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

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

INTRODUCCIÓN

I. Generalidades de la Empresa

1. Nombre de la Empresa

El nombre de la empresa es DEVLEN

2. Visión

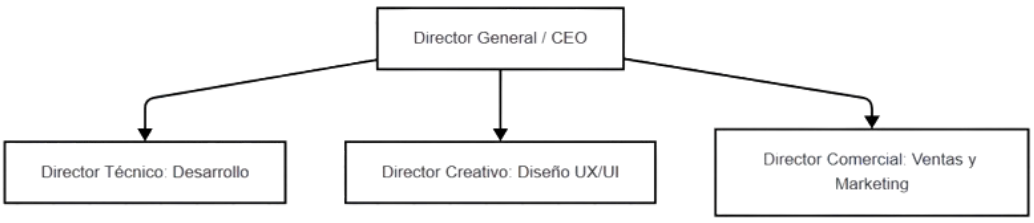
Ser una empresa líder en el desarrollo de soluciones tecnológicas innovadoras y automatizadas que impulsen la eficiencia, calidad y competitividad de empresas, estudiantes y profesionales del sector TI a nivel nacional y regional.

3. Misión

Diseñar y ofrecer productos tecnológicos que resuelvan problemas comunes en el desarrollo de software, automatización de procesos, gestión de datos y productividad digital, con foco en la simplicidad, eficiencia y accesibilidad.

4. Organigrama

A continuación se presenta un organigrama básico para la empresa DEVLEN, que puede adaptarse según el crecimiento y necesidades de la organización:



II. Visionamiento de la Empresa

1. Descripción 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 la provincia de Tacna.

2. Objetivos de Negocios

- **Reducir los Tiempos de Respuesta de Emergencia:** El sistema proporcionará a la Policía Nacional del Perú y al Serenazgo una herramienta de despacho automatizado y asistido por geoposicionamiento. Esto permitirá la optimización del uso de recursos, asegurando que la unidad más cercana y mejor capacitada sea asignada a la emergencia en cuestión de segundos, eliminando los retrasos inherentes a la comunicación verbal por radio y la interpretación manual de ubicaciones.

- **Aumentar la Confianza Ciudadana y la Percepción de Seguridad:** Al ofrecer un servicio de alerta que es percibido como confiable y de respuesta inmediata, el proyecto fortalecerá el vínculo entre las fuerzas del orden y la ciudadanía. Esto es crucial para las víctimas de violencia, quienes obtendrán una herramienta que les brinda la seguridad de que su llamado de auxilio será atendido de manera efectiva, lo que contribuye directamente a la prevención de daños mayores.

- **Mejorar la Eficiencia Operativa de las Unidades de Respuesta:** A diferencia de las soluciones dependientes de la infraestructura de telecomunicaciones comercial, el sistema con tecnología LoRaWAN asegura la funcionalidad en áreas con baja o nula cobertura celular. Esto representa una ventaja competitiva y un objetivo de negocio fundamental para las entidades públicas, ya que garantiza que el servicio de alerta de emergencia no se vea interrumpido en las situaciones más críticas, como en zonas rurales o dentro de estructuras cerradas.

3. Objetivos de Diseño

- Objetivo de Diseñar un dispositivo con una autonomía de batería que permita un funcionamiento continuo de al menos 6 meses en modo de reposo o que soporte un mínimo de 500 activaciones de emergencia.

- Reducir la latencia de transmisión de la alerta a un promedio de 5 segundos o menos, desde el momento en que se presiona el botón del dispositivo hasta que la alerta es registrada en el software de monitoreo de la central.

- Lograr un porcentaje de confiabilidad de transmisión superior al 98% en la provincia de Tacna, asegurando que la alerta llegue a la central de monitoreo en diversas condiciones de entorno (áreas con mala cobertura celular, dentro de edificios, etc.).

4. Alcance del proyecto

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.

5. Viabilidad del Sistema

El desarrollo e implementación del sistema de alerta personal con dispositivo autónomo y comunicación LoRaWAN es altamente viable y plenamente justificado. Técnicamente, el proyecto se sustenta en tecnologías maduras como LoRaWAN, ESP-IDF para el firmware optimizado, y plataformas robustas y gestionadas como The Things Stack y Firebase/Firestore, garantizando eficiencia, fiabilidad y capacidades en tiempo real que son esenciales para el sistema.

