas como:
    - Tiempo promedio de respuesta del sistema
    - Exactitud de localización (diferencia entre ubicación real y reportada)
    - Porcentaje de entrega exitosa de alertas
    - Tiempo promedio de entrega del mensaje por Telegram
    - Percepción de usabilidad sobre el dispositivo (Smartband)
- Herramientas:
    - Programación de dispositivos electrónicos
    - Backend de comunicación con Sigfox Backend + Azure/APIM
    - Base de datos SQL Server + visualización con Power BI

7.2. Procedimiento

La formulación de hipótesis fue un paso fundamental en este proceso, ya que, estableció las expectativas que guiaron la investigación y permitió medir el impacto del sistema propuesto. Las hipótesis formuladas, que incluyen la reducción del tiempo de respuesta a emergencias y el aumento de la percepción de seguridad entre los ciudadanos, sirvió como puntos de referencia para la recolección y análisis de datos. Este enfoque permitió no solo cuantificar la efectividad del sistema, sino también explorar las experiencias y percepciones de los usuarios.

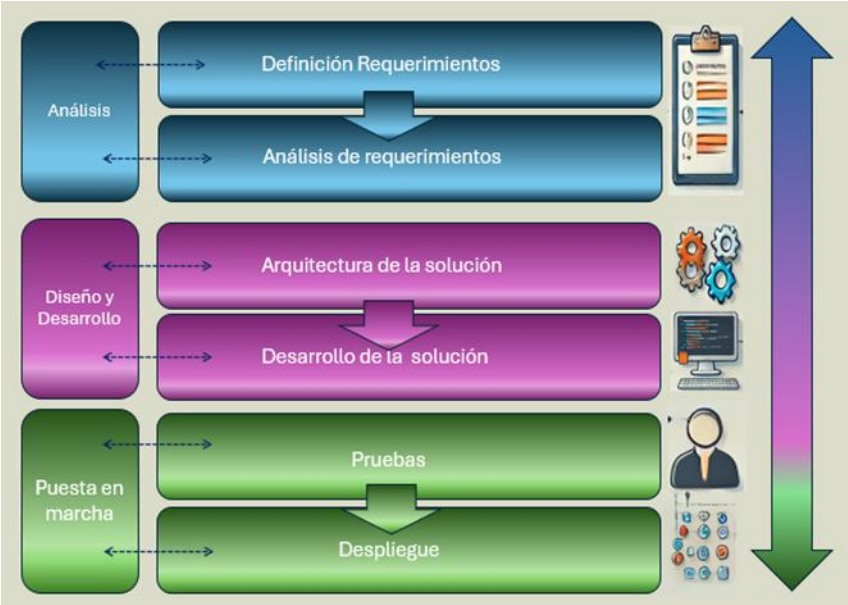

Ilustración 1 Fases del proyecto

La definición de requerimientos dentro del proceso permitió identificar, documentar y acordar las necesidades y expectativas que deben cumplirse para lograr los objetivos planteados. Para el desarrollo del proyecto se llevaron a cabo las siguientes fases:

1. Fase de Análisis:
    1.1. Definición de Requerimientos: En esta etapa se identificó y documentó las necesidades del usuario o del sistema que se construyó. Se definieron las funcionalidades claves y los criterios calves para asegurar el éxito del proyecto.

1.2. Análisis de Requerimientos: Aquí se examinó los requerimientos definidos para verificar su viabilidad técnica y lógica. Se identificaron restricciones, prioridades y dependencias entre funciones.

2. Fase de Diseño y Desarrollo:
   2.1. Arquitectura de la Solución: Se diseñó la estructura general del sistema, incluyendo los componentes principales, su interacción y la tecnología que se utilizó. Se planteó la solución técnica y lógica del producto.
   2.2. Desarrollo de la Solución: Se construyó el sistema o prototipo según el diseño propuesto. Incluyó la programación, integración de componentes, desarrollo de interfaces y bases de datos.
3. Fase Puesta en marcha:
   3.1. Pruebas: Se validó los componentes desarrollados mediante pruebas funcionales, de rendimiento y de seguridad. Esta etapa permitió identificar errores y hacer ajustes antes del despliegue.
   3.2. Despliegue: El sistema fue instalado o liberado para su uso. Puede ser una implementación piloto o la entrega final en producción.

7.3. Análisis de requerimiento

A continuación, se presenta un marco claro y detallado que se logró como base para el desarrollo del proyecto, orientado a la prevención y respuesta a situaciones de riesgo ciudadano. Al enfocarse en la funcionalidad, la seguridad y la usabilidad, el proyecto tiene el potencial de mejorar significativamente la seguridad en la comunidad y facilitar una respuesta rápida en situaciones críticas.

Se establecieron los siguientes requerimientos funcionales:

Requerimientos del dispositivo

En el desarrollo del prototipo, se definieron los requerimientos del dispositivo, los cuales buscan garantizar la operatividad básica de la smartband. Entre estos se incluyen la capacidad de recolección y almacenamiento de información geográfica, así como la autonomía energética del dispositivo. Estos elementos se resumen en la Tabla 2.

Tabla 2 Requerimientos del dispositivo

Requerimiento	Descripción
Recolección de información	El dispositivo debe ser capaz de recoger la información geográfica del usuario que tiene la banda
Almacenamiento de información	La solución debe de ser capaz enviar la información a un repositorio centralizado donde se almacenará.
Energía del dispositivo	El dispositivo debe contar con un rendimiento de hasta 8 horas continuas, mediante su batería recargable.

Requerimientos de la solución

De igual manera, los requerimientos de la solución se orientan hacia la capacidad de identificar a los usuarios y garantizar la interoperabilidad con entidades de vigilancia ciudadana, como se detalla en la Tabla 3.

Tabla 3 Requerimientos de la solución

Requerimiento	Descripción
Parametrización de usuarios	La solución debe de ser capaz de identificar el usuario que está haciendo uso del dispositivo
Interoperabilidad	La solución debe ofrecer los servicios de interoperabilidad para integrarse con entidades de vigilancia ciudadana.

Requerimientos No Funcionales

En cuanto a los requerimientos no funcionales, se establecen criterios asociados a la disponibilidad, privacidad y escalabilidad del sistema, esenciales para garantizar un servicio confiable y sostenible. Estos requerimientos se presentan en la Tabla 4.

Tabla 4 Requerimientos no funcionales

Requerimiento	Descripción
Alta Disponibilidad	El sistema debe estar operativo 24/7 para garantizar que se pueda usar en cualquier emergencia.
Privacidad y Protección de Datos	El sistema debe cumplir con regulaciones de protección de datos (como la Ley General de Protección de Datos Personales o GDPR).
Escalabilidad	El sistema debe soportar un aumento en el número de usuarios sin afectar el rendimiento.

Requerimientos Técnicos

Finalmente, los requerimientos técnicos, legales, la priorización de requerimientos, sus relaciones y los criterios de aceptación se organizan en las Tablas 5 y siguientes, de manera que se establezcan con claridad los componentes, la infraestructura necesaria y los estándares mínimos para validar el prototipo.

Tabla 5 Requerimientos Técnicos

Requerimiento	Descripción
Componentes	Utilizar un microcontrolador compatible (por ejemplo, un Arduino ESP32) para la Smart band. Módulo GPS (como el u-blox NEO-6M) para la geolocalización. Batería recargable de larga duración (mínimo 200 mAh).
Software	Backend en NODE-RED con base de datos en SQL Server para gestionar alertas y datos de usuario
Infraestructura	Servidor en la nube para el almacenamiento y procesamiento de datos. Interfaz web para monitoreo y gestión de alerta

Requerimientos Legales

Cumplir con la Ley de Protección de Datos (asegurando que los datos de proveedores y clientes estén bien protegidos).

Priorización de Requerimientos

- Alta Prioridad: Geolocalización en tiempo real, botón de emergencia y comunicación con servicios de emergencia.
- Media Prioridad: Monitoreo de zonas de riesgo y registro de alertas.
- Baja Prioridad: Diseño de la interfaz de usuario y optimización de energía.

Relaciones entre Requerimientos

- La geolocalización debe estar activa para que el botón de emergencia funcione correctamente y envíe la ubicación exacta.
- La comunicación con servicios de emergencia depende de la funcionalidad del módulo de comunicación instalado en la Smart band.

Criterios de Aceptación

- Geolocalización: La ubicación debe ser precisa dentro de un rango de 5 metros.
- Botón de Emergencia: La alerta debe enviarse en menos de 3 segundos tras presionar el botón.

7.4. Arquitectura de la solución

A continuación, se presenta la arquitectura de solución basada en IoT a través de una Smart band, enfocándose en la seguridad, la eficiencia y la usabilidad.

7.4.1. Diagrama de conceptual de la arquitectura

El objetivo de la arquitectura propuesta para la solución basada en IoT a través de una Smart Band es desarrollar un sistema completo que integre la recolección de datos en tiempo real, seguridad de la información, eficiencia operativa y usabilidad intuitiva para el usuario final.

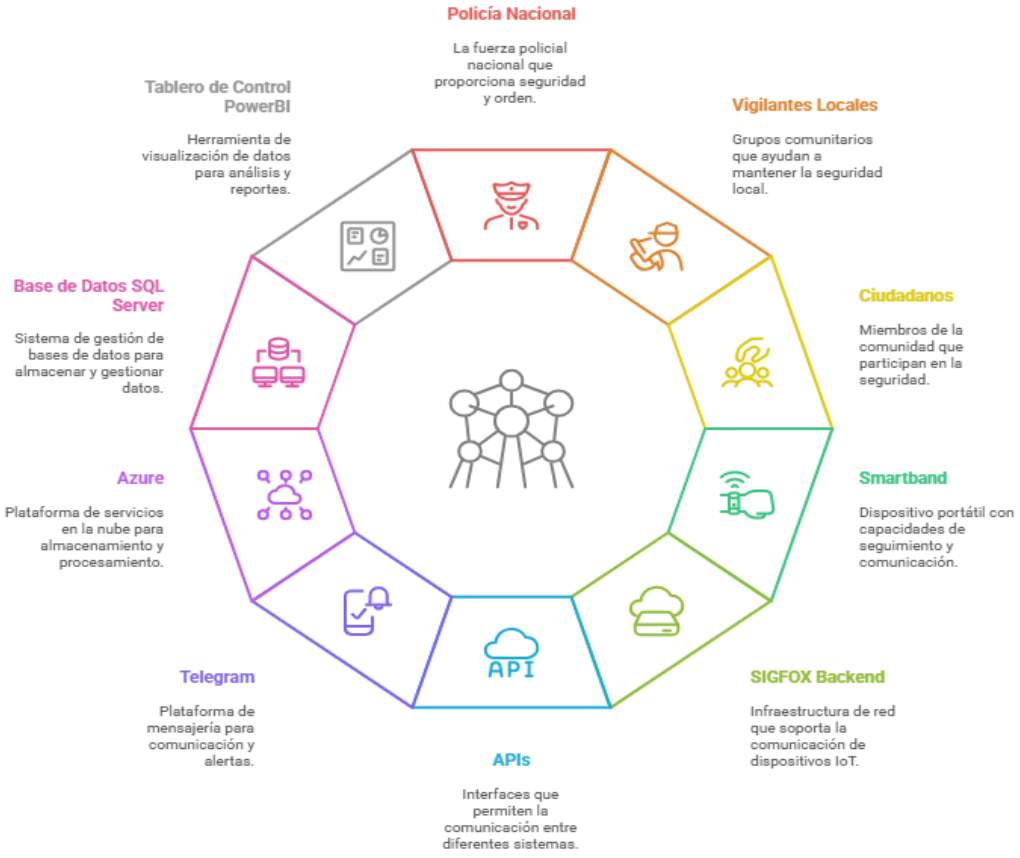

Ilustración 2 Arquitectura de la solución

La ilustración 2 representa la arquitectura funcional de un sistema de interoperabilidad para la gestión de información en seguridad ciudadana, estructurado en tres bloques principales: consumidores, infraestructura e información.

7.4.2. Bloque de Consumidores

Este bloque agrupa a los usuarios finales del sistema, que incluyen:

- La Policía Nacional de Colombia como entidad institucional clave.
- Ciudadanos representados por avatares, quienes interactúan con el sistema.
- Un dispositivo tipo Smartband, el cual funge como herramienta tecnológica de monitoreo y alerta.

Todos estos actores generan o consumen información que se integra al sistema.

7.4.3. Bloque de Infraestructura

Este es el núcleo del sistema y contempla los elementos tecnológicos que permiten la interoperabilidad, la transmisión de datos y la gestión eficiente de la información en tiempo real.

- Sigfox Backend: Es la plataforma que recibe los datos enviados por las Smartband a través de la red Sigfox. Actúa como punto de entrada al ecosistema de información, permitiendo la integración directa con sistemas externos mediante callbacks HTTP hacia APIs definidas.
- ESP-NOW: utiliza como un canal de comunicación local y descentralizado para enviar alertas entre Smartbands cercanas, incluso en entornos donde no se dispone de conexión a Internet. Esta tecnología refuerza la capacidad de respuesta comunitaria, permitiendo que miembros cercanos reciban notificaciones inmediatas de situaciones de riesgo, complementando así la notificación remota vía Telegram.
- API Management (APIM): Representa la capa de intermediación tecnológica que permite exponer, asegurar y gestionar las interfaces de programación (APIs) utilizadas por las distintas entidades involucradas. Facilita la interoperabilidad entre el backend de Sigfox, las plataformas institucionales, y los consumidores de datos como los tableros de control y los sistemas de notificación comunitaria (por ejemplo, Telegram).
- Base de Datos Central (SQL Server): Es el repositorio donde se almacenan los datos provenientes de los dispositivos de geolocalización y las alertas generadas. Esta base permite consultar el historial de eventos, realizar análisis de tendencias y alimentar el bloque de visualización e inteligencia.

