
# UNIVERSIDAD PRIVADA DE TACNA

## FACULTAD DE INGENIERÍA

### Escuela Profesional de Ingeniería de Sistemas

# "Sistema de alerta basado en tecnología LoRaWAN para optimizar la respuesta de emergencias por violencia contra la mujer e integrantes del grupo familiar en Perú, 2025"

Curso: *CONSTRUCCIÓN DE SOFTWARE I*

Docente: *Ing. Alberto Johnatan Flor Rodríguez*

Integrantes:

Daleska Nicolle Fernandez Villanueva (2021070308)

**Tacna – Perú**
**2025**

# Sistema de alerta basado en tecnología LoRaWAN para optimizar la respuesta de emergencias por violencia contra la mujer e integrantes del grupo familiar en Perú, 2025

## Resumen Ejecutivo

***Versión 1.0***

| CONTROL DE VERSIONES | | | | | |
|---|---|---|---|---|---|
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | DFV | DFV | DFV | 29/10/2025 | Versión Original |

## ÍNDICE GENERAL

## RESUMEN EJECUTIVO

### 1. Propuesta narrativa

#### 1. Planteamiento del Problema

La violencia contra las mujeres y los integrantes del grupo familiar representa una problemática social de grave incidencia en el Perú, con un impacto significativo tambien en la provincia de Tacna. Según datos del Ministerio de la Mujer y Poblaciones Vulnerables (MIMP), se ha evidenciado una tendencia alarmante. Entre enero y junio de 2025, la Línea 100 y los Centros de Emergencia Mujer (CEM) registraron un total de 6,948 atenciones por violencia familiar en la región Tacna, lo que subraya la prevalencia de este flagelo. De estas atenciones, un 84% correspondió a mujeres, con la violencia psicológica como la forma más recurrente (76%). Estas cifras confirman la necesidad imperante de reforzar los mecanismos de protección para las víctimas.

Actualmente, las herramientas digitales implementadas, como la versión más reciente del Servicio Judicial de Alerta: Botón de Pánico, si bien representan un avance importante, presentan ciertas limitaciones. Al ser una aplicación móvil, su funcionamiento depende de la cobertura de red celular y de la autonomía de la batería de los teléfonos, lo que compromete su confiabilidad en entornos de baja conectividad o cuando el dispositivo de la víctima se queda sin energía. Además, el flujo de alerta actual se basa en un proceso semi-manual que, aunque mejorado, aún incorpora un tiempo de procesamiento humano en el centro de monitoreo, con etapas de comunicación por radio que pueden introducir demoras críticas y errores.

Esta realidad crea una dicotomía entre la necesidad de una respuesta inmediata y las limitaciones tecnológicas y operativas de los sistemas existentes. Se identifica una brecha de investigación y desarrollo en la creación de una solución que sea verdaderamente autónoma, confiable y con una latencia de transmisión mínima para garantizar que la alerta llegue a las autoridades en segundos, sin depender de la infraestructura de telecomunicaciones comercial ni de la intervención manual del personal. La ausencia de un sistema de alerta

que aborde estas deficiencias representa un riesgo continuo para la seguridad de las víctimas.

Por consiguiente, el problema se centra en cómo desarrollar un sistema de alerta que, a través de la implementación de tecnología de vanguardia y un diseño enfocado en la fiabilidad, pueda mitigar los riesgos inherentes a los sistemas actuales y proporcionar una protección efectiva a los ciudadanos en situación de vulnerabilidad en el Peru.

## 2. Justificación del Proyecto

El desarrollo del presente proyecto se justifica por su impacto social, tecnológico y de seguridad. Al implementar un sistema de alerta basado en tecnología LoRaWAN, se propone una alternativa de comunicación de largo alcance, bajo consumo energético y alta confiabilidad, capaz de operar incluso en lugares sin cobertura celular. Este sistema permitirá reducir los tiempos de respuesta ante emergencias y fortalecer la coordinación entre las entidades de auxilio como la Policía Nacional del Perú en cada ciudad.

Desde una perspectiva tecnológica, la propuesta integra múltiples componentes de software y hardware: un dispositivo IoT autónomo, un servidor central de monitoreo, una aplicación web y una app móvil para las unidades de respuesta. Esta arquitectura garantiza la trazabilidad completa del proceso de alerta —desde su activación hasta la intervención—, promoviendo un enfoque de ingeniería de sistemas orientado a la eficiencia, escalabilidad y seguridad de los datos.