La solución propuesta es intuitiva para las personas vulnerables y representa una mejora sustancial en la eficiencia de las operaciones de las unidades de respuesta (PNP/Serenazgo), automatizando el despacho y proporcionando información crítica en tiempo real. Socialmente, el sistema aborda una necesidad urgente de seguridad, empoderando a las personas ulnerables y fortaleciendo la confianza en las instituciones. Esta convergencia de solidez tecnológica, eficiencia operativa y un impacto social positivo, valida la viabilidad y necesidad del sistema.

6. Información obtenida del Levantamiento de Información

La definición del presente sistema de alerta personal se ha fundamentado en un riguroso proceso de levantamiento de información, empleando diversas técnicas y fuentes para asegurar una comprensión integral del problema.

Principalmente, la información se obtuvo de las siguientes fuentes:

- **Análisis Documental y Comparativo de Sistemas Actuales:** Se realizó un estudio detallado del "Funcionamiento del Servicio Judicial de Alerta: Botón de Pánico" actualmente implementado. Este análisis permitió identificar las limitaciones inherentes a su dependencia de smartphones y redes de telecomunicaciones convencionales (cobertura, autonomía de batería, latencia de respuesta, necesidad de intervención humana), que el presente proyecto busca superar. Además, se revisaron documentos relacionados con

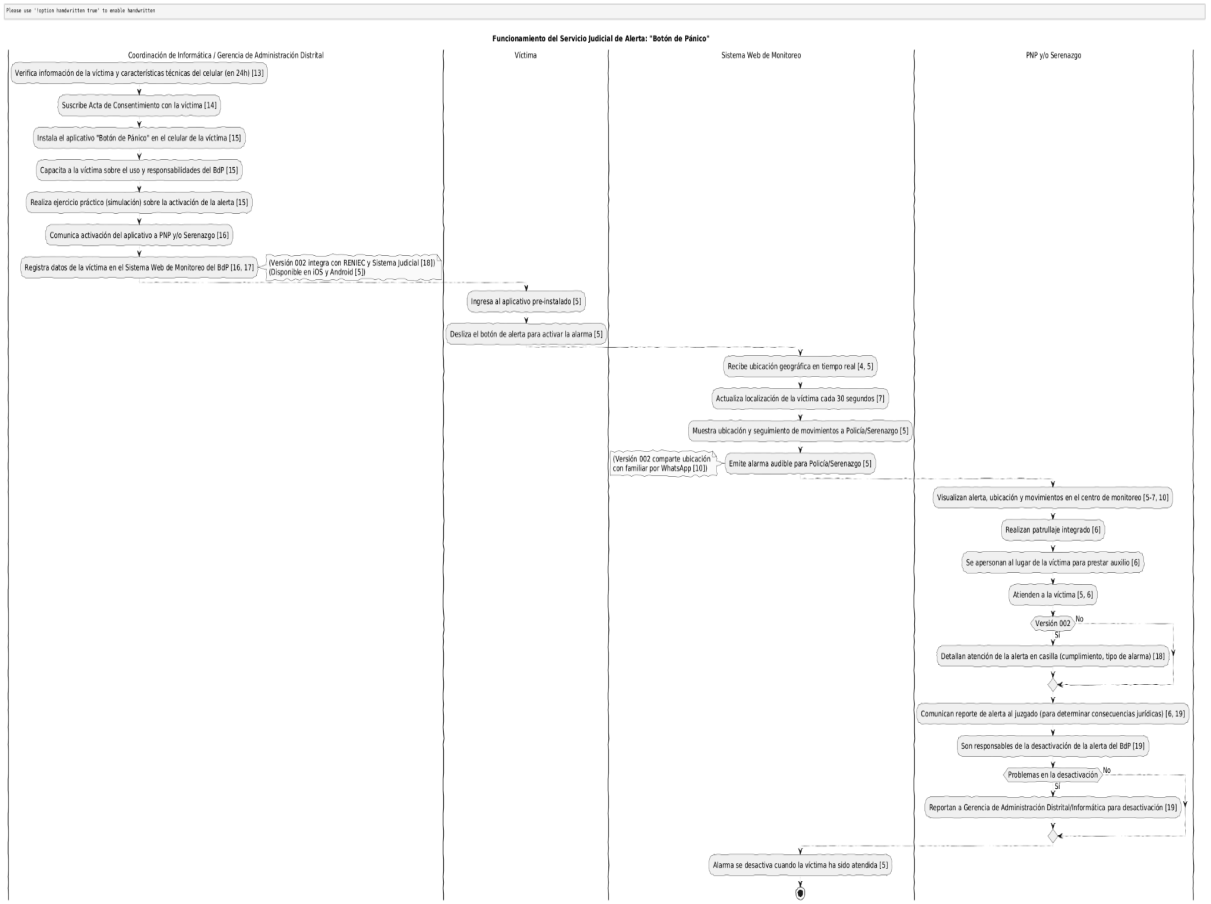
protocolos de seguridad ciudadana y marcos legales de protección a personas vulnerables en Perú, lo que proporcionó un contexto fundamental para los requisitos del sistema.