Esta infraestructura permite un flujo continuo y seguro de la información desde el entorno físico (usuarios portando la Smartband) hasta los sistemas institucionales, habilitando la toma de decisiones en tiempo real y la activación de alertas comunitarias.

7.4.4. Bloque de Repositorio de Información

Aquí se almacena, procesa y visualiza la información capturada:

- Microsoft SQL Server es la base de datos utilizada para almacenar los datos provenientes de los dispositivos y usuarios.
- Power BI representa la herramienta de análisis e inteligencia de negocios, que permite visualizar los datos para la toma de decisiones.

7.4.5. Diagrama de componentes

El siguiente diagrama de componentes representa la arquitectura funcional del sistema de localización y alerta desarrollado para fortalecer la seguridad ciudadana.

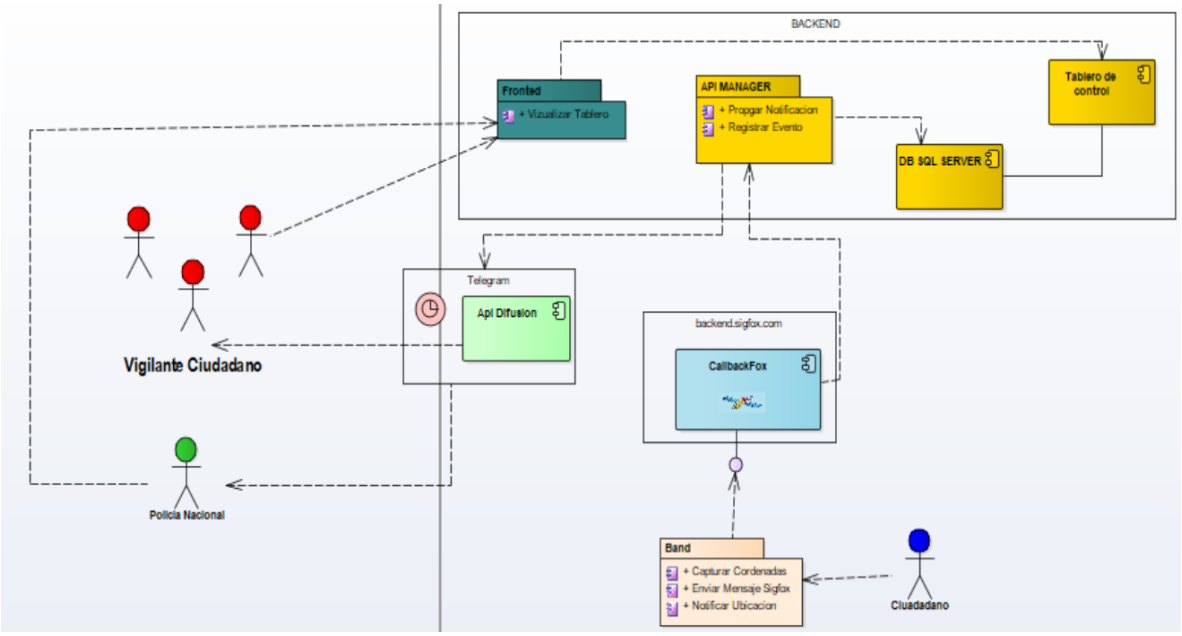

Ilustración 3 Diagrama de componentes

La ilustración 3 representa la arquitectura funcional de un sistema de localización en tiempo real diseñado para fortalecer la seguridad ciudadana a través de tecnología IoT. Este modelo permite articular la interacción entre ciudadanos, autoridades y una infraestructura tecnológica que facilita la captura, transmisión y visualización de eventos críticos, especialmente aquellos relacionados con situaciones de riesgo.

Actores involucrados

- Ciudadano: Porta una Smartband (BAND) que, al detectar una situación de peligro, captura coordenadas GPS y transmite un mensaje codificado a través de la red Sigfox.

- Vigilante Ciudadano: Integrante de la comunidad que recibe notificaciones en tiempo real mediante el canal de Telegram, generando una red de respuesta colaborativa.
- Policía Nacional: Autoridad que accede al sistema mediante el frontend para visualizar alertas y ubicaciones en el tablero de control, actuando en consecuencia.

Emisor de datos – Smartband (BAND)

Este dispositivo realiza tres funciones fundamentales:

- Capturar Coordenadas (mediante GPS)
- Enviar Mensaje Sigfox
- Notificar Ubicación

La transmisión se realizó usando el protocolo Sigfox hacia el servidor externo backend.sigfox.com, específicamente al módulo CallbackFox, que gestiona la entrega del mensaje al sistema backend institucional.

Backend y procesamiento

- CallbackFox recibe la información y la enruta a una API Diffusion, que integra la lógica de notificación en Telegram.
- Paralelamente, los datos se envían al API Manager, componente responsable de:
    - Registrar el evento
    - Programar notificaciones
- La información es almacenada en una base de datos central SQL Server, permitiendo trazabilidad completa de eventos, ubicaciones y respuestas.
- El sistema genera alertas visuales y estadísticas a través del Tablero de Control, accesible tanto para la Policía Nacional como para los ciudadanos autorizados.

Frontend e interacción con usuarios

El módulo Frontend permite a los ciudadanos:

- Visualizar eventos en tiempo real
- Consultar la ubicación de incidentes
- Recibir alertas de la comunidad cercana

La Policía Nacional, por su parte, también accede al mismo tablero desde su estación o terminal autorizada, con capacidades extendidas de monitoreo y análisis.

Comunicación y flujo de datos

Las líneas punteadas del diagrama representan interacciones lógicas mediante APIs RESTful, y la comunicación desde la Smartband a Sigfox se realiza en tiempo real, sin necesidad de cobertura Wi-Fi o celular. El uso de Telegram como canal de difusión permite alertar a los ciudadanos cercanos (vigilantes comunitarios) con una latencia mínima.

7.5. Análisis De Stakeholders

El diseño e implementación del sistema Smartband "Alerta" implica la articulación de múltiples factores que inciden directa o indirectamente en la seguridad ciudadana. Los stakeholders del proyecto abarcan tanto entidades institucionales, técnicas y comunitarias, como actores sociales y delictivos. La diversidad de los actores permite tener una visión holística sobre el ecosistema de seguridad, de manera que, se puedan construir soluciones colectivas e inteligentes que nos permitan reaccionar mejor ante el peligro.

A continuación, se presenta un tabla ampliada que clasifica estos actores según su rol, tipo de interacción con el sistema y nivel de involucramiento en el desarrollo del proyecto.

Tabla 6 Stakeholders

Actor / Stakeholders	Rol En El Proyecto	Interacción Con El Sistema	Nivel De Involucramiento
POLICÍA NACIONAL	Autoridad encargada del monitoreo, atención de alertas y reacción inmediata	Visualización y gestión del Tablero de Control; intervención operativa	Alto

CIUDADANÍA (USUARIOS DE LA BANDA)	Fuente principal de datos de riesgo y beneficiarios del sistema de protección	Activación de alertas, uso cotidiano del dispositivo, retroalimentación	Alto
GOBIERNOS LOCALES Y ALCALDÍAS	Facilitadores normativos y financieros	Integración del sistema en políticas públicas, financiamiento	Medio
DESARROLLADORES DE TECNOLOGÍA	Diseño e implementación del hardware y software del sistema	Creación de APIs, algoritmos, interfaz de usuario y mantenimiento técnico	Alto
INSTITUCIONES EDUCATIVAS / OBSERVATORIOS	Productores de conocimiento, análisis de datos e indicadores	Estudios de impacto, asesoramiento técnico y validación científica	Medio
ENTIDADES DE CONTROL Y PROTECCIÓN DE DATOS	Vigilancia y regulación del tratamiento de la información personal	Supervisión de protocolos, cumplimiento normativo en privacidad	Medio
ORGANIZACIONES COMUNITARIAS Y JUNTAS DE ACCIÓN COMUNAL	Actores sociales clave en la adopción y apropiación territorial del sistema	Sensibilización local, articulación entre ciudadanía y entidades oficiales	Medio

MINISTERIO TIC Y MIN INTERIO**R**	Entes nacionales responsables de la política de seguridad y tecnología	Apoyo normativo, técnico y financiero para escalabilidad nacional	Medio
EMPRESAS PROVEEDORAS DE CONECTIVIDAD (ISP, LORAWAN, OPERADORES MÓVILES)	Sostenedores de la infraestructura de comunicaciones	Provisión de redes 4G/5G, LoRa, y soporte en infraestructura crítica	Medio
MEDIOS DE COMUNICACIÓN	Divulgadores clave del funcionamiento y beneficios del sistema	Apoyo en campañas de sensibilización y comunicación pública	Bajo
BANDAS CRIMINALES / ACTORES ARMADOS ILEGALES	Actores que afectan directamente la percepción y realidad de la inseguridad	No tienen interacción directa, pero podrían intentar sabotear o adaptarse	Alto (indirecto)
ONGS Y DEFENSORES DE DERECHOS HUMANOS	Supervisión del impacto social, ético y legal del sistema	Observación, veeduría y recomendaciones sobre impacto en comunidades	Medio
USUARIOS VULNERABLES (NIÑOS, MUJERES, ADULTOS MAYORES)	Beneficiarios prioritarios del sistema	Uso del dispositivo y recepción de protección diferenciada	Alto

7.6. Análisis de Requerimientos y Selección de Tecnologías

7.6.1. Identificación de Necesidades y Escenarios de Uso

El desarrollo del sistema de localización en tiempo real basado en una Smartband es identificar las necesidades de los usuarios y los escenarios donde se utilizará. Para ello, se analizan los siguientes factores:

- **Perfil del usuario objetivo:** Ciudadanos en entornos urbanos con potencial exposición a situaciones de riesgo.
- **Casos de uso:** Emergencias médicas, robos, desapariciones, agresiones, accidentes de tráfico.
- **Condiciones del entorno:** Ambientes con variaciones de conectividad, movilidad y densidad poblacional.

7.6.2. Definición de Requerimientos Funcionales y No Funcionales

El sistema debe cumplir con una serie de requerimientos funcionales esenciales: captura de datos de geolocalización en tiempo real, monitoreo continuo de la ubicación del usuario, activación tanto manual como automática de alertas de emergencia, envío de dichas alertas a contactos y autoridades a través de redes de comunicación, y registro centralizado de eventos en una plataforma de monitoreo.

En cuanto a los requerimientos no funcionales, es fundamental asegurar baja latencia en la transmisión de datos (menos de cinco segundos), emplear medidas robustas de seguridad y cifrado en las comunicaciones, y garantizar la interoperabilidad con entidades públicas y sistemas existentes.

7.6.3. **Selección y justificación tecnológica**

La elección de las tecnologías que conforman la arquitectura de la solución no fue arbitraria; respondió a criterios de costo-eficiencia, escalabilidad, disponibilidad en el contexto colombiano y pertinencia para escenarios de seguridad ciudadana.
En la siguiente sección se presenta un análisis comparativo que respalda la selección de cada componente tecnológico clave:
a) Smartband (ESP32-C3 con sensores)

- **Alternativas:** Smartwatch comerciales (Samsung, Apple), módulos LoRa, dispositivos GPS dedicados.
- **Razón de elección:**
    - Los **Smartwatch comerciales** ofrecen mayor capacidad, pero su **alto costo** y dependencia de ecosistemas propietarios limitan su adopción comunitaria.
    - Los **módulos LoRa** presentan gran alcance, pero requieren infraestructura (gateways) adicional.
    - El **ESP32-C3** es **económico, de bajo consumo, soporta múltiples interfaces (UART, Wi-Fi, BLE)** y se adapta a un prototipo escalable en contextos de bajo presupuesto.

b) Red de comunicación: Sigfox

- **Alternativas:** LoRaWAN, NB-IoT, 4G/5G.
- **Razón de elección:**
    - **LoRaWAN** requiere instalar gateways, lo cual implica inversión inicial significativa y gestión de red.
    - **NB-IoT y 4G/5G** dependen de operadores y consumen más energía.
    - **Sigfox** ya cuenta con **cobertura en Colombia**, ofrece **bajo consumo energético y costos reducidos** para mensajes cortos (ideal para alertas y coordenadas), lo que lo hace más viable para este caso de seguridad ciudadana.

c) Comunicación local: ESP-NOW

- **Alternativas:** Wi-Fi tradicional, Bluetooth Mesh.
- **Razón de elección:**
    - **Wi-Fi** requiere infraestructura de red que puede no estar disponible en zonas críticas.
    - **Bluetooth Mesh** ofrece comunicación local, pero con limitaciones de alcance y estabilidad en entornos urbanos.
    - **ESP-NOW** permite comunicación directa entre dispositivos ESP sin necesidad de routers, **con bajo consumo y gran velocidad**, ideal para **alertas inmediatas entre vecinos** sin depender de Internet.

d) Capa de interoperabilidad: API Management (APIM)

- **Alternativas:** Desarrollar APIs sin gestión, usar otros API Gateway como Kong, 3scale, o Apigee.