Finalmente, el proyecto se sustenta en su pertinencia social, al alinearse con los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas, específicamente el ODS 5 (igualdad de género) y el ODS 16 (paz, justicia e instituciones sólidas). Su implementación no solo busca mejorar la capacidad tecnológica del país frente a emergencias, sino también contribuir activamente a la protección de la vida y la integridad de las personas vulnerables.

3. **Objetivo General**

Diseñar e implementar un sistema de alertas basado en tecnología LoRaWAN para las respuestas de emergencia en casos de violencia contra la mujer e integrantes del grupo familiar en Perú, asegurando confiabilidad, cobertura y eficiencia en la transmisión de alertas.

## 4. Beneficios

La implementación del sistema de alerta basado en tecnología **LoRaWAN** ofrece múltiples beneficios en términos de seguridad, eficiencia operativa y sostenibilidad tecnológica. En primer lugar, proporciona una **comunicación confiable y continua**, incluso en zonas rurales o con limitada cobertura celular, permitiendo que las víctimas puedan generar alertas discretas y efectivas sin depender del servicio de internet móvil. Esto representa un avance significativo frente a los sistemas actuales que se ven limitados por la infraestructura de telecomunicaciones.

En segundo lugar, el sistema destaca por su **bajo consumo energético**, lo que prolonga la autonomía del dispositivo y reduce la necesidad de recargas frecuentes. Este beneficio es especialmente relevante en comunidades que carecen de acceso constante a electricidad, asegurando un funcionamiento continuo y confiable del dispositivo. Además, la transmisión eficiente mediante LoRaWAN minimiza costos operativos y contribuye a la sostenibilidad del sistema.

Finalmente, la integración del **dispositivo, servidor central y aplicaciones web y móviles** permite una **gestión automatizada de alertas** en tiempo real. Las autoridades competentes (PNP o Serenazgo) reciben notificaciones instantáneas, lo que reduce los tiempos de respuesta y mejora la coordinación interinstitucional. Este enfoque integral no solo fortalece la **seguridad ciudadana** y la **protección de las personas vulnerables**, sino que también optimiza los recursos tecnológicos y humanos destinados a la atención de emergencias.

## 5. Alcance

El sistema se encargará de las siguientes funcionalidades y módulos principales:

- **Gestión del Dispositivo Autónomo de Alerta Personal:**
  - Implementar el firmware optimizado (en C/C++ con ESP-IDF) para la gestión eficiente de la energía (modo deep sleep), la activación bajo demanda del módulo GPS para geolocalización precisa, la compilación de datos de alerta (ID del dispositivo, coordenadas GPS, nivel de batería) y su transmisión vía LoRaWAN.

  - Controlar un LED de confirmación en el dispositivo para indicar al usuario el envío exitoso de la alerta, proporcionando retroalimentación visual inmediata.

- **Conectividad y Reenvío de Datos LoRaWAN:**
  - Utilizar el servidor de red The Things Stack (TTS) para la recepción segura, desduplicación, desencriptación y reenvío confiable de los paquetes de datos LoRaWAN originados en el dispositivo autónomo.

  - Configurar integraciones (Webhooks o MQTT) en TTS para asegurar una entrega de datos en tiempo real y estructurada al Servidor Central de Monitoreo.

- **Procesamiento Central de Alertas (Servidor Central de Monitoreo):**
  - Desarrollar la capacidad del backend para recibir, decodificar y procesar los datos de alerta enviados desde The Things Stack.

  - Consultar la base de datos Firestore para correlacionar el ID del dispositivo con el perfil completo de la víctima y la información en tiempo real de las unidades de respuesta.

- Implementar la lógica para identificar la unidad policial o de serenazgo más cercana a la ubicación de la alerta y automatizar el despacho digital de dicha alerta.

- **Almacenamiento y Gestión de Datos en Tiempo Real (Firestore):**
  - Establecer una base de datos Firestore para el almacenamiento seguro y la gestión en tiempo real de perfiles de víctimas, registros históricos de alertas y, crucialmente, la ubicación actualizada de las unidades de respuesta (cada 5 segundos).

  - Facilitar la sincronización de datos en tiempo real para que tanto el dashboard central como las aplicaciones de las patrullas vean la información más reciente de manera instantánea.

- **Interfaz y Gestión para Unidades de Respuesta (Aplicación Móvil/Tablet):**
  - Desarrollar una aplicación móvil para el personal de la PNP y Serenazgo, que sirva como interfaz de usuario primaria en campo.