- **Investigación Tecnológica y Pruebas Preliminares:** Se llevó a cabo una investigación profunda sobre las capacidades de la tecnología LoRaWAN, incluyendo sus alcances de cobertura, eficiencia energética y mecanismos de transmisión de datos. Esto incluyó la evaluación de hardware (microcontroladores ESP32, módulos LoRa y GPS) y plataformas de software (ESP-IDF, The Things Stack, Firebase/Firestore, Google Maps API, frameworks de desarrollo web/móvil) para determinar su idoneidad técnica y viabilidad para los objetivos del proyecto.

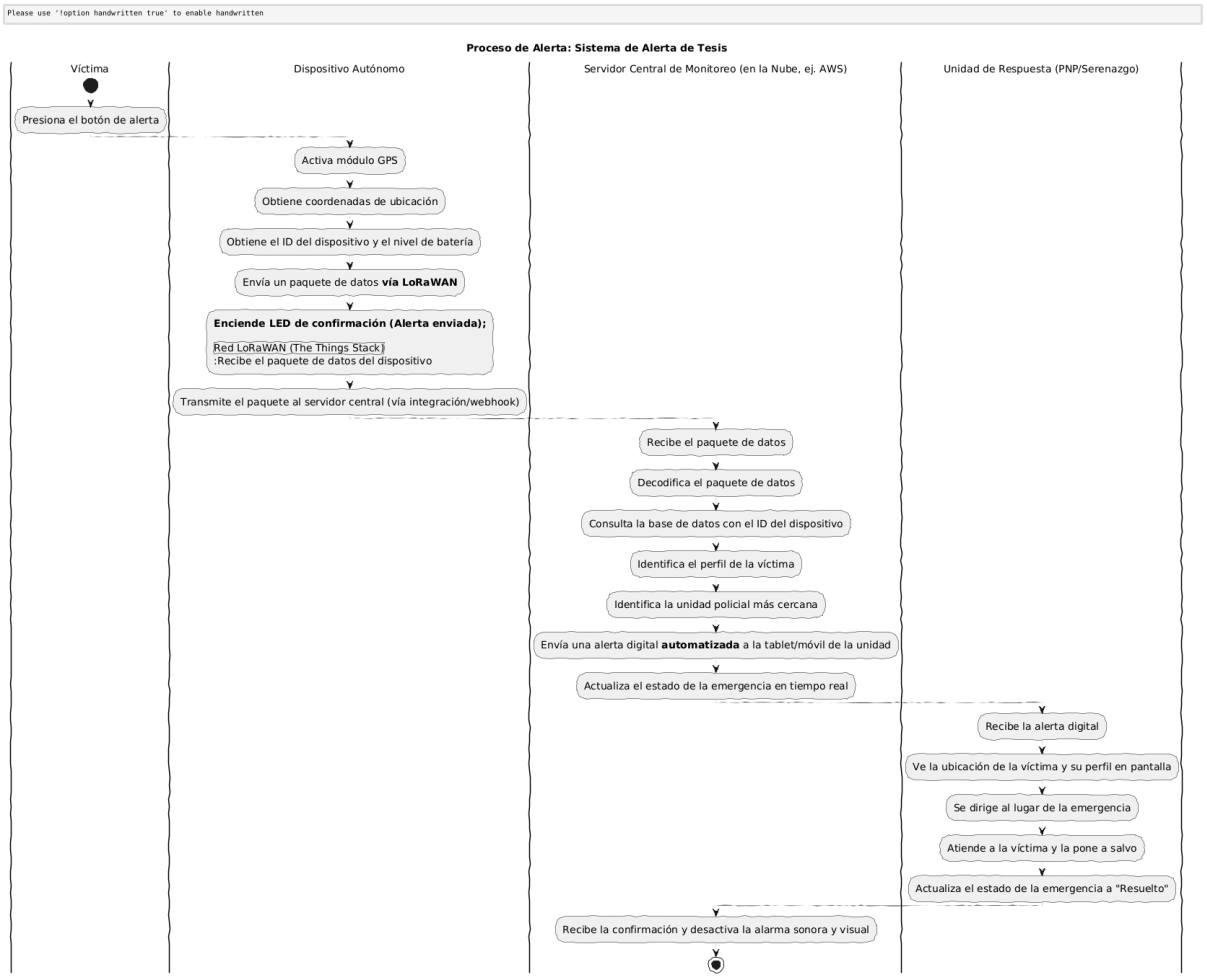
- **Identificación de Usuarios y Contexto Operativo:** Aunque no se realizaron entrevistas directas extensivas con víctimas debido a la naturaleza sensible del proyecto de tesis, se identificaron claramente los roles de los usuarios finales y las entidades operativas. Esto incluye a las personas vulnerables (quienes necesitan una activación sencilla y confiable), la Policía Nacional del Perú (PNP) y el Serenazgo (como unidades de respuesta en campo), y el personal de la central de monitoreo (quienes gestionan las alertas).