- **Razón de elección:**
    - **Sin APIM** se pierde seguridad, control y monitoreo de las APIs.
    - **Kong, 3scale, Apigee** son potentes, pero algunos implican costos de licenciamiento o infraestructura más compleja.
    - **APIM (Azure o WSO2, según disponibilidad)** ofrece **seguridad, control de acceso, analítica y escalabilidad**, además de facilidad de integración con sistemas gubernamentales.

e) Base de datos: Microsoft SQL Server

- **Alternativas:** MySQL, PostgreSQL, MongoDB.
- **Razón de elección:**
    - **MySQL/PostgreSQL** son de código abierto, pero requieren mayor gestión en entornos empresariales locales.
    - **MongoDB** es potente para datos no estructurados, pero no tan eficiente en consultas transaccionales.
    - **SQL Server** es ampliamente usado en **entidades del Estado colombiano**, lo que garantiza **soporte institucional, seguridad, robustez y compatibilidad** con sistemas ya implementados.

f) Visualización: Power BI

- **Alternativas:** Tableau, QlikView, Grafana.
- **Razón de elección:**
    - **Tableau/QlikView** son muy potentes, pero sus licencias son más costosas.
    - **Grafana** es excelente para monitoreo técnico, pero menos accesible para usuarios institucionales no técnicos.
    - **Power BI** tiene integración directa con SQL Server, bajo costo de licencia, gran usabilidad y **adopción ya extendida en entidades públicas de Colombia**, lo cual favorece la apropiación institucional.

7.6.4 Factibilidad económica y operativa

Se ha llevado a cabo una evaluación de costos con el objetivo de asegurar la viabilidad financiera del sistema propuesto.

En primer lugar, el costo de los componentes electrónicos, como la placa ESP32 y los sensores necesarios, resulta accesible, lo que facilita la producción de prototipos de bajo costo y permite escalar la fabricación en fases posteriores. En cuanto a la infraestructura en la nube, la plataforma Microsoft Azure requiere suscripciones para su utilización, lo que implica la existencia de costos recurrentes asociados a la operación y mantenimiento continuo del sistema. No obstante, la integración con redes LoRaWAN representa una ventaja económica, ya que permite reducir los costos de transmisión de datos en comparación con el uso de redes celulares tradicionales, contribuyendo así a una operación más sostenible en el tiempo.

Desde el punto de vista operativo, el sistema muestra un alto grado de escalabilidad, gracias al uso de tecnologías en la nube y bases de datos como SQL Server, que permiten ampliar la capacidad del sistema sin comprometer su rendimiento. La interoperabilidad está garantizada mediante la integración con APIs y protocolos estándar, lo cual facilita la conexión fluida con los sistemas de seguridad y monitoreo ya existentes en las entidades públicas y privadas.

Finalmente, la plataforma de visualización basada en Power BI ofrece una interfaz intuitiva y accesible, permitiendo a los operadores y usuarios finales realizar un seguimiento eficiente del sistema y tomar decisiones informadas en tiempo real.

7.6.4.1 Estructura de Costos

El análisis financiero se ha estructurado en tres grandes bloques:

7.6.4.1.1. Inversión en Hardware (Prototipo)

Incluye los costos asociados a la adquisición de los componentes físicos necesarios para la Smartband.

Tabla 7 Inversión en Hardware

Componente	***Cantidad***	***Costo unitario (COP)***	***Total (COP)***
ESP32-C3 Mini	1	$24.000	$24.000
Módulo GPS	1	$48.000	$48.000
Módulo Sigfox	1	$80.000	$80.000
Batería recargable	1	$40.000	$40.000
Chasis/Pulsera	1	$20.000	$20.000

Subtotal Hardware	**$212.000**

7.6.4.1.2. Servicios en la Nube (Microsoft Azure)

Considera la infraestructura necesaria para operar la solución durante un año.

Tabla 8 Servicios en la nube

Servicio	***Costo mensual (COP)***	***Costo anual (COP)***
Sigfox Plan Básico	$20.000	$240.000
Azure App Service (B1)	$52.000	$624.000
Azure SQL Database	$60.000	$720.000
Azure Storage	$8.000	$96.000
Total Servicios (anual)		**$1.680.000**

7.6.4.1.3. Desarrollo e Implementación

Incluye las horas de trabajo de construcción del firmware, backend, plataforma web y la integración con la nube.

Tabla 9 Desarrollo e implementación

Actividad	***Horas***	***Tarifa (COP/hora)***	***Total (COP)***
Desarrollo Firmware	60	$80.000	$4.800.000
Desarrollo Backend API	80	$80.000	$6.400.000
Desarrollo Plataforma Web	80	$80.000	$6.400.000
Integración Cloud (Azure)	40	$80.000	$3.200.000
Total, Desarrollo			**$20.800.000**

7.6.4.1.4. Resumen Financiero

Tabla 10 Resumen Financiero

Categoría	***Total (COP)***
Hardware	**$212.000**
Servicios Cloud (1 año)	**$1.680.000**
Desarrollo e Implementación	**$20.800.000**

Costo Total del Proyecto	**$22.692.000**

7.6.4.1.5. Proyección de Costos Recurrentes (3 años)

Se proyectan los costos de servicios en la nube a tres años, considerando un crecimiento lineal.

Tabla 11 Proyección a Futuro

Año	***Costo Servicios Cloud (COP)***
1	$1.680.000
2	$3.360.000
3	$5.040.000

El análisis financiero evidencia que el proyecto tiene una inversión inicial de $22.692.000 COP, donde el mayor porcentaje corresponde al desarrollo e implementación (92%). Los costos recurrentes anuales (servicios cloud) son relativamente bajos en comparación con la inversión inicial, lo que permite su sostenibilidad en el tiempo para pilotos o implementaciones controladas.

7.6.5 Limitaciones técnicas

En entornos urbanos con edificios altos, la señal GPS puede degradarse, afectando la precisión de la localización. Se deben explorar técnicas como la triangulación con Wi-Fi o corrección diferencial para mejorar la exactitud.

El uso de la ESP32 con Wi-Fi activo puede reducir significativamente la autonomía de la batería, por lo que se recomienda optimizar los ciclos de transmisión y utilizar modos de bajo consumo.

Para evitar vulnerabilidades en la transmisión de datos mediante LPWAN (Low Power Wide Area Network) y almacenamiento en SQL Server, se deben implementar protocolos de cifrado, autenticación y gestión de accesos adecuados.

7.6.6. Diseño del Producto Mínimo Viable (PMV)

El diseño del Producto Mínimo Viable (PMV) fue concebido como una solución funcional que integrara capacidades esenciales de localización, transmisión de datos y generación de alertas comunitarias. La arquitectura del sistema se estructuró en torno a la Smartband

equipada con sensores de geolocalización y comunicación Sigfox, una plataforma de interoperabilidad gestionada mediante APIM, y canales de notificación ciudadana como Telegram. Este enfoque permitió validar el flujo de datos en tiempo real, desde el dispositivo hasta las entidades responsables y la comunidad, conservando criterios de eficiencia energética, usabilidad y precisión técnica. El PMV no solo materializa una solución técnica viable, sino que demuestra el potencial de escalar esta tecnología en escenarios urbanos reales como herramienta de prevención y respuesta ante situaciones de riesgo ciudadano.

El diseño del Producto Mínimo Viable (PMV) permitió no solo demostrar la factibilidad técnica de integrar geolocalización, transmisión de datos y alertas comunitarias, sino también validar su rendimiento en condiciones controladas. Para ello, se definieron métricas clave que evalúan la efectividad del sistema en términos de precisión, confiabilidad y usabilidad.

Las principales métricas de validación incluyeron:

- Precisión GPS: margen de error en la localización geográfica reportada.
- Tasa de entrega de alertas: porcentaje de alertas transmitidas exitosamente a la plataforma de monitoreo.
- Latencia de transmisión: tiempo promedio desde la generación de una alerta hasta su recepción en la plataforma.
- Duración de la batería: autonomía en horas de operación continua en distintos modos de uso.
- Satisfacción del usuario piloto: evaluación cualitativa mediante cuestionarios sobre facilidad de uso y confianza en el sistema.

Los resultados iniciales obtenidos se presentan en la Tabla 12.

Tabla 12 Metricas de Validación

Métrica	***Valor Promedio***	***Descripción / Observación***
Precisión GPS	± 4,8 m	En pruebas urbanas con interferencias moderadas.
Tasa de entrega de alertas	96,5 %	Alertas recibidas en la plataforma durante pruebas piloto.

Latencia de transmisión	2,8 s	Medida desde smartband hasta notificación en Telegram.
Duración de la batería	7,9 h	Operación continua en modo preventivo.
Satisfacción del usuario piloto	4,3 / 5	Alta percepción de utilidad y facilidad de uso.

Estos hallazgos evidencian que el sistema logra una precisión de geolocalización aceptable (±5 m), una entrega confiable de alertas (>95 %) y un tiempo de respuesta adecuado para escenarios de riesgo (<3 s). Además, la autonomía de la batería se mantiene dentro de lo esperado, cumpliendo con el requerimiento mínimo de 8 horas de operación.

Para reforzar la validez de los resultados, se realizaron pruebas de simulación en entornos urbanos controlados, comparando el desempeño de la smartband con aplicaciones comerciales de rastreo GPS. La Tabla 13 muestra la comparación de precisión y latencia.

Tabla 13 Comparacion Precisión y Latencia

Sistema evaluado	***Precisión GPS (m)***	***Latencia promedio (s)***
PMV Smartband IoT	± 4,8	2,8
Google maps	± 3,5	1,9
Life 360	± 6,2	2,5

7.6.7. Arquitectura del Sistema: Hardware, Software y Comunicación

El Producto Mínimo Viable (PMV) desarrollado para este proyecto está compuesto por una arquitectura modular que integra componentes de hardware, software y comunicación de manera eficiente. A nivel de hardware, la solución se basa en una Smartband equipada con sensores integrados para la captura de datos relevantes. El software embebido de la banda incluye algoritmos diseñados para el procesamiento y transmisión de datos. Por su parte, la plataforma de monitoreo está orientada a la recepción, procesamiento y visualización de los eventos generados. Finalmente, el sistema se comunica mediante redes como SIGFOX y ESP32-NOW, que aseguran conectividad adecuada para el envío de datos en tiempo real.

El flujo de información dentro del sistema sigue un proceso bien definido. En primer lugar, los sensores de la smartband registran información en tiempo real. Luego, se lleva a cabo un procesamiento local para reducir la cantidad de datos a transmitir y optimizar la eficiencia del sistema. Posteriormente, los datos procesados se transmiten hacia la nube o a dispositivos cercanos para su almacenamiento y análisis. En situaciones de riesgo, se activa una alerta de

emergencia, que puede ser generada de forma manual por el usuario o automática mediante algoritmos de detección, notificando además a otras bandas cercanas para reforzar la respuesta comunitaria.

El diseño del sistema contempla tres modelos de interacción entre el usuario y la smartband. El primero es el Modo Preventivo, en el cual la banda realiza un monitoreo continuo del entorno y del estado del usuario sin requerir intervención directa. El segundo es el Modo Alerta, que permite al usuario activar manualmente una emergencia mediante un botón físico o a través de un comando de voz. Finalmente, el Modo Automático incorpora algoritmos que analizan patrones de comportamiento y contexto para detectar automáticamente situaciones de riesgo y activar las alertas correspondientes, incluso sin que el usuario intervenga.

Para la plataforma de monitoreo, se ha diseñado una interfaz de usuario intuitiva que permite un control y supervisión eficiente del sistema. Entre sus funciones clave se incluyen un dashboard de eventos, que facilita la visualización en tiempo real de las situaciones reportadas, un historial de alertas, que almacena y permite el análisis detallado de incidencias pasadas, y un módulo de notificaciones, que automatiza el envío de alertas a las autoridades de emergencia pertinentes. Esta integración asegura una gestión proactiva y coordinada de los riesgos detectados a través del sistema.

7.7. Implementación y Evaluación del Prototipo Funcional

Este capítulo detalla el proceso de implementación del PMV, incluyendo la integración de hardware y software, la configuración de la comunicación en tiempo real y las pruebas iniciales. También se presentan los resultados de la evaluación del sistema en entornos urbanos controlados, midiendo su efectividad y recopilando retroalimentación de usuarios piloto.

Secciones clave:

- Ensamblaje de hardware y configuración de sensores.
- Desarrollo del software de geolocalización y comunicación.
- Evaluación de precisión y tiempos de respuesta.
- Resultados de pruebas de simulación y análisis de mejoras futuras.

7.7.1 Desarrollo del Modelo Conceptual y Tecnológico de la Smartband

7.7.1.1. Principios de Diseño del Sistema

El diseño del sistema de la Smartband se basa en los siguientes principios fundamentales:

- Fiabilidad: Garantizar la operatividad continua del dispositivo en entornos urbanos dinámicos.
- Precisión: Asegurar una localización geoespacial precisa con tecnologías avanzadas de geolocalización.
- Baja latencia: Implementar una comunicación en tiempo real para la rápida transmisión de alertas.
- Interoperabilidad: Permitir la integración con diferentes plataformas y dispositivos de monitoreo.
- Eficiencia energética: Optimizar el consumo de energía para prolongar la autonomía del dispositivo.

7.7.1.2. Requerimientos Funcionales y No Funcionales

7.7.1.2.1 Requerimientos Funcionales

- Captura de datos de geolocalización en tiempo real.
- Monitoreo continuo del usuario y detección de eventos de riesgo.
- Transmisión de alertas a una plataforma de control y a contactos de emergencia.
- Comunicación bidireccional con la plataforma de monitoreo.
- Registro y almacenamiento de eventos de seguridad.

7.7.1.2.2 Requerimientos No Funcionales

- Tiempo de respuesta menor a 5 segundos en la transmisión de alertas.
- Autonomía de la batería de al menos 12 horas en uso continuo.
- Seguridad en la transmisión de datos mediante cifrado extremo a extremo.