  - Proveer funcionalidades para la visualización interactiva de las alertas en un mapa (vía API de Google Maps), mostrando la ubicación de la víctima, los datos de su perfil y la posición de la propia patrulla y otras unidades.

  - Permitir la actualización del estado de la emergencia (aceptar, en ruta, resuelto) y el envío de la ubicación de la patrulla cada 5 segundos.

- **Validación y Pruebas del Prototipo:**
  - Ejecutar pruebas exhaustivas en laboratorio y en un entorno de campo controlado para validar la eficiencia energética del dispositivo, la tasa de éxito y la latencia de transmisión de la

alerta de extremo a extremo, así como la precisión de la geolocalización y la efectividad del sistema de despacho automatizado.

## 6. Requerimientos del Sistema

| ID | Nombre del Requisito | Descripción de Requisito |
|---|---|---|
| RF-001 | Gestión de Energía del Dispositivo | El firmware del dispositivo autónomo debe gestionar eficientemente el consumo de energía, utilizando modos de bajo consumo (deep sleep), para maximizar la autonomía de la batería. |
| RF-002 | Activación y Captura de Ubicación GPS | El dispositivo autónomo debe activar el módulo GPS bajo demanda (tras una pulsación) para adquirir las coordenadas geográficas precisas de la víctima. |
| RF-003 | Compilación y Preparación de Datos de Alerta | El firmware debe compilar los datos de alerta, incluyendo el ID único del dispositivo, las coordenadas GPS obtenidas y el nivel actual de la batería, en un formato apto para transmisión LoRaWAN. |
| RF-004 | Transmisión LoRaWAN de Alerta | El dispositivo autónomo debe transmitir de forma robusta y segura el paquete de datos de alerta a |

| | | |
|---|---|---|
| | | través del módulo LoRaWAN hacia la red LoRaWAN (The Things Stack). |
| RF-005 | Indicador LED de Confirmación | El dispositivo autónomo debe activar un LED de confirmación para proporcionar retroalimentación visual al usuario sobre el envío exitoso de la alerta. |
| RF-006 | Recepción y Procesamiento de Datos LoRaWAN (TTS) | El servidor de red The Things Stack (TTS) debe recibir, desduplicar y desencriptar los paquetes de datos provenientes de los dispositivos LoRaWAN. |
| RF-007 | Reenvío de Alertas a Servidor Central (TTS) | The Things Stack debe reenviar los datos de alerta procesados al Servidor Central de Monitoreo mediante integraciones configuradas (Webhooks o MQTT) en tiempo real. |
| RF-008 | Recepción y Decodificación de Alertas (SCM) | El Servidor Central de Monitoreo debe ser capaz de recibir y decodificar los datos de alerta enviados por The Things Stack. |
| RF-009 | Correlación de Dispositivo/Víctima | El Servidor Central de Monitoreo debe consultar la base de datos Firestore para correlacionar el ID del dispositivo de alerta con el perfil completo de la víctima asociada. |

| | | |
|---|---|---|
| RF-010 | Identificación de Unidad de Respuesta Cercana | El Servidor Central de Monitoreo debe identificar la unidad policial o de serenazgo más cercana a la ubicación de la alerta activa, basándose en las posiciones actualizadas de las patrullas en Firestore. |
| RF-011 | Despacho Automatizado de Alerta | El Servidor Central de Monitoreo debe enviar de forma automatizada la alerta digital, incluyendo los datos de la víctima y su ubicación, a la Aplicación Cliente de la unidad de respuesta identificada. |
| RF-012 | Almacenamiento y Gestión de Datos (Firestore) | El sistema debe utilizar Firestore para almacenar de forma segura los perfiles de víctimas, los registros históricos de alertas y las ubicaciones en tiempo real de las unidades de respuesta. |
| RF-013 | Sincronización de Datos en Tiempo Real | Firestore debe sincronizar en tiempo real las ubicaciones de las patrullas y el estado de las alertas entre el Servidor Central y las Aplicaciones Cliente, garantizando información actualizada para todos los usuarios. |
| RF-014 | Visualización de Alertas en Mapa (App Patrulla) | La Aplicación Cliente (móvil/tablet) para las unidades de respuesta debe |