III. Análisis de Procesos

1. Diagrama del Proceso Actual – Diagrama de actividades



2. Diagrama del Proceso Propuesto – Diagrama de actividades Inicial



IV. Especificación de Requerimientos de Software

1. Cuadro de Requerimientos funcionales Inicial

ID	Nombre del Requerimiento	Descripción	Prioridad
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.	Alta

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.	Alta
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.	Alta
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).	Alta
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.	Alta
RF006	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.	Alta
RF007	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.	

RF008	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).	Alta

2. Cuadro de Requerimientos No funcionales

	ID	**Nombre del Requerimiento**	**Descripción**	**Prioridad**
Fiabilidad	RNF001	Disponibilidad del Sistema	El Servidor Central de Monitoreo, la base de datos Firestore y las integraciones con The Things Stack deben estar operativos y accesibles (24/7).	Alta
	RNF002	Resistencia a Fallos de Transmisión (Dispositivo)	El firmware del dispositivo autónomo debe implementar mecanismos, como por ejemplo: reintentos de envío para asegurar que, ante una pérdida momentánea de señal LoRaWAN, la alerta se transmite exitosamente tan pronto como la red esté disponible.	Alta
	RNF003	Tolerancia a Fallos de Componentes	El dispositivo debe estar diseñado con componentes robustos para resistir condiciones	Media

		(Dispositivo)	ambientales moderadas (temperatura, humedad) propias del uso diario en exteriores, sin que esto comprometa su funcionalidad principal.	
	RNF004	Manejo de Errores (Sistema)	El Servidor Central de Monitoreo y las aplicaciones cliente deben manejar de forma elegante y robusta los errores, por ejemplo: GPS no disponible, pérdida de conexión a Internet, datos inválidos.	Alta
Rendimiento	RNF005	Latencia de Alerta	El tiempo transcurrido desde la activación del botón en el dispositivo hasta la notificación de la alerta en la Aplicación Cliente del patrullero y en el Dashboard del operador no debe exceder los 15 segundos. Esto es crucial para la inmediatez de la respuesta.	Crítica
	RNF006	Frecuencia de Actualización de Ubicación de Patrullas	La Aplicación Cliente de los patrulleros debe actualizar su ubicación en la base de datos con una frecuencia de cada 10 segundos para permitir una identificación precisa de la unidad más cercana.	Alta
	RNF007	Capacidad de Procesamiento	El Servidor Central de Monitoreo debe ser capaz de procesar y despachar simultáneamente al	Media

			menos 10 alertas por minuto sin degradación significativa del rendimiento. (Este valor puede ajustarse en base a la expectativa de incidentes).	
Usabilidad	RNF008	Simplicidad de Activación (Dispositivo)	La activación de la alerta en el dispositivo autónomo debe realizarse mediante una única acción de pulsar un botón, sin requerir secuencias complejas, pantallas o habilidades técnicas previas por parte del usuario vulnerable.	Crítica
	RNF009	Claridad de Interfaz (Aplicaciones)	La Aplicación Cliente del patrullero y el Dashboard de la Central deben presentar la información de manera clara, concisa e intuitiva, con elementos visuales fáciles de interpretar (mapas, iconos, estados de alerta).	Alta
	RNF010	Operación Táctil Intuitiva (Aplicaciones)	La Aplicación Cliente debe ser totalmente funcional y fácil de operar mediante gestos táctiles en dispositivos móviles, incluso en condiciones de estrés.	Alta
	RNF011	Autenticación de Dispositivos	Cada dispositivo autónomo debe autenticarse de forma segura en la red LoRaWAN (TTS) utilizando credenciales únicas (DevEUI, AppKey, NwkKey) para asegurar	Alta