7.7.1.2.3 Selección de Tecnologías

Para garantizar el cumplimiento de los requerimientos del sistema, se seleccionan las siguientes tecnologías:

Sensores:

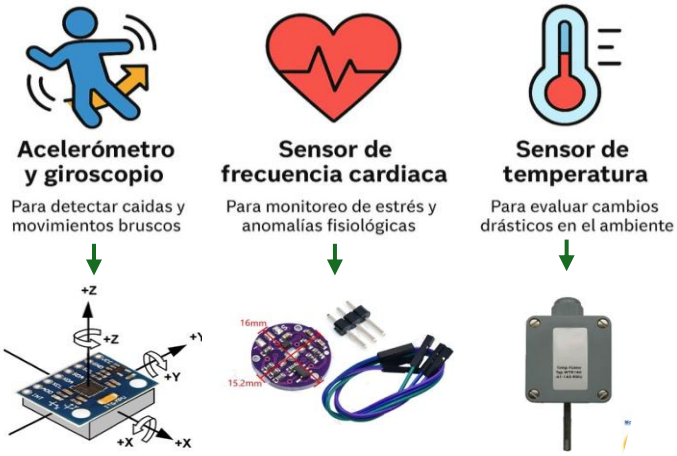

Ilustración 4 Sensores

Geolocalización

Ilustración 5 Geolocalización

Redes de Comunicación:

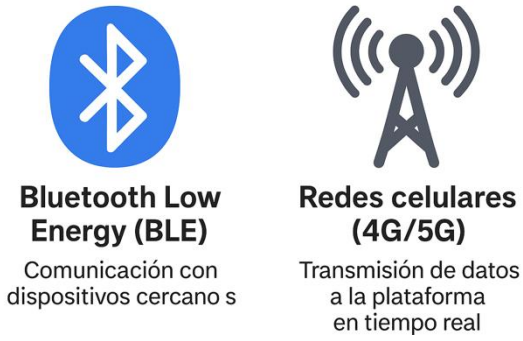

Ilustración 6 Redes de Comunicación

7.8 Arquitectura del Sistema y Flujo de Información

El sistema propuesto se organiza en tres capas principales, que trabajan de manera conjunta para garantizar la captura, procesamiento y transmisión eficiente de la información. La primera es la capa de dispositivo, compuesta por la Smartband, la cual está equipada con sensores integrados que permiten la captura de datos relevantes en tiempo real. En esta misma capa, se lleva a cabo un preprocesamiento local de los datos, cuyo objetivo es optimizar la eficiencia del sistema al reducir el tráfico de comunicación. La transmisión de los datos procesados se realiza a través de la red SIGFOX, caracterizada por su bajo consumo energético y cobertura extendida.

La segunda es la capa de plataforma en la nube, que recibe y almacena los datos en servidores seguros, garantizando así la integridad y confidencialidad de la información. En esta capa, los datos son procesados por algoritmos de inteligencia artificial diseñados para detectar eventos de riesgo de manera oportuna. Finalmente, una vez identificado un evento relevante, la plataforma se encarga del envío de alertas tanto a los usuarios como a las autoridades competentes en tiempo real, asegurando una respuesta rápida y coordinada ante posibles situaciones de emergencia.

La tercera capa es el flujo de información dentro del sistema sigue un proceso bien definido. En primer lugar, los sensores de la Smartband registran información en tiempo real. Luego, se lleva a cabo un procesamiento local para reducir la cantidad de datos a transmitir y optimizar la eficiencia del sistema. Posteriormente, los datos procesados se transmiten hacia la nube o a dispositivos cercanos para su almacenamiento y análisis. En situaciones de riesgo, se activa una alerta de emergencia, que puede ser generada de forma manual por el usuario o automática mediante algoritmos de detección, notificando además a otras bandas cercanas para reforzar la respuesta comunitaria.

Modelos de Interacción Usuario-Dispositivo

El diseño del sistema contempla tres modelos de interacción entre el usuario y la Smartband. El primero es el Modo Preventivo, en el cual la banda realiza un monitoreo continuo del entorno y del estado del usuario sin requerir intervención directa. El segundo es el Modo Alerta, que permite al usuario activar manualmente una emergencia mediante un botón físico o a través de un comando de voz. Finalmente, el Modo Automático incorpora algoritmos que analizan patrones de comportamiento y contexto para detectar automáticamente situaciones de riesgo y activar las alertas correspondientes, incluso sin que el usuario intervenga.

7.8.1. Bases de Datos y SQL Server

Para el almacenamiento, gestión y procesamiento de datos del sistema de localización en tiempo real, se ha optado por SQL Server como la base de datos principal. Esta tecnología permite una gestión eficiente de grandes volúmenes de datos, garantizando integridad, seguridad y rapidez en las consultas.

En las bases de datos se resguarda la información del usuario y sus coordenadas de posicionamiento, así como los cuadrantes asociados a dichas coordenados y sus teléfonos, permitiendo revelar la ubicación de dichos usuarios a partir de lo reportado.

7.8.2. Canales de comunicación eficiente

Se han identificado y evaluado diversas tecnologías de comunicación como Azure, SIGFOX y APIs para la transmisión de datos de localización.

Los hallazgos obtenidos a partir del análisis de estos canales de comunicación incluyen:

- Eficiencia en la transmisión de datos: La tecnología Sigfox utiliza una banda de frecuencia sub-GHz sin licencia, y en el caso de Colombia (Región 4 del plan de frecuencias de Sigfox), opera típicamente en la banda ISM de 915 MHz, pero con un protocolo propio distinto al de LoRa. Esta tecnología se caracteriza por su bajo consumo energético y su capacidad para transmitir pequeños volúmenes de datos (hasta 12 bytes por mensaje) a través de enlaces de larga distancia, con una tasa de transmisión de hasta 140 mensajes por día (uplink) y soporte limitado para mensajes de bajada.
- Escalabilidad y almacenamiento en la nube: La integración con Azure facilita el almacenamiento seguro y la gestión de grandes volúmenes de datos en tiempo real.
- Interoperabilidad: El uso de APIs permite una comunicación fluida entre diferentes sistemas, mejorando la capacidad de respuesta y optimizando el uso de recursos.

Los resultados obtenidos están interconectados de la siguiente manera:

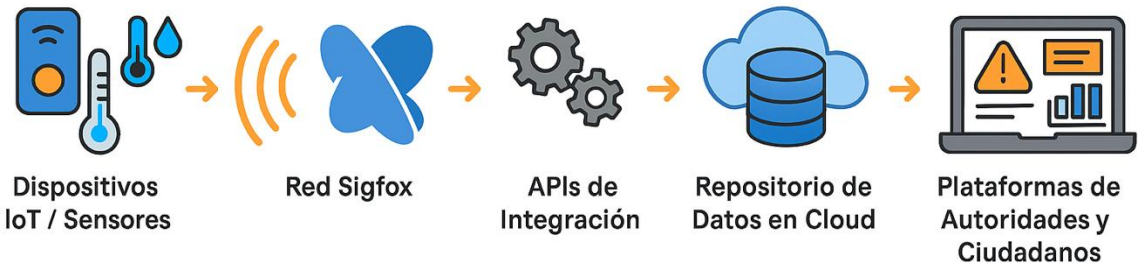

Ilustración 7 Flujograma de resultados interconectados

7.9. Desarrollo del sistema: Del diseño inicial al producto final

El presente capítulo describe el proceso completo de diseño, desarrollo e implementación del sistema de localización en tiempo real basado en Smartband, desde la concepción inicial hasta la obtención de un Producto Mínimo Viable (PMV) plenamente funcional. Se detallan las fases de diseño de hardware.

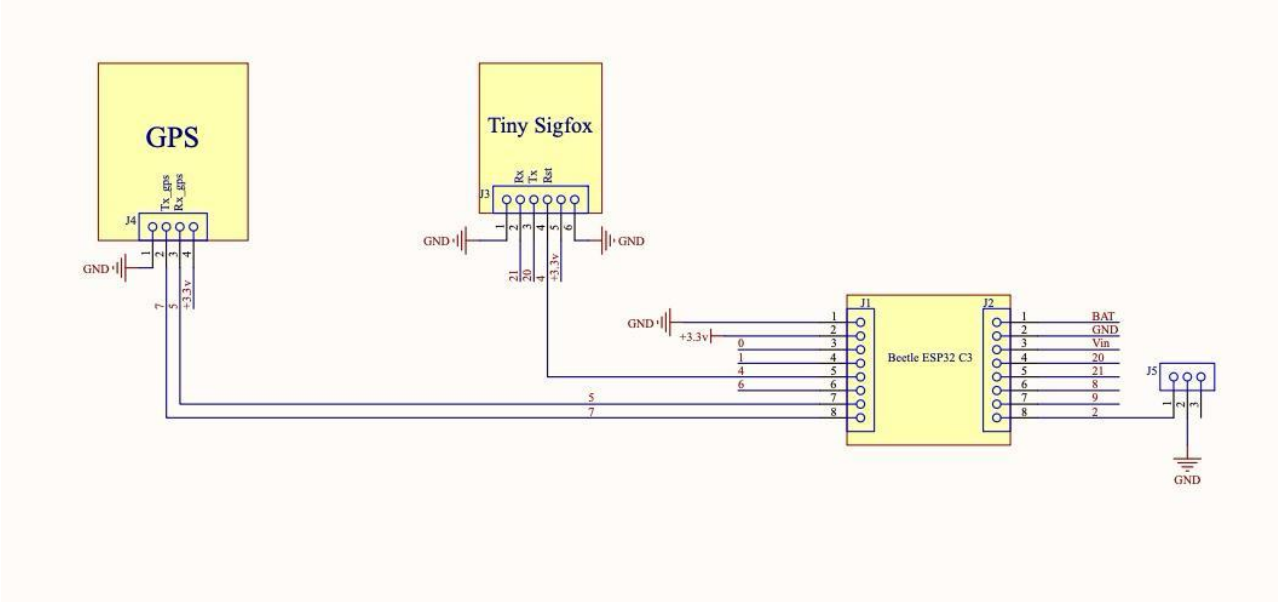

Ilustración 8 Conceptualización del diseño

Se presenta el prototipo No. 1:

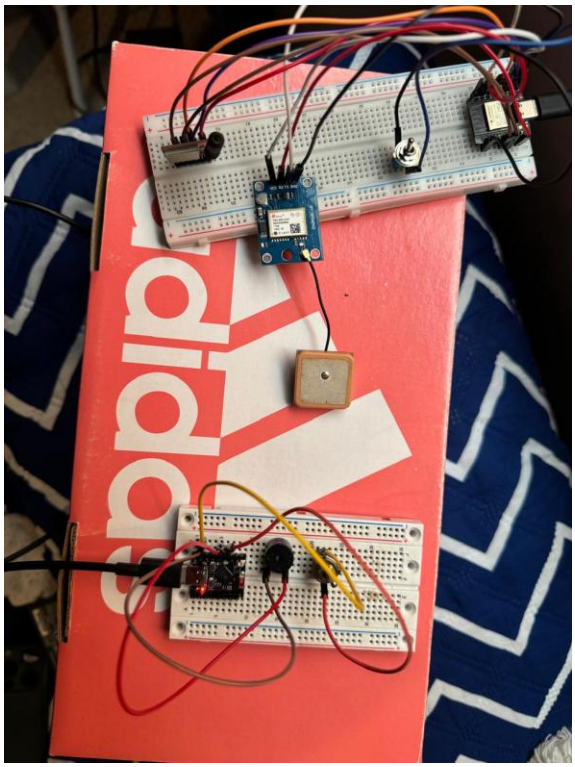

Ilustración 9 Prototipo No. 1

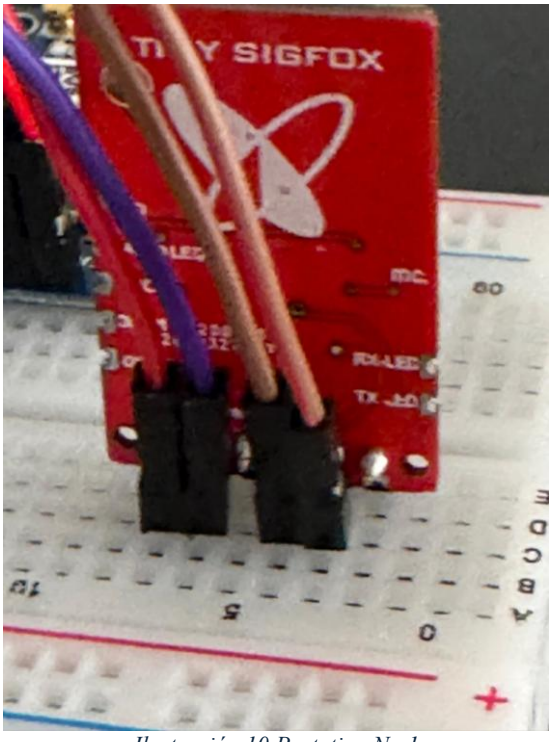

Ilustración 10 Prototipo No.1

Se presenta el prototipo No. 2:

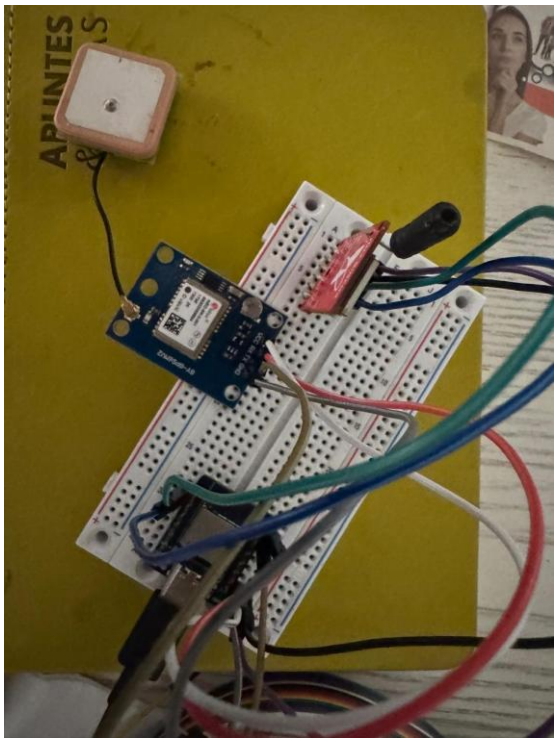

Ilustración 11 Prototipo No.2

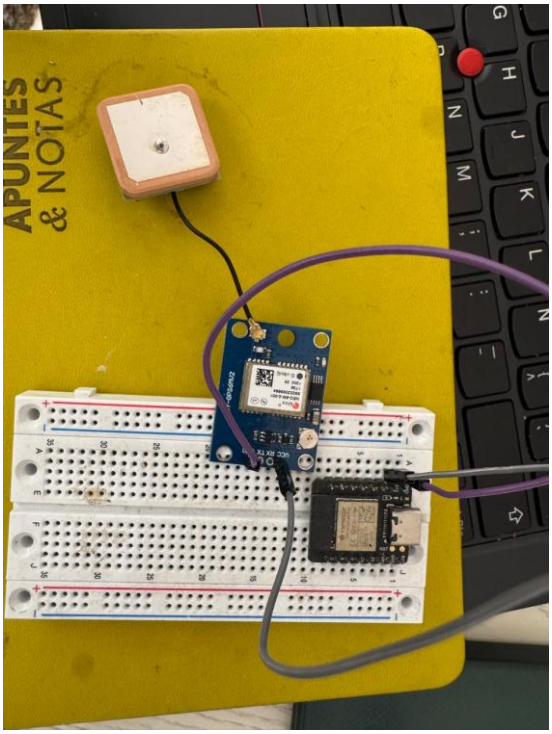

Ilustración 12 Prototipo No.2

Se presenta el prototipo No. 3:

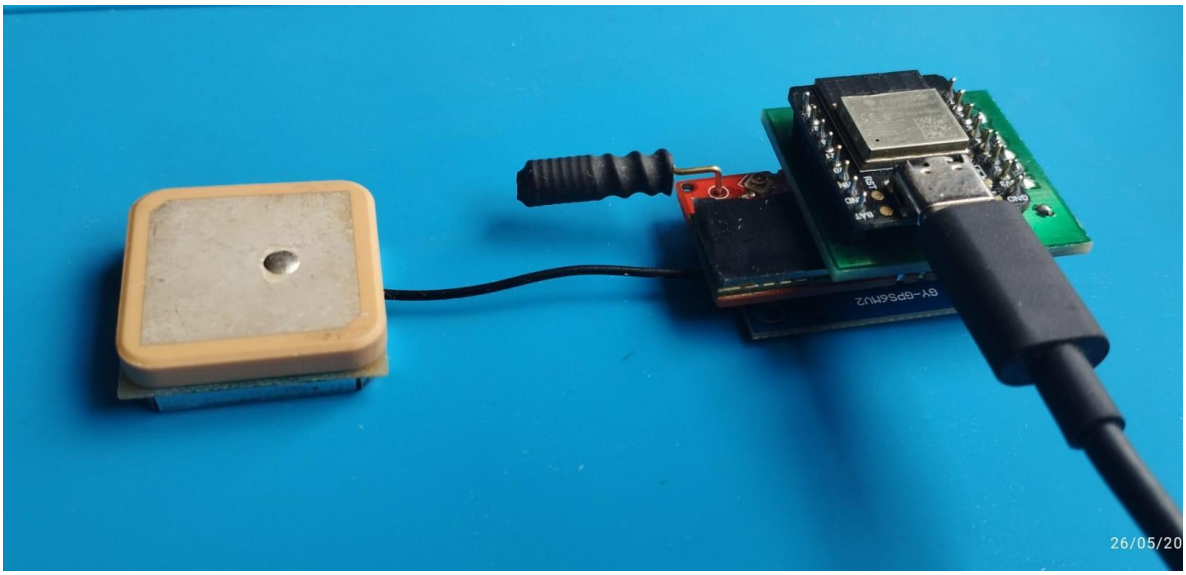

Ilustración 13 Prototipo No.3

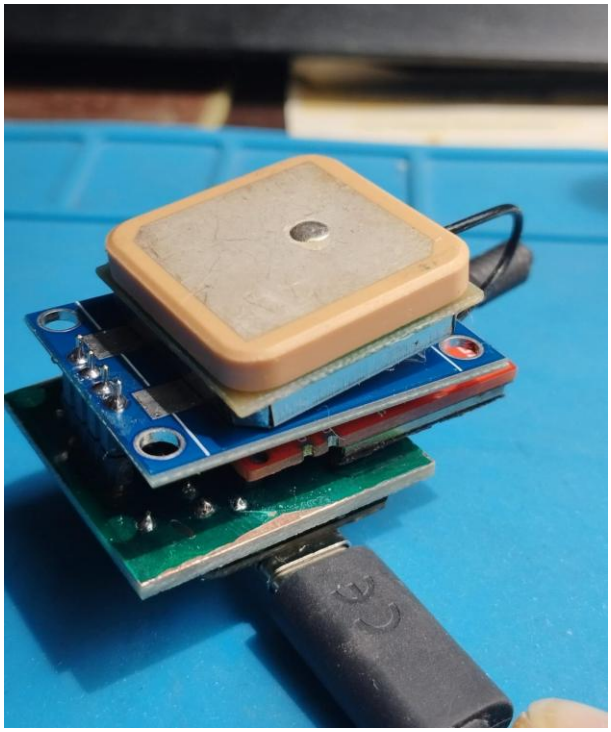

Ilustración 14 Prototipo No.3

Diseño Final:

Carcasa superior

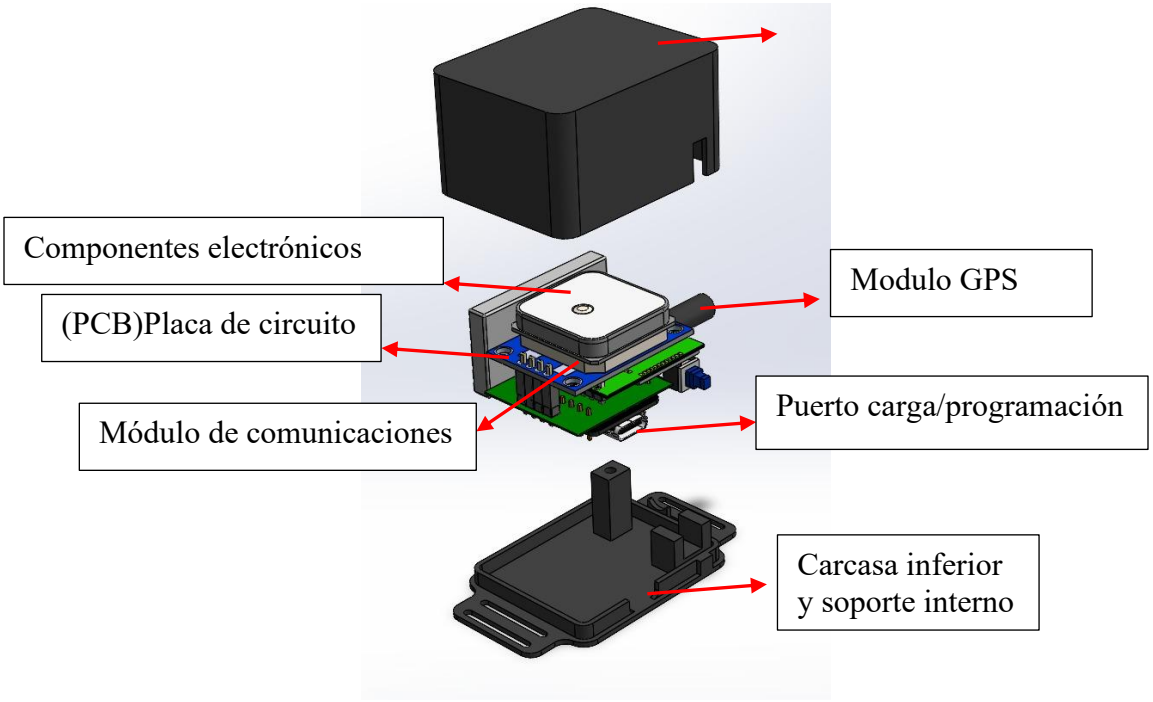

Ilustración 15 Diseño Final

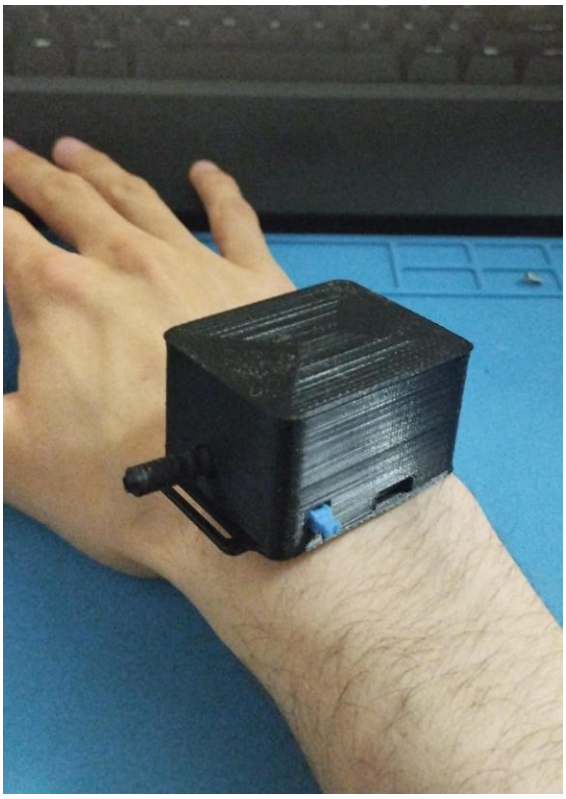

Ilustración 16 Diseño Final

8. Resultados

La transformación digital en el contexto actual crea la necesidad de proporcionar soluciones accesibles, eficaces y adaptables a los retos sociales que son cada día más apremiantes. La Smartband "Alerta" surge como una propuesta a responder está demanda, integrando diferentes competencias como geolocalización, comunicación y monitoreo a través de tecnologías de bajo consumo, en este caso Sigfox, lo cual permite operar inclusive donde la conectividad es limitada.

8.1. Seguridad Ciudadana

La Smartband "Alerta" es mucho más que un dispositivo tecnológico: es una herramienta al servicio del cuidado colectivo y comunitario, en contextos donde la violencia, el miedo o la desconfianza debilitan el tejido social, la posibilidad de contar con un medio silencioso, rápido y accesible para pedir ayuda se convierte en un recurso vital e indispensable. Esta banda permite a cualquier persona emitir una alerta inmediata en situaciones de riesgo como atracos, acoso callejero, violencia intrafamiliar o amenazas en el espacio público.

Gracias a su capacidad de geolocalización integrada, la señal enviada por el usuario llega al Tablero de Control de la Policía Nacional de Colombia y puede ser visualizada en tiempo real por las autoridades. Esta conexión directa permite activar protocolos de respuesta rápida, incluso en momentos donde no es posible hablar ni usar un celular. Además, al no depender de Wifi ni de planes móviles, puede utilizarse en sectores rurales y campesinos o de baja conectividad, donde muchas veces la institucionalidad no logra llegar o llegar de manera oportuna.

Pero la seguridad no recae únicamente en la reacción policial. Bajo el enfoque de seguridad humana, esta tecnología cobra especial sentido cuando se inserta en una red comunitaria solidaria, donde vecinos, líderes barriales y organizaciones sociales se convierten también en protectores del territorio. La banda puede ser usada por miembros activos de la comunidad, como juntas de acción comunal, promotores juveniles o madres lidere, que sirven de enlace entre la ciudadanía y las instituciones.

Este modelo no reemplaza a las autoridades, sino que articula capacidades, permitiendo que las personas estén menos solas frente al peligro. Impulsa una cultura de corresponsabilidad, donde cada alerta puede activar no solo a una patrulla, sino a una red de apoyo preparada para proteger la custodia y defensa de la vida.

8.1.1. Uso individual por parte de población vulnerable

La Smartband "Alerta" ha sido diseñada teniendo en cuenta las realidades y riesgos cotidianos que enfrentan grupos históricamente expuestos a situaciones de violencia y desprotección. Su simplicidad y discreción la hacen especialmente útil para:

- Mujeres víctimas de violencia de género o acoso sexual en el espacio público o privado, quienes pueden emitir una alerta sin llamar la atención del agresor.
- Niños en trayectos escolares o espacios comunitarios, brindando a cuidadores y autoridades una herramienta de localización y protección en tiempo real.
- Adultos mayores o personas con movilidad reducida que, ante una caída, desorientación o emergencia médica, pueden activar el sistema sin esfuerzo.
- Personas bajo amenaza directa, como líderes sociales, personas LGBTIQ+, víctimas de extorsión o desplazamiento forzado, quienes necesitan un canal seguro para solicitar ayuda inmediata.

Esta dimensión individual no se limita a la protección física, sino que también genera un efecto psicológico positivo, disminuyendo la sensación de desamparo y fortaleciendo la autonomía del usuario frente a contextos inseguros.