| | | |
|---|---|---|
| | | mostrar interactivamente la ubicación de las alertas activas, la víctima y la propia patrulla en un mapa (API Google Maps). |
| RF-015 | Visualización de Perfil de Víctima (App Patrulla) | La Aplicación Cliente debe permitir al personal de la patrulla visualizar el perfil completo de la víctima asociada a una alerta. |
| RF-016 | Gestión del Estado de la Alerta (App Patrulla) | La Aplicación Cliente debe permitir a la unidad de respuesta actualizar el estado de la emergencia (ej. "aceptar", "en ruta", "resuelto"). |
| RF-017 | Actualización de Ubicación de Patrulla (App Patrulla) | La Aplicación Cliente debe enviar la ubicación actual de la patrulla al Servidor Central de Monitoreo cada 10 segundos para su registro y análisis de proximidad. |
| RF-018 | Interfaz de Usuario para Central de Monitoreo (Dashboard) | El Servidor Central de Monitoreo debe proporcionar una interfaz de usuario web (dashboard) para la visualización y gestión global de alertas y unidades por parte del personal de la central. |
| RF-019 | Autenticación de Patrullero | El sistema debe requerir que el patrullero inicie sesión en la aplicación móvil con credenciales |

| | | |
|---|---|---|
| | | válidas antes de acceder a las funcionalidades de gestión de alertas. |
| RF-020 | Autenticación para Dashboard | El sistema debe requerir que el operador y el administrador inicien sesión en la interfaz web (dashboard) para acceder a las funciones de monitoreo y administración. |
| RF-021 | Gestión de Usuarios y Roles | El administrador del sistema debe poder crear, editar, eliminar y asignar roles (patrullero, operador, administrador) a los usuarios del sistema. |
| RF-022 | Registro de Dispositivo y Víctima | El operador o el administrador deben poder registrar un nuevo dispositivo de alerta, asociándolo con el perfil de una víctima específica en la base de datos del sistema. |
| RF-023 | Actualización de Ubicación de Patrulla | La aplicación del patrullero debe enviar automáticamente la ubicación actual de la unidad al servidor central en intervalos regulares para su monitoreo y correlación con las alertas. |

| | | |
|---|---|---|
| RF-024 | Reenvío de Alerta del Servidor LoRaWAN | El Servidor LoRaWAN (The Thing Stack) debe estar configurado para reenviar los datos de alerta, de forma inmediata y automática, al Servidor Central de Monitoreo. |

## 5. Restricciones

- El sistema dependerá de la disponibilidad de la red LoRaWAN en las zonas de implementación; en áreas sin gateways activos, la cobertura será limitada.

- El alcance de las pruebas estará condicionado a la infraestructura tecnológica disponible durante la fase piloto (número de gateways, dispositivos y estaciones de monitoreo).

- La autonomía del dispositivo estará sujeta a las condiciones ambientales, frecuencia de transmisión y calidad del módulo de batería empleado.

- Las entidades receptoras de las alertas (PNP y PJ) deberán contar con dispositivos compatibles y conectividad mínima para recibir notificaciones en tiempo real.

- El proyecto se desarrollará dentro de los límites presupuestarios y temporales establecidos, priorizando el funcionamiento esencial del sistema antes que la escalabilidad masiva.

## 6. Supuestos

- Se asumirá que las instituciones de respuesta (PNP y PJ) mantendrán una coordinación operativa y tecnológica activa con el sistema de monitoreo central.

- Se prevé que el entorno de prueba cuente con cobertura LoRaWAN suficiente para validar la transmisión de datos.

- Los usuarios del dispositivo (víctimas con medidas de protección) recibirán capacitación básica sobre su uso y mantenimiento.

- Se espera la colaboración del MIMP o gobiernos locales para facilitar la integración del sistema en programas de prevención de violencia.

- El servidor central y la aplicación web estarán alojados en un entorno seguro con disponibilidad continua durante el periodo de evaluación.

## 7. Resultados esperados

- Implementación de un prototipo funcional de sistema de alerta basado en LoRaWAN, con integración entre dispositivo, servidor y plataforma web.

- Reducción del tiempo de respuesta ante alertas de emergencia en comparación con el sistema actual de botón de pánico.

- Mayor cobertura operativa en zonas rurales y periurbanas donde no existe señal celular estable.

- Optimización del consumo energético, logrando una autonomía superior respecto a los dispositivos móviles tradicionales.

- Validación de la arquitectura tecnológica y la comunicación LoRaWAN mediante pruebas en entorno controlado.

- Fortalecimiento de la seguridad ciudadana y mejora en la protección de mujeres y poblaciones vulnerables mediante una solución tecnológica confiable y sostenible.