			que solo dispositivos autorizados puedan transmitir alertas.	
Seguridad	RNF012	Acceso Controlado a la Información	El Servidor Central de Monitoreo (SCM) y las aplicaciones deben implementar un sistema de autenticación y autorización basado en roles, como: patrullero, operador, para asegurar que solo el personal autorizado acceda a la información pertinente (perfiles de víctimas, ubicación de patrullas, gestión de alertas).	Alta
	RNF013	Comunicación Segura	Todas las comunicaciones entre los componentes del sistema (TTS a SCM, SCM a Aplicaciones Cliente) deben realizarse a través de canales seguros, como: HTTPS, MQTT sobre TL para proteger la integridad y confidencialidad de los datos transmitidos.	Alta
Mantenibilidad y	RNF014	Autonomía del Dispositivo	El dispositivo autónomo debe tener una autonomía de batería de al menos 6 meses aproximadamente en modo de reposo o soportar un mínimo de 100 activaciones de emergencia, para reducir la frecuencia de recarga y asegurar su disponibilidad a largo plazo.	Crítica

Escalabilidad	RNF015	Modularidad y Claridad del Código	El código fuente del firmware (ESP-IDF), el backend (Python/Node.js) y las aplicaciones cliente debe estar bien estructurado, modularizado y documentado para facilitar su futura modificación, mantenimiento y extensión.	Media

3. Cuadro de Requerimientos funcionales Final

ID	Nombre del Requisito	Descripción de Requisito	Prioridad
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.	Alta
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.	Alta
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	Alta

		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).	Alta
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.	Alta
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.	Alta
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.	Alta
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.	Alta

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.	Alta
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.	Alta
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.	Media
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.	Alta
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.	Alta

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).	Alta
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.	Media
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").	Alta
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.	Alta
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.	Alta
RF-019	Autenticación de Patrullero	El sistema debe requerir que el patrullero inicie sesión en la aplicación móvil con	Alta

		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.	Alta
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.	Alta
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.	Alta
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.	Alta
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.	Alta

4. Reglas de Negocio

La funcionalidad principal de este sistema de alerta personal se centra en la automatización completa y la fiabilidad de la respuesta de emergencia. El dispositivo autónomo operará con una gestión de energía optimizada, activando su GPS bajo demanda y transmitiendo su ID único, ubicación precisa y nivel de batería vía LoRaWAN, con una confirmación visual. Toda la cadena, desde la recepción del paquete LoRaWAN por The Things Stack hasta su reenvío en tiempo real al Servidor Central de Monitoreo, está diseñada para ser automática y sin intervención manual, asegurando la inmediatez en el flujo de información de alerta.

Una regla fundamental para garantizar la seguridad e integridad de los datos y la efectividad de la respuesta es la correlación automática del ID del dispositivo con el perfil de la víctima en Firestore. El Servidor Central identificará de forma automática la unidad de respuesta más cercana y despachará la alerta digital a su aplicación móvil/tablet dedicada, la cual actualizará la ubicación de la patrulla cada 5 segundos en tiempo real. Esto asegura que el personal de seguridad siempre cuente con la información más reciente y precisa para actuar, mientras que el sistema gestiona los estados de la alerta de manera fluida y persistente, manteniendo la transparencia y la trazabilidad de cada incidente.

V. Fase de Desarrollo

1. Perfiles de Usuario

Persona Vulnerable (Usuario Final del Dispositivo): Este perfil corresponde al individuo que se encuentra en situación de riesgo y es el portador directo del dispositivo autónomo de alerta. Su interacción con el sistema se limita a la activación de la alerta en momentos de peligro. Sus necesidades se centran en la simplicidad, discreción y alta fiabilidad del dispositivo. Requiere una operación instintiva con una única pulsación, sin necesidad de interactuar con pantallas o interfaces complejas, y con una confirmación clara de envío.

Patrullero (Usuario de la Aplicación Cliente en Campo): Este perfil representa al personal de la Policía Nacional del Perú (PNP) o del Serenazgo que opera en las unidades de respuesta en campo. Su principal interacción es a través de la aplicación móvil dedicada, la cual será su herramienta esencial para la gestión de