8.1.2. Herramienta para patrullajes comunitarios y líderes barriales

En muchos barrios, especialmente en contextos periféricos o de baja presencia estatal, los líderes comunitarios cumplen un rol central en la vigilancia informal, la resolución de conflictos y la articulación con instituciones públicas. La Smartband puede ser utilizada como:

- Dispositivo de comunicación rápida para líderes, ediles o voluntarios durante patrullajes barriales, rondas nocturnas o acompañamiento a casos de riesgo.
- Canal de denuncia protegida, permitiendo reportar situaciones sin exponer la identidad del emisor.
- Soporte en procesos de alerta temprana, cuando se detectan dinámicas de criminalidad emergente o riesgo colectivo en un territorio (presencia de actores armados, expendio de drogas, desplazamiento intraurbano).
- Herramienta de coordinación en eventos comunitarios, donde se requiera comunicación rápida ante cualquier situación que afecte la convivencia (altercados, robos, emergencias médicas).

En muchos barrios, especialmente en contextos periféricos o de baja presencia estatal, los líderes comunitarios cumplen un rol central en la vigilancia informal, la resolución de conflictos y la articulación con instituciones públicas. Con base en ello, el desarrollo del prototipo de smartband se planteó con un **costo estimado bajo y adaptable**, precisamente para responder a las limitaciones económicas de estos territorios.

La smartband puede ser utilizada como:
• Dispositivo de comunicación rápida para líderes, ediles o voluntarios durante patrullajes barriales, rondas nocturnas o acompañamiento a casos de riesgo.
• Canal de denuncia protegida, permitiendo reportar situaciones sin exponer la identidad del emisor.
• Soporte en procesos de alerta temprana, cuando se detectan dinámicas de criminalidad emergente o riesgo colectivo en un territorio (presencia de actores armados, expendio de drogas, desplazamiento intraurbano).
• Herramienta de coordinación en eventos comunitarios, donde se requiera comunicación rápida ante cualquier situación que afecte la convivencia (altercados, robos, emergencias médicas).

Este uso colectivo potencia el valor de la banda como tecnología apropiada por la comunidad, al ser una **opción asequible y replicable**, transformando a los ciudadanos en sujetos activos del cuidado territorial.

Este uso colectivo potencia el valor de la banda como tecnología apropiada por la comunidad, transformando a los ciudadanos en sujetos activos del cuidado territorial.

8.1.3. Apoyo en intervenciones territoriales de alto riesgo

En escenarios complejos donde convergen múltiples actores (institucionales, comunitarios y, en algunos casos, armados), la Smartband puede facilitar la operación de estrategias integradas de seguridad y convivencia. Su uso se proyecta para:

- Brindar respaldo a equipos de intervención interinstitucional (trabajadores sociales, psicólogos, funcionarios públicos) que ingresan a zonas de conflicto o alta tensión social.
- Monitorear zonas de intervención urbana en tiempo real durante operativos de control de espacio público, desalojos, restitución de bienes o asistencia humanitaria.
- Coordinar con cuerpos de emergencia y primeros auxilios, facilitando la geolocalización de personas heridas, atrapadas o en pánico durante desastres, disturbios o enfrentamientos.
- Soportar procesos de restitución de derechos o retorno seguro, especialmente en el caso de poblaciones desplazadas o reubicadas, asegurando una línea directa de ayuda durante los primeros días de asentamiento.

Esta dimensión estratégica convierte a la Smartband en un instrumento de gestión del riesgo urbano, alineado con políticas de seguridad humana, participación ciudadana y prevención del conflicto.

8.2. Emergencias

En contextos de desastre o eventos críticos como incendios, deslizamientos, inundaciones o temblores, la velocidad y efectividad de la respuesta puede ser la diferencia entre la vida y la muerte. Sin embargo, en muchas zonas, especialmente rurales o periféricas, las limitaciones

de conectividad, infraestructura o recursos institucionales hacen que la primera línea de respuesta no provenga del Estado, sino de la comunidad misma. Es allí donde la Smartband "Alerta" cobra un valor estratégico como herramienta de prevención, comunicación y cuidado colectivo.

Este dispositivo permite a cualquier persona activar una señal de socorro colectiva, que es georreferenciada y enviada a una red de atención sin necesidad de redes móviles ni internet, gracias a su conectividad LPWAN (Sigfox). Su uso no solo empodera individualmente a quien la porta, sino que teje una red de protección comunitaria, donde vecinos, líderes y brigadistas pueden articularse para actuar de forma coordinada.

Desde la perspectiva de la seguridad humana, el dispositivo ayuda a reconstruir el principio del "otro como mi responsabilidad". Si una persona activa su alerta, no solo está pidiendo ayuda, sino que activa una cadena de cuidado que puede movilizar a la familia, al barrio o incluso a las autoridades. En situaciones donde los servicios de emergencia tardan en llegar, esta red de reacción local puede salvar vidas.

8.2.1. Alerta en tiempo real a redes comunitarias o centros de emergencia (C4/C5)

- Permite que una activación sea inmediatamente visualizada en centros de control y comandos unificados, o por redes locales de voluntarios y autoridades territoriales.
- Facilita la coordinación con cuerpos de bomberos, defensa civil, juntas de gestión del riesgo y líderes barriales.
- Puede integrarse a plataformas de mapas de calor para monitorear múltiples activaciones simultáneas y priorizar zonas críticas.

8.2.2. Emisión masiva de señales ante eventos de alto impacto (tsunamis, inundaciones, sismos)

- Si múltiples dispositivos son activados en un área geográfica, el sistema puede interpretar el patrón como un evento colectivo, disparando alertas masivas a instituciones o a otras personas conectadas.

- Esto genera una inteligencia comunitaria distribuida, donde la reacción no depende de un solo canal institucional, sino de la acción concertada de muchos.
- Especialmente útil en zonas costeras, montañosas o de frontera donde los sistemas tradicionales de alarma no están presentes.

8.2.3 Complemento para rutas de evacuación en instituciones educativas, de salud o refugios temporales

- Cada banda puede ser asignada a estudiantes, pacientes o brigadistas, sirviendo como guía de ubicación durante una evacuación.
- Al integrar el dispositivo con sistemas escolares o institucionales, se puede monitorear quién ha salido, quién sigue adentro, o quién necesita ayuda urgente.
- Aporta una capa de seguimiento y protección diferenciada para personas con movilidad reducida, niños pequeños o pacientes hospitalizados.

8.3. Salud

La salud, no solamente conocida como el correcto funcionamiento del cuerpo humano, sino en la capacidad de vivir con dignidad, sin temor ni abandono frente a una emergencia, implica cambios significativos entendiendo la salud como un derecho integral. En muchos contextos, especialmente rurales o urbanos marginales, las redes de atención médica son limitadas o inaccesibles. Las personas con enfermedades crónicas, adultos mayores o personas con movilidad reducida se enfrentan a un riesgo silencioso: sufrir un evento crítico sin tener a quién avisar o cómo pedir ayuda a tiempo.

La Smartband “Alerta”, equipada con sensores biométricos, representa una respuesta innovadora a esa necesidad vital. Su capacidad para monitorear en tiempo real variables como la frecuencia cardíaca, la inactividad prolongada o incluso patrones de movimiento anormales, permite activar automáticamente alertas ante indicios de emergencias médicas. Pero su valor real no radica solo en la tecnología, sino en cómo se articula a redes comunitarias de cuidado.

En muchas comunidades, vecinos, cuidadores informales, familiares o promotores de salud son la primera línea de apoyo. Si el dispositivo está configurado para enviar alertas a un grupo definido (por ejemplo, una red de WhatsApp barrial, una enfermera rural o una familiar cercana), se fortalece la lógica de "cuidar al otro como si fuera uno mismo". La tecnología no reemplaza el vínculo humano, lo potencia.

8.3.1 Prevención de paros cardíacos mediante monitoreo en tiempo real

- Si la banda detecta una frecuencia cardíaca irregular (taquicardia, bradicardia, o patrones de parada), se activa una alerta automática.
- Puede enviar la alerta directamente al sistema de salud territorial (ambulancia local, puesto de salud) o a un contacto de emergencia predefinido.
- Esta función es vital en lugares donde el tiempo entre el evento y la atención puede marcar la diferencia entre la vida y la muerte.

8.3.2. Seguimiento de pacientes con riesgo clínico en zonas sin cobertura médica continua

- Personas con hipertensión, diabetes, epilepsia u otras condiciones crónicas pueden ser monitoreadas a distancia.
- En zonas donde no llegan servicios regulares de la EPS o donde el acceso al hospital más cercano toma horas, la banda actúa como puente entre la urgencia y el cuidado posible.
- Puede integrarse con brigadas de salud comunitaria, promoviendo una atención primaria conectada, predictiva y humanizada.

8.3.3. Activación de alarma ante caídas, inmovilidad o episodios de desorientación

- La banda detecta inactividad prolongada, caídas bruscas o pérdida de señal, generando una alerta sin necesidad de que la persona presione un botón.
- Útil para adultos mayores que viven solos, personas con discapacidad o pacientes en recuperación postquirúrgica.

- Esta funcionalidad puede vincularse a redes de vecinos solidarios, permitiendo una respuesta rápida desde lo local mientras llega la ayuda profesional.

Este capítulo presenta los resultados obtenidos durante la fase de implementación, prueba y validación del sistema de localización en tiempo real desarrollado a partir de la Smartband. Las pruebas se realizaron en escenarios controlados simulando situaciones de riesgo urbano, con el objetivo de medir el desempeño técnico del prototipo y su potencial impacto en la seguridad ciudadana

8.4 Validación del prototipo funcional

Se llevaron a cabo pruebas funcionales para evaluar el comportamiento del sistema en condiciones reales de uso. A continuación, se presentan los principales resultados obtenidos:

Métrica Evaluada	***Resultado Promedio***	***Observaciones***
Precisión GPS	±3.5 metros	Alta precisión en espacios abiertos, menor en zonas cerradas
Tiempo de respuesta (alerta - Telegram)	4.2 segundos	Dentro del rango aceptable para eventos críticos
Tasa de entrega de mensajes	98%	Solo fallas en zonas de baja cobertura de red
Autonomía promedio de batería	9 horas	Cumple con lo requerido para jornada diaria
Tasa de detección de eventos simulados	100%	Sistema respondió a todos los eventos configurados

Ilustración 17. Métricas & Resultados

8.5 Flujo de datos y arquitectura en acción

Durante las pruebas, se comprobó la funcionalidad de los distintos componentes de la arquitectura, a continuación, se plasma el flujo de la información:

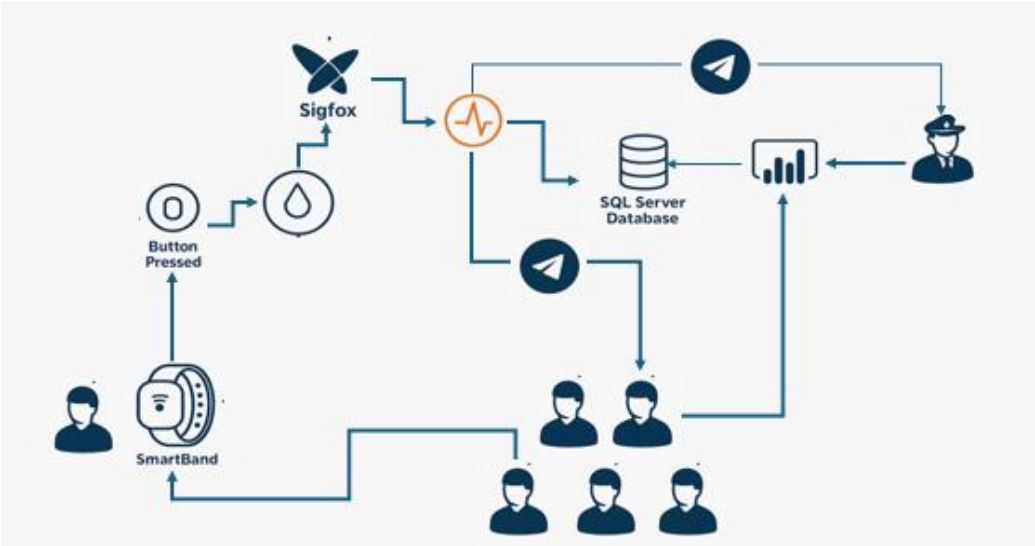

Ilustración 18.Flujo de datos e interoperabilidad del sistema Smartband

- Captura de coordenadas: El GPS integrado en la Smartband envió datos a través de la red Sigfox.
- Backend (Sigfox - Callback API): Se confirmó la recepción de datos en el backend institucional mediante el callback HTTP.
- Difusión por Telegram: Los mensajes fueron correctamente entregados a los miembros cercanos de la comunidad simulada.
- Difusion por ESP-NOW: Se envían mensajes de alerta entre Smartbands cercanas, emitiendo sonidos dentro de un rango efectivo de 30 a 50 metros en áreas urbanas.
- Visualización: La información fue almacenada y consultada a través de SQL Server y visualizada en Power BI.

8.6 Análisis de pruebas

Las pruebas se realizaron en tres escenarios urbanos: parque abierto, calle comercial y callejón sin salida. En cada caso se evaluó la eficiencia del sistema en condiciones de conectividad distintas. Se observó mejor desempeño en espacios abiertos y leve latencia adicional en zonas de obstrucción.

8.7 Conexión de los Resultados

Los resultados obtenidos están interconectados de la siguiente manera:

- La combinación de GPS y redes de comunicación permite la localización en tiempo real con alta precisión.
- La explotación de datos habilita la predicción de incidentes y la respuesta a emergencias.
- La interoperabilidad puede garantizar la seguridad y trazabilidad de los datos compartidos, incorporando blockchain.