## 8. Metodología de implementación

La metodología aplicada para el desarrollo del sistema de alerta personal se basa en el Rational Unified Process (RUP), un enfoque iterativo e incremental que permite gestionar de manera estructurada las distintas fases del ciclo de vida del software. RUP divide el proceso en cuatro etapas principales: inicio, elaboración, construcción y transición, asegurando una evolución controlada del sistema. En la fase de inicio se definieron los requerimientos y el alcance del proyecto; en la fase de elaboración se diseñó la arquitectura del sistema, considerando la integración entre el botón de pánico y la red LoRaWAN; durante la construcción se desarrollaron e implementaron los módulos de hardware y software; y finalmente, en la fase de transición se realizaron las pruebas, validaciones y ajustes necesarios para su despliegue. Esta metodología permitió garantizar la calidad del producto, la trazabilidad de los requerimientos y la reducción de riesgos técnicos y funcionales en el desarrollo del sistema.

## 9. Actores claves

- **Víctimas o usuarios finales:** Personas en situación de riesgo que utilizarán el botón de pánico para emitir alertas de emergencia de manera discreta y segura.

- **Centros de monitoreo o instituciones receptoras:** Entidades como la Policía Nacional del Perú (PNP) y el Poder Judicial (PJ), responsables de recibir, validar y atender las alertas generadas por el sistema.

- **Equipo de desarrollo tecnológico:** Ingenieros y técnicos encargados del diseño, implementación y mantenimiento del sistema de hardware y software, incluyendo la red LoRaWAN y la plataforma de gestión de alertas.

- **Administradores del sistema:** Personal encargado de supervisar el correcto funcionamiento del sistema, gestionar usuarios, mantener la base de datos y asegurar la disponibilidad del servicio.

## 10. Papel y responsabilidad del personal

| **ORGANIZACIÓN Y ROLES** | |
|---|---|
| **Integrante** | **Rol** |
| Fernandez Villanueva Daleska Nicolle | Diseño UX/UI y gráficos |
| Fernandez Villanueva Daleska Nicolle | Desarrollo Backend |
| Fernandez Villanueva Daleska Nicolle | Conecciones y manejo del The Think Stack |
| Fernandez Villanueva Daleska Nicolle | Desarrollo Frontend |
| Fernandez Villanueva Daleska Nicolle | Pruebas unitarias, de integración y QA |

## 11. Plan de monitoreo y evaluación

El plan de monitoreo y evaluación del Sistema de Alerta basado en tecnología LoRaWAN se centrará en garantizar su funcionamiento continuo, confiabilidad en la transmisión de alertas y eficiencia energética. Se establecerán métricas clave como el tiempo de respuesta del sistema (menos de 5 segundos por alerta), porcentaje de transmisión exitosa (mínimo 95%), y autonomía energética del dispositivo (mínimo 72 horas de operación continua). Además, se

realizará un monitoreo constante de la conectividad LoRaWAN y del rendimiento del servidor y la aplicación web. Se aplicarán pruebas unitarias, de integración y de campo, junto con auditorías de seguridad y revisiones mensuales para verificar la integridad de los datos y la correcta comunicación entre el hardware, el backend y la plataforma de monitoreo.