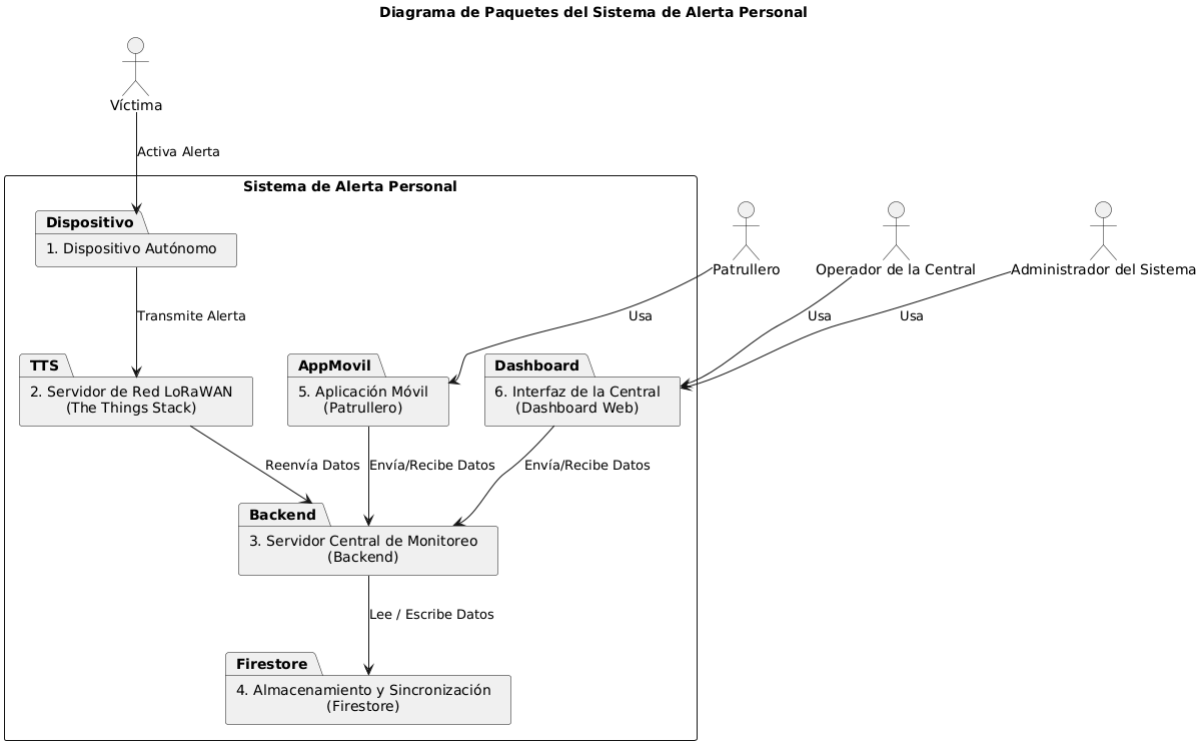
emergencias. Sus necesidades clave incluyen la recepción inmediata de alertas, la visualización clara y en tiempo real de la ubicación exacta de la víctima en un mapa, el acceso rápido al perfil de la víctima, y la capacidad de actualizar el estado de la emergencia de forma sencilla. Requieren una interfaz ágil, con notificaciones confiables y que les permita registrar su propia ubicación de manera constante para el despacho automatizado.

Operador de la Central de Monitoreo (Usuario del Dashboard Web): Este perfil corresponde al personal encargado de supervisar y coordinar las emergencias desde la central. Su interacción se realiza a través del dashboard web del Servidor Central de Monitoreo. Sus necesidades se enfocan en tener una visión global y en tiempo real de todas las alertas activas, la ubicación de todas las unidades de respuesta, y el estado de cada incidente. Requieren una interfaz clara para la gestión y seguimiento de las alertas, capacidad para visualizar detalles de las víctimas, y herramientas para coordinar recursos si fuera necesario, basándose en la información actualizada en Firestore.

Administrador del Sistema (Gestión de Datos y Configuración); Este perfil, generalmente un técnico o responsable de seguridad de la institución, se encarga de la configuración inicial del sistema y el mantenimiento de los datos maestros. Sus actividades incluyen el registro y la asociación de los IDs de los dispositivos autónomos con los perfiles de las personas vulnerables, la gestión de las cuentas de los patrulleros y operadores, y la supervisión del estado general del sistema. Sus necesidades se centran en tener herramientas intuitivas para la administración de usuarios y dispositivos, y para asegurar la integridad y seguridad de la información almacenada en Firestore.