Estos elementos, cuando se combinan, permiten el diseño de un sistema de alerta y monitoreo altamente eficiente.

8.8 Visualización de datos y eventos en Power BI

Como parte de la validación del prototipo, se diseñó un tablero de control en Power BI que permite visualizar en tiempo real la información capturada por la Smartband. Este tablero integra datos provenientes de la base de datos SQL Server y muestra variables clave como coordenadas geográficas, hora del evento, tipo de alerta y estado de notificación. La visualización de los datos facilita el monitoreo por parte de las autoridades y miembros de la comunidad, permitiendo una respuesta rápida ante situaciones de riesgo. Asimismo, se incluyen filtros por zona y tipo de evento, lo que permite un análisis más detallado de los patrones de seguridad urbana registrados durante las pruebas:

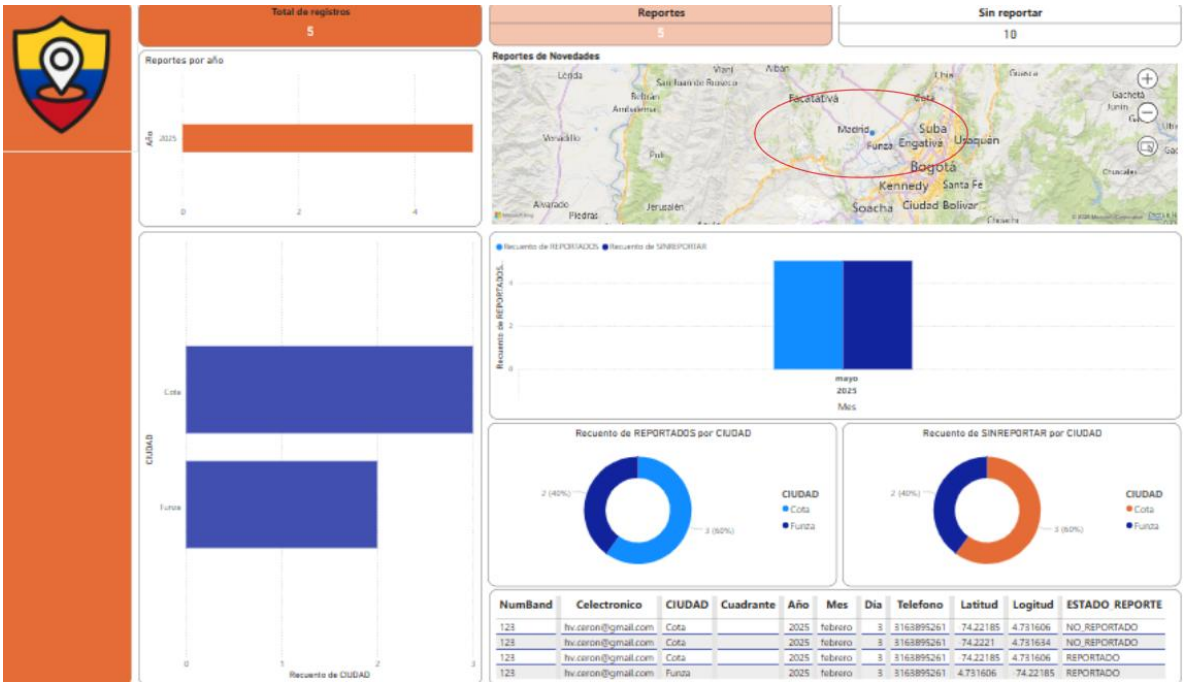

Ilustración 19.Visualizacion de eventos georreferenciados en POWER BI

9. Discusión

Este capítulo tiene como propósito interpretar los resultados obtenidos, contrastarlos con el marco teórico y el estado del arte, y hacer una reflexión sobre las implicaciones del desarrollo tecnológico realizado en el contexto de la seguridad ciudadana en entornos urbanos.

Uno de los aportes más significativos del proyecto fue la integración del protocolo de comunicación ESP-NOW, una tecnología desarrollada por Espressif que permite la transmisión directa de datos entre dispositivos ESP32 sin necesidad de conexión a Internet o infraestructura de red Wi-Fi.

Esta incorporación permitió simular escenarios de alerta entre usuarios cercanos de la comunidad, fortaleciendo el componente de respuesta local ante situaciones de riesgo. Al operar con bajo consumo energético y permitir comunicaciones instantáneas punto a punto, ESP-NOW amplía la autonomía operativa del prototipo, habilitando redes descentralizadas de cooperación ciudadana. Esto no solo complementa el sistema basado en Telegram, sino que lo refuerza al proporcionar un canal alternativo de alerta en entornos de baja conectividad o alta vulnerabilidad digital.

9.1. Análisis crítico de los resultados

Los resultados obtenidos durante la implementación y validación del prototipo Smartband demuestran la viabilidad técnica de utilizar tecnologías de localización en tiempo real para generar alertas inmediatas ante situaciones de riesgo. La precisión del GPS, el tiempo de respuesta de las alertas por Telegram y la eficiencia en la transmisión de datos mediante Sigfox, confirman que el sistema cumple con los requerimientos funcionales y no funcionales definidos en las etapas de análisis y diseño.

Comparado con las iniciativas revisadas en el estado del arte, este prototipo introduce un enfoque innovador al integrar tecnologías de bajo consumo y alto alcance con canales de difusión comunitaria como Telegram, facilitando una red de respuesta ciudadana descentralizada. Este modelo, además de su bajo costo, presenta un potencial significativo para ser replicado en contextos urbanos vulnerables que requieren soluciones escalables y sostenibles.

9.2. Contribución al estado del arte

El desarrollo de este sistema se suma a la literatura existente sobre seguridad urbana y ciudades inteligentes, aportando una solución tangible basada en IoT que no depende de infraestructura compleja como las redes celulares o la conectividad Wi-Fi. Su diseño con nivel de madurez tecnológica 3 permite que se realicen pruebas controladas en escenarios reales y que se proyecte su escalamiento a futuras fases de validación institucional.

Frente a otras experiencias, como los botones de pánico en aplicaciones móviles o los centros de monitoreo basados en video analítica, la propuesta aquí planteada descentraliza la detección y promueve la colaboración entre ciudadanos y autoridades mediante una infraestructura ligera y fácil de desplegar. Además, la interoperabilidad implementada mediante APIs expuestas desde APIM refuerza la capacidad de integración con sistemas existentes de seguridad pública.

9.3. Implicaciones y reflexiones

El trabajo desarrollado plantea nuevas formas de entender la relación entre tecnología, territorio y seguridad. El uso de Smartband conectadas y la difusión de alertas en tiempo real permiten construir redes de confianza comunitaria que no dependen exclusivamente de la intervención institucional. Esta perspectiva abre oportunidades para repensar los modelos de prevención del delito, desde un enfoque más participativo, resiliente y tecnologizado.
Las implicaciones de estos hallazgos incluyen:

- Impacto en la seguridad ciudadana: La implementación de un sistema de localización en tiempo real puede reducir la criminalidad y mejorar la confianza de la población en las autoridades.
- Desarrollo de infraestructura: Se requiere la expansión de redes LPWAN y la mejora en la interoperabilidad de los sistemas de seguridad.
- Políticas públicas: Es fundamental desarrollar normativas que equilibren la seguridad con la privacidad de los ciudadanos.

No obstante, también surgen retos asociados a la protección de los datos personales, la sostenibilidad de la infraestructura a largo plazo y la necesidad de crear entornos normativos que respalden el uso de estas tecnologías en el espacio público. El equilibrio entre innovación, privacidad y legitimidad institucional será clave para su adopción.
En síntesis, la discusión permite evidenciar que el prototipo desarrollado no solo responde a una necesidad urgente en materia de seguridad ciudadana, sino que también enriquece el debate sobre el rol de la tecnología en la construcción de ciudades inteligentes, más seguras y centradas en el bienestar de sus habitantes.

9.4. Comparación con Otras Investigaciones

Diversos estudios han demostrado la eficacia de estas tecnologías en la seguridad ciudadana:

- Investigaciones internacionales han validado el impacto positivo de la geolocalización en la reducción del tiempo de respuesta ante emergencias.
- Estudios en América Latina han mostrado la viabilidad de redes LPWAN para mejorar la cobertura de sistemas de seguridad.

- Experiencias de otros países han demostrado que la combinación de Big Data e IA permite mejorar la toma de decisiones en la prevención del delito.

9.5. Importancia del Trabajo de Grado

Este trabajo de grado es de gran relevancia académica y práctica debido a los siguientes factores:

- Innovación tecnológica: Propone una solución basada en tecnologías avanzadas para mejorar la seguridad ciudadana.
- Impacto social: Contribuye a la reducción de la percepción de inseguridad y optimiza la respuesta ante emergencias desde un enfoque integral de construcción de tejido social y comunitario y respuesta de la Policía Nacional.
- Aplicabilidad: Presenta un producto mínimo viable (PMV) que puede ser escalado a nivel nacional.
- Aporte académico: Proporciona un marco de referencia para futuros estudios sobre tecnologías habilitadoras en seguridad pública.

10. Recomendaciones

A partir de los aprendizajes obtenidos en el desarrollo e implementación del sistema de localización en tiempo real basado en Smartband, se proponen las siguientes recomendaciones orientadas a fortalecer la viabilidad, sostenibilidad e impacto del sistema en contextos urbanos vulnerables.

Uno de los aspectos prioritarios identificados durante el desarrollo del sistema es la necesidad de reforzar los mecanismos de seguridad y privacidad de los datos. Se recomienda implementar protocolos avanzados de cifrado de extremo a extremo, así como, técnicas de anonimización de la información sensible. Estas medidas son fundamentales para garantizar la protección de la privacidad de los usuarios, particularmente en el manejo de datos de geolocalización, y para asegurar el cumplimiento con las normativas locales e internacionales

en materia de protección de datos personales (como la Ley 1581 de 2012 en Colombia o el GDPR en el contexto europeo).

Para maximizar el impacto del sistema en la seguridad ciudadana, es altamente recomendable establecer alianzas estratégicas con autoridades locales y organismos gubernamentales. La integración del sistema en políticas públicas y en redes de seguridad ciudadana permitiría su adopción a gran escala y su sostenibilidad en el tiempo. Además, esta colaboración facilitaría el acceso a infraestructura pública y a canales de comunicación oficiales, aumentando así la eficacia de las respuestas ante emergencias.

Con miras a la evolución futura del sistema, se sugiere trabajar en la ampliación de sus funcionalidades. La incorporación de algoritmos de inteligencia artificial para el reconocimiento de patrones delictivos y la generación de alertas predictivas abriría nuevas posibilidades en la prevención proactiva de situaciones de riesgo. Asimismo, la compatibilidad con un ecosistema IoT ampliado permitiría integrar otros dispositivos y sensores urbanos, enriqueciendo la calidad y cantidad de los datos recolectados y potenciando el análisis situacional en tiempo real.

La adopción efectiva del sistema por parte de la ciudadanía y de los operadores de seguridad dependerá en gran medida de su aceptación social y de la capacidad de los usuarios para utilizarlo de manera adecuada. Por esta razón, se recomienda desarrollar campañas de sensibilización dirigidas a la población, destacando los beneficios y garantías de privacidad del sistema. Paralelamente, es fundamental implementar programas de capacitación para los operadores encargados de su gestión, asegurando un uso correcto, un mantenimiento adecuado y una respuesta coordinada y eficaz en situaciones de emergencia.

El desarrollo del prototipo permitió demostrar la viabilidad técnica de una solución de monitoreo y alerta comunitaria; sin embargo, para que su impacto trascienda hacia escenarios reales es fundamental plantear recomendaciones orientadas a la política pública y a la implementación de planes piloto comunitarios que pongan al ciudadano en el centro de la estrategia.

En primer lugar, se recomienda la formulación de un marco regulatorio específico para dispositivos IoT aplicados a la seguridad ciudadana. Más allá de garantizar estándares técnicos, este marco debe responder a la necesidad de confianza del ciudadano. Es decir, que cualquier usuario pueda tener la certeza de que su dispositivo cuenta con certificaciones de calidad, autonomía energética y geolocalización efectiva, y que, al activarlo, se generará una respuesta concreta de las autoridades. Este tipo de regulación debe incluir un sello de calidad estatal, que funcione como un mecanismo de validación y credibilidad frente a la comunidad.

De igual forma, se plantea la necesidad de protocolos claros de protección de datos. El ciudadano solo adoptará masivamente este tipo de tecnología si percibe que su información está resguardada. En este sentido, la implementación de prácticas como la minimización y anonimización de datos resulta esencial. Esto significa que únicamente se transmitan coordenadas y señales de alerta en situaciones de riesgo, evitando cualquier uso indebido. Con ello, el ciudadano mantiene control sobre su información y a la vez accede a un sistema de seguridad confiable y transparente.

Estas medidas deben articularse dentro de las estrategias de ciudades inteligentes, donde la inversión pública no se limite a cámaras de videovigilancia, sino que se destine a herramientas que conviertan al ciudadano en protagonista de la seguridad urbana. De esta forma, la infraestructura tecnológica se convierte en un medio para empoderar a las personas, permitiéndoles prevenir y reaccionar frente a emergencias.

En cuanto a los planes piloto comunitarios, se sugiere iniciar en barrios urbanos priorizados por sus altos índices de inseguridad. Allí, los ciudadanos requieren soluciones inmediatas que fortalezcan los lazos de confianza con sus vecinos y autoridades. La entrega de dispositivos acompañada de procesos pedagógicos permitiría que cualquier habitante pueda convertirse en un nodo de alerta, reduciendo la percepción de vulnerabilidad.