## 12. Cronograma del proyecto

| Actividad | Mes 1 | Mes 2 | Mes 3 | Mes 4 | Mes 5 | Mes 6 | Mes 7 | Mes 8 |
|---|---|---|---|---|---|---|---|---|
| **1. Análisis y Diseño (Iterativo)** | | | | | | | | |
| - Definición detallada de requisitos del SRS | | | | | | | | |
| - Diseño de arquitectura de hardware (esquemáticos, PCB) | | | | | | | | |
| - Diseño de arquitectura de software (firmware, backend, app cliente) | | | | | | | | |
| - Diseño de base de datos (Firestore) | | | | | | | | |
| - Plan de pruebas inicial | | | | | | | | |
| **2. Desarrollo de Firmware (Dispositivo Autónomo)** | | | | | | | | |
| - Configuración del entorno de desarrollo ESP-IDF | | | | | | | | |
| - Programación de gestión de energía (deep sleep) | | | | | | | | |
| - Implementación de captura GPS | | | | | | | | |
| - Implementación de comunicación LoRaWAN | | | | | | | | |
| - Programación del LED de | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| confirmación | | | | | | | | |
| - Pruebas unitarias y refactorización | | | | | | | | |
| **3. Desarrollo de Servidor Central (Backend y BD)** | | | | | | | | |
| - Configuración del entorno en la nube (AWS) | | | | | | | | |
| - Configuración de The Things Stack (integraciones Webhooks/MQTT) | | | | | | | | |
| - Implementación del backend (Python/Node.js) para recepción y procesamiento de alertas | | | | | | | | |
| - Implementación de lógica de correlación víctima/patrulla | | | | | | | | |
| - Configuración y modelado de datos en Firestore | | | | | | | | |
| **4. Desarrollo de Aplicación Cliente (Patrullas y Dashboard)** | | | | | | | | |
| - Diseño de UI/UX para la aplicación móvil/tablet y dashboard web | | | | | | | | |
| - Desarrollo de la aplicación móvil/tablet (visualización de mapa, perfil víctima, gestión de estado) | | | | | | | | |
| - Implementación de actualización de ubicación de patrullas (cada 5 seg) | | | | | | | | |
| - Desarrollo del dashboard web para la central | | | | | | | | |
| **5. Integración y Pruebas Continuas** | | | | | | | | |
| - Integración de todos los componentes (dispositivo, TTS, servidor, aplicaciones) | | | | | | | | |
| - Pruebas de | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| funcionamiento de extremo a extremo (latencia, fiabilidad) | | | | | | | | |
| - Pruebas de eficiencia energética del dispositivo | | | | | | | | |
| - Pruebas de carga y escalabilidad básicas | | | | | | | | |
| - Refactorización y corrección de errores en ciclos cortos | | | | | | | | |
| **6. Validación y Documentación Final** | | | | | | | | |
| - Pruebas de validación en entorno controlado (simulaciones de alerta) | | | | | | | | |
| - Recopilación y análisis de resultados | | | | | | | | |
| - Redacción de la tesis y documentación técnica final | | | | | | | | |
| - Presentación de resultados y defensa del proyecto | | | | | | | | |

## 2. Presupuesto

### 1. Presupuesto

| Categoría | Costos Total (S/) |
|---|---|
| Costos generales | 695.00 |
| Costos operativos | 320.00 |
| Costos del ambiente | 450.00 |
| Costos de personal | 12,000.00 |
| **Total** | 13,465.00 |

## 2. Análisis de factibilidad

El análisis de factibilidad del proyecto sistema alerta basado en tecnologia lorawan indica que es viable en términos técnicos, económicos, operativos, legales, sociales y ambientales.

- Factibilidad Operativa: El sistema es operativamente viable, ya que su uso es sencillo tanto para las víctimas como para el personal de seguridad. El botón de pánico permite activar la alerta sin conocimientos técnicos, mientras que la interfaz de monitoreo facilita la respuesta inmediata. El principal desafío será la capacitación del personal, pero se mitiga mediante manuales y entrenamientos adecuados.
- Factibilidad Legal: El proyecto es legalmente factible, siempre que se garantice el cumplimiento de las leyes de protección de datos personales y se obtenga el consentimiento informado de los usuarios. Se requerirán convenios con instituciones como la PNP o la municipalidad, aunque no existen restricciones legales sobre el uso de LoRaWAN para este propósito, lo que facilita su implementación.
- Factibilidad Social: La factibilidad social es muy alta, ya que el sistema atiende una necesidad urgente de protección frente a la violencia familiar. Promueve la seguridad ciudadana, mejora la confianza en las instituciones, optimiza la respuesta de emergencia y fomenta la inclusión tecnológica al ofrecer una herramienta accesible incluso para quienes no poseen un smartphone o conexión móvil.
- Factibilidad Ambiental: El proyecto es ambientalmente sostenible, dado que utiliza dispositivos de bajo consumo energético, baterías recargables y una infraestructura mínima. Además, favorece la reducción de residuos electrónicos mediante actualizaciones de firmware y mantenimiento responsable, alineándose con los principios de eficiencia y responsabilidad ecológica.

## 3. Evaluación financiera

De acuerdo a los resultados VAN, TIR, y B/C.

| | |
|---|---|
| **VAN** | S/ 1,125 |
| **TIR** | 12.5% |
| **B/C** | 1.57 |

Podemos concluir que el proyecto es rentable.

**Anexo 01 - FD01-EPIS-Informe de Factibilidad**

**Anexo 02 - FD02-EPIS-Informe Visión**

**Anexo 03- FD03-EPIS-Informe de Especificación de Requerimientos de Software**

**Anexo 04 - FD04-EPIS-Informe de Arquitectura de Software**