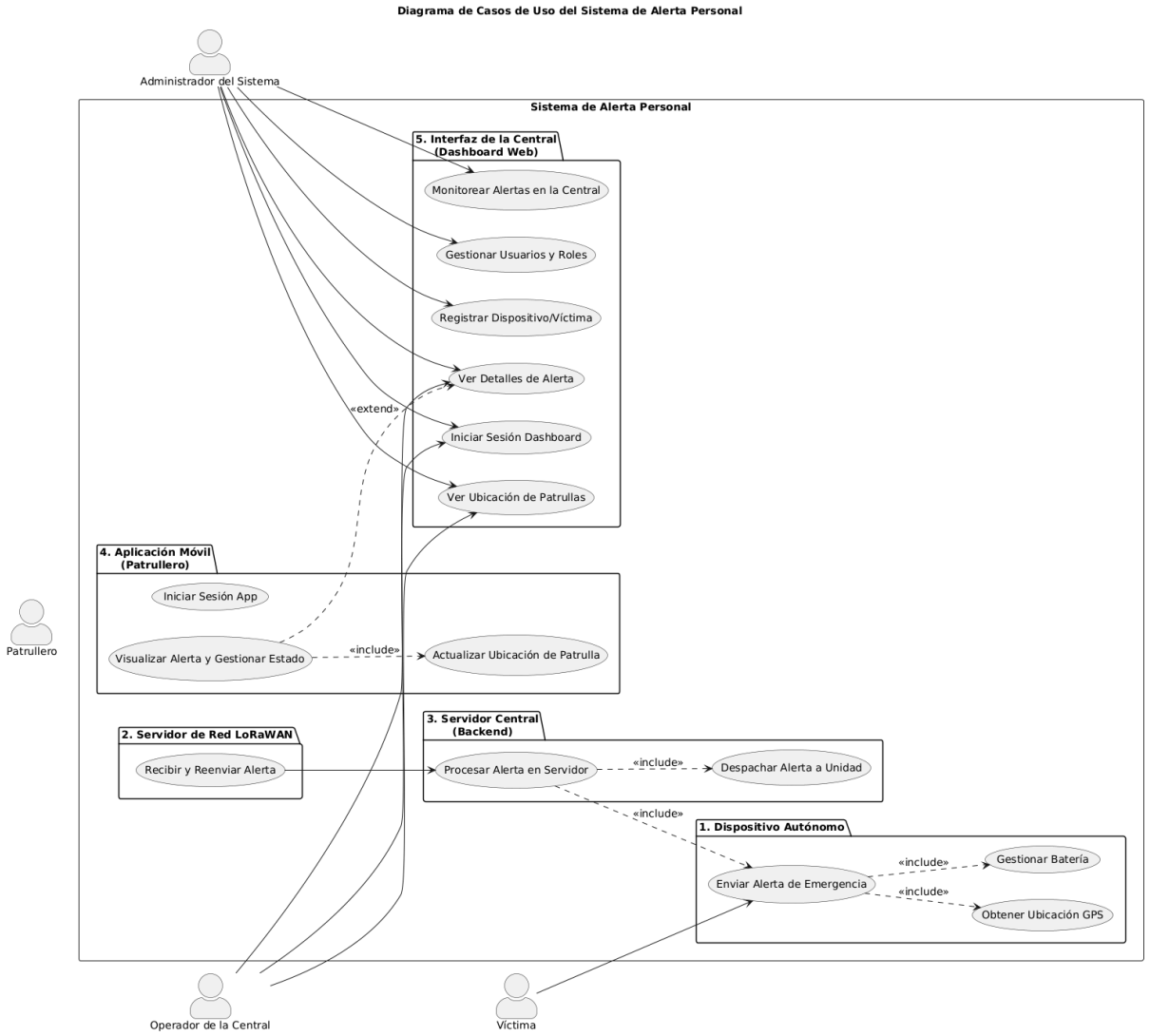
2. Modelo Conceptual

   a. Diagrama de Paquetes



https://drive.google.com/file/d/1WlPatHQCFipPHUgErLxDde5q0Vqii72j/view?usp=sharing

b. Diagrama de Casos de Uso



https://drive.google.com/file/d/1wRhitCffQwXFgBCiw5y32uQml-79trWV/view?usp=sharing

c. Escenarios de Caso de Uso (narrativa)

Caso de uso	CUS001 - Activar Alerta de Emergencia
Actores	Persona vulnerable
Propósito	Permitir a una persona en situación de riesgo activar de manera rápida y discreta una alerta de emergencia, garantizando que su ubicación y estado sean comunicados al sistema central.
Tipo	Principal
Descripción	La persona vulnerable activa su dispositivo. Este activa su módulo GPS para obtener coordenadas, compila un paquete de datos con su identificador único y el nivel de batería, y lo transmite de forma segura a través de la red LoRaWAN. Una confirmación visual mediante un LED indica el éxito de la transmisión.
Precondición	● La Víctima posee un dispositivo de alerta funcional y registrado. ● El dispositivo tiene batería suficiente y está dentro del rango de cobertura LoRaWAN.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema (Dispositivo)**

1. **Acción del Actor:** La Víctima presiona y mantiene presionado el botón físico del dispositivo por 3 segundos para evitar activaciones accidentales.	2. **Acción del Sistema (Dispositivo):** El microcontrolador del dispositivo detecta la pulsación y verifica la duración. 3. El firmware del dispositivo activa el módulo GPS para iniciar el proceso de adquisición de coordenadas. 4. El sistema verifica el nivel de batería para incluirlo en el paquete de datos. 5. El firmware compila el paquete de datos de alerta, que incluye el ID único del dispositivo (DevEUI), las coordenadas GPS obtenidas y el nivel de batería actual. 6. El módulo LoRaWAN del dispositivo establece comunicación con el gateway LoRaWAN más cercano y transmite el paquete de datos. 7. El dispositivo espera una confirmación de la transmisión desde el gateway. 8. Una vez recibida la confirmación, el firmware activa el LED de confirmación por un breve periodo. 9. El firmware desactiva el módulo GPS y entra en modo de bajo consumo para conservar energía.

Caso de uso	CUS002 - Obtener Ubicación GPS
Actores	Dispositivo
Propósito	Adquirir las coordenadas geográficas precisas de la Víctima en el momento de la alerta.
Tipo	Incluido
Descripción	Este caso de uso es activado automáticamente cuando la Víctima presiona el botón de pánico. El dispositivo activa su módulo GPS para obtener la latitud y longitud, un dato crítico para la respuesta de emergencia.
Precondición	● El caso de uso (Enviar Alerta de Emergencia) se ha iniciado.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema (Dispositivo)**
	1. **Acción del Sistema:** El firmware del dispositivo activa el módulo GPS. 2. El módulo GPS comienza a buscar satélites y triangula la posición geográfica. 3. El firmware monitorea la adquisición de una posición válida. 4. Una vez que se obtienen las coordenadas precisas, estas se pasan

	al caso de uso (Enviar Alerta de Emergencia) para ser incluidas en el paquete de datos. 5. Si el GPS no obtiene una posición en un tiempo predefinido (ej., 30 segundos), el sistema utiliza la última posición conocida y marca los datos como "aproximados".

Caso de uso	CUS003 - Gestionar Batería
Actores	Dispositivo
Propósito	Monitorear el nivel de batería del dispositivo para asegurar su operatividad y reportar su estado junto con la alerta.
Tipo	Incluido
Descripción	Este caso de uso es activado cuando la Víctima genera una alerta. El dispositivo verifica su nivel de batería y lo añade al paquete de datos que será transmitido, permitiendo al sistema central conocer el estado de carga del dispositivo de forma remota.
Precondición	El caso de uso (Enviar Alerta de Emergencia) se ha iniciado.

Curso normal de eventos	
Acciones de actores	**Acciones del sistema (Dispositivo)**
	1. **Acción del Sistema:** El microcontrolador del dispositivo lee el voltaje de la batería a través de un pin analógico. 2. El firmware calibra la lectura del voltaje para determinar el porcentaje de carga actual. 3. El nivel de batería, como un valor porcentual, se incluye en el paquete de datos de la alerta. 4. El sistema en el servidor central recibe la información y, si el nivel es crítico, puede generar una alerta para que el Administrador notifique a la Víctima.

Caso de uso	CUS004 - Recibir y Reenviar Alerta
Actores	Servidor LoRaWAN
Propósito	Procesar la alerta de baja potencia enviada desde el dispositivo y reenviarla al Servidor Central del sistema para su gestión.
Tipo	Secundario

Descripción	Este caso de uso describe cómo el Servidor LoRaWAN (The Thing Stack) recibe la alerta transmitida desde el dispositivo, la desencripta, valida la integridad de los datos y la reenvía al Servidor Central del sistema para su procesamiento y gestión.
Precondición	El dispositivo ha transmitido con éxito una alerta a través de LoRaWAN. El paquete de datos ha llegado al gateway LoRaWAN.
Curso normal de eventos	
Acciones de actores	**Acciones del app móvil**
1. **Acción del Actor:** El Servidor LoRaWAN (The Things Stack) recibe el paquete de datos LoRaWAN del gateway.	2. **Acción del Sistema:** El servidor LoRaWAN desduplica el paquete de datos (si múltiples gateways lo recibieron). 3. Desencripta la carga útil utilizando la clave de sesión