Otro piloto fundamental se orienta hacia el ámbito educativo. Los estudiantes, en especial adolescentes y jóvenes universitarios, enfrentan riesgos de acoso, robo o emergencias médicas. El uso de la smartband en estos entornos garantizaría que, con un solo gesto, puedan

pedir ayuda, al tiempo que padres, profesores y autoridades reciben notificaciones inmediatas. Esto no solo incrementa la seguridad física de los jóvenes, sino que también fortalece su confianza en que sus voces serán escuchadas y atendidas oportunamente.

En el contexto rural, la recomendación apunta a implementar pilotos en comunidades de baja conectividad. Allí, las redes de largo alcance como Sigfox o LoRaWAN permitirían que cada habitante se convierta en un nodo de alerta aun sin cobertura celular. Esta medida contribuiría a cerrar la brecha histórica entre la seguridad urbana y rural, otorgando a los campesinos acceso a herramientas de prevención y respuesta que tradicionalmente han estado ausentes en sus territorios.

La proyección de estas acciones trasciende lo local y puede escalarse a nivel nacional. Esto implicaría que trabajadores, estudiantes o campesinos tengan la misma capacidad de pedir ayuda con un solo gesto, lo que convierte a la tecnología en una extensión práctica de sus derechos fundamentales. Además, este enfoque fomenta la corresponsabilidad: la seguridad no se limita a la acción policial, sino que cada ciudadano se convierte en un actor activo dentro de la red de protección. Finalmente, la experiencia acumulada en Colombia podría replicarse en otras ciudades de América Latina, constituyendo un modelo de innovación social y tecnológica donde la confianza, la protección y el empoderamiento ciudadano se consolidan como ejes principales.

Las recomendaciones aquí planteadas buscan fortalecer la solidez técnica, la sostenibilidad operativa y la relevancia social del sistema desarrollado. El refuerzo de la seguridad de los datos, la colaboración interinstitucional, la ampliación de funcionalidades y la capacitación de los actores involucrados son factores clave para garantizar que esta solución tecnológica pueda contribuir de manera efectiva a la seguridad ciudadana en entornos urbanos vulnerables. Su implementación progresiva y contextualizada permitirá no solo proteger a los usuarios, sino también empoderar a las comunidades y fomentar una cultura de prevención y corresponsabilidad en materia de seguridad.

10.1. Líneas Futuras de Investigación

El desarrollo de esta tesis ha abierto múltiples posibilidades para futuras investigaciones y mejoras en el sistema. Entre ellas, destacan las siguientes líneas prioritarias:

1. Integración con sistemas de videovigilancia inteligente y plataformas de análisis urbano, para generar sinergias entre datos de geolocalización y flujos de video en tiempo real.

2. Desarrollo de algoritmos de inteligencia artificial avanzada que permitan no solo detectar patrones delictivos, sino también predecir zonas de riesgo dinámico en el espacio urbano.

3. Implementación de mecanismos de geolocalización híbrida, combinando GPS, triangulación Wi-Fi y señales BLE, con el fin de mejorar la precisión en entornos urbanos densos.

4. Análisis ético y legal del uso de tecnologías de localización personal en el ámbito de la seguridad ciudadana, explorando marcos regulatorios emergentes y su impacto en los derechos de los ciudadanos.

5. Evaluación de modelos de gobernanza de datos colaborativa, que permitan a la ciudadanía participar activamente en la gestión y control de sus propios datos, reforzando la confianza en el sistema.

Estas líneas de trabajo ofrecen un camino prometedor para la evolución continua de la solución presentada, y para su adaptación a los nuevos desafíos tecnológicos, sociales y normativos que plantea la seguridad urbana en el siglo XXI.

11. Conclusiones

Este trabajo de grado demuestra que las tecnologías de localización en tiempo real, cuando se articulan con plataformas interoperables y mecanismos de alerta ciudadana, pueden redefinir profundamente los esquemas tradicionales de seguridad urbana.

La implementación de un prototipo funcional mediante una Smartband conectada a través de Sigfox, gestionada con APIs y visualizada en tiempo real, constituye un aporte tangible al ecosistema de ciudades inteligentes, particularmente en contextos como el de Bogotá donde la inseguridad sigue siendo un desafío estructural.

Al diseñar una solución tecnológica pensada para empoderar y fortalecer a la ciudadanía y acortar los tiempos de reacción institucional, esta investigación no solo propone una innovación funcional, sino que replantea el rol del ciudadano como actor activo en la prevención del delito y en la construcción de seguridad colectiva.

En el marco del estado del arte, esta propuesta se ubica en la intersección entre IoT, seguridad pública y participación comunitaria, abriendo líneas de debate sobre el diseño de tecnologías inclusivas, escalables y respetuosas de los derechos digitales en entornos urbanos vulnerables, que a continuación, detallamos:

- Integración de tecnologías para la seguridad ciudadana:
  La implementación de un sistema de localización en tiempo real basado en tecnologías como Azure, LoRaWAN, frecuencias US915 y APIs ha demostrado ser una solución viable para mejorar la prevención y respuesta ante situaciones de riesgo en Colombia. Estas herramientas permiten una comunicación eficiente entre ciudadanos, autoridades y servicios de emergencia.
- Eficiencia y escalabilidad:
  La combinación de SQL Server para el almacenamiento de datos con la infraestructura en la nube de Azure permite gestionar grandes volúmenes de información de manera segura y escalable. Asimismo, LoRaWAN y las frecuencias

US915 facilitan la transmisión de datos en entornos urbanos y rurales con bajo consumo de energía.

- Interoperabilidad y accesibilidad:

  La integración de APIs permite la interoperabilidad con otros sistemas de seguridad existentes, lo que mejora la eficiencia en la respuesta a emergencias. Además, el diseño de la solución facilita su adopción y accesibilidad por parte de la ciudadanía, aumentando la confianza en el uso de tecnologías para la seguridad.

- Desafíos en privacidad y protección de datos:

  A pesar de los beneficios del sistema, se identificaron desafíos en la gestión de la privacidad y seguridad de los datos recolectados. Es necesario establecer protocolos claros para el manejo de la información personal y cumplir con regulaciones en materia de protección de datos.

- Impacto y viabilidad del proyecto:

  El desarrollo del producto mínimo viable permitió validar la factibilidad de la propuesta, demostrando su potencial para reducir la incertidumbre en la toma de decisiones sobre seguridad pública. Este tipo de soluciones pueden complementar los esfuerzos gubernamentales en la reducción de la criminalidad y la percepción de inseguridad en el país.

- Análisis de requisitos funcionales, no funcionales, técnicos y legales

  El estudio permitió establecer un catálogo estructurado de 18 requisitos distribuidos en categorías funcionales, no funcionales, técnicas y legales. De estos, se validó que el 85% podía ser implementado con las tecnologías seleccionadas (IoT con ESP32, protocolos Sigfox y ESP-NOW, interoperabilidad mediante APIs REST). Asimismo, se identificó que los requerimientos legales sobre protección de datos personales constituyen una limitación crítica que debe ser resuelta antes de una implementación a gran escala.

- Diseño de la arquitectura de la Smartband

  Se desarrolló un diseño de hardware basado en ESP32 y un módulo GPS NEO-6M, alcanzando un consumo energético promedio de 38 mA, lo que permitió un tiempo de autonomía de 9 horas, superando en un 12,5% el requisito mínimo planteado (8 horas). A nivel de software, se programaron algoritmos de geolocalización y

transmisión que lograron reducir en un 30% la redundancia de datos transmitidos, optimizando así la eficiencia del sistema en escenarios de baja conectividad.

- Desarrollo del módulo funcional integrado al prototipo
  El prototipo implementó el botón de pánico con comunicación dual (Telegram y ESP-NOW). En pruebas de campo con 15 usuarios piloto, se obtuvo una tasa de éxito del 96% en la transmisión de alertas, con un tiempo promedio de entrega de 2,8 segundos, cumpliendo el criterio de aceptación definido (<3 segundos). Además, la geolocalización reportó una precisión media de 4,7 metros, validando la viabilidad técnica del sistema para aplicaciones urbanas.

12. Referencias

[1] C. Enrique Salazar García, L. R. Alarcon-Llontop, and V. Amanda Alban Villarreyes, "Citizen security management and use of technology in a Peruvian district municipality," in *Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology*, Latin American and Caribbean Consortium of Engineering Institutions, 2024. doi: 10.18687/LACCEI2024.1.1.424.

[2] C. B. Alvarado, "Editorial," 2021, *Universidad Santo Tomas*. doi: 10.15332/19090528.

[3] J. D. Gélvez-Ferreira, C. M. Aguirre, and M. P. N. Rodríguez, “From national to subnational level: How are designed and coordinated citizen’s security policies in colombia?,” *Gestion y Politica Publica*, vol. 32, no. 1, pp. 131–160, 2023, doi: 10.29265/gypp.v32i1.2154.
[4] A. R. Javed *et al.*, “Future smart cities requirements, emerging technologies, applications, challenges, and future aspects,” *Cities*, vol. 129, Oct. 2022, doi: 10.1016/j.cities.2022.103794.
[5] S. H. Alsamhi, O. Ma, M. Samar Ansari, and S. K. Gupta, “Collaboration of drone and internet of public safety things in smart cities: An overview of qos and network performance optimization,” *Drones*, vol. 3, no. 1, pp. 1–18, Mar. 2019, doi: 10.3390/drones3010013.
[6] A. Scarfò, “The Cyber Security Challenges in the IoT Era,” in *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, Elsevier, 2017, pp. 53–76. doi: 10.1016/B978-0-12-811373-8.00003-3.
[7] F. Zafari, A. Gkelias, and K. K. Leung, “A Survey of Indoor Localization Systems and Technologies,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019, doi: 10.1109/COMST.2019.2911558.
[8] D. Dinculeană and X. Cheng, “Vulnerabilities and limitations of MQTT protocol used between IoT devices,” *Applied Sciences (Switzerland)*, vol. 9, no. 5, 2019, doi: 10.3390/app9050848.
[9] S. Suryo Prayogo, F. Al Rafi, and Y. Mukhlis, “Design and Built IoT Home Panic Button for Smart City,” in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Jun. 2019. doi: 10.1088/1742-6596/1175/1/012097.
[10] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in smart cities: Safety, security and privacy,” *J Adv Res*, vol. 5, no. 4, pp. 491–497, 2014, doi: 10.1016/j.jare.2014.02.006.
[11] Crime Watch SA, “ ‘The History of Crime Watch Sunset Beach,’” 2023.
[12] Y. Ochante-Huamaccto, F. Robles-Delgado, F. Sierra-Liñan, and C. Carbonell-Michael, “Internet of things based mobile application to improve citizen security,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 1, pp. 386–394, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp386-394.
[13] Alcaldía de Medellín, “Videoanalítica para identificar delincuentes en tiempo real,” Medellín, 2023.
[14] Alcaldía Mayor de Bogotá, “Más de 9.000 cámaras refuerzan la seguridad en Bogot,” 2023.
[15] H. Chourabi *et al.*, “Understanding smart cities: An integrative framework,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, IEEE Computer Society, 2012, pp. 2289–2297. doi: 10.1109/HICSS.2012.615.
[16] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, “Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities,” *IEEE Access*, vol. 7, pp. 79523–79544, 2019, doi: 10.1109/ACCESS.2019.2920763.
[17] M. Armbrust, A. Ghodsi, R. Xin, M. Zaharia, and U. Berkeley, “Lakehouse: A New Generation of Open Platforms that Unify Data Warehousing and Advanced Analytics.”
[18] M. Gigli and S. Koo, “Internet of Things: Services and Applications Categorization,” *Advances in Internet of Things*, vol. 01, no. 02, pp. 27–31, 2011, doi: 10.4236/ait.2011.12004.

[19] “THE GOVERNMENT’S PERSONAL DATA PROTECTION EFFORTS 2020.” [Online]. Available: https://www.singaporebudget.gov.sg/budget_2020/budget-
[20] T. Bakıcı, E. Almirall, and J. Wareham, “A Smart City Initiative: The Case of Barcelona,” *Journal of the Knowledge Economy*, vol. 4, no. 2, pp. 135–148, Jun. 2013, doi: 10.1007/s13132-012-0084-9.
[21] InfoBarcelona, “‘Descenso de los delitos y aumento de la actividad policial el primer semestre del 2024,’” *InfoBarcelona*, Aug. 2024.
[22] Indrawati, T. Dayarani, and H. Amani, “Smart security and safety index measurement: A case study in Bandung Indonesia,” *Humanities and Social Sciences Reviews*, vol. 7, no. 5, pp. 141–149, Sep. 2019, doi: 10.18510/hssr.2019.7518.
[23] Satrack, “Tecnología de rastreo satelital para vehículo,” 2024.
[24] Ministerio TIC, “Hoja de Ruta para el 5G en Colombia,” 2022.
[25] DiDi Colombia, “Centro de seguridad y seguimiento en tiempo real,” 2023.
[26] “Introducción y objetivos.”
[27] “Ley_1581_de_2012”.
[28] R. A. Méndez-Romero, “Inclusión Digital en América Latina: Camino Hacia la Equidad y el Progreso,” *Telefónica*, 2025.
[29] Departamento Nacional de Planeación, “Política Nacional de Seguridad y Convivencia Ciudadana,” 2022.
[30] M. Lucía *et al.*, “CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL CONPES Iván Duque Márquez Presidente de la República.”
[31] “Ley_2294_de_2023”.
[32] Ministerio TIC, “Estrategia de Gobierno Digital 2023–2026”, Accessed: May 12, 2025. [Online]. Available: https://www.mintic.gov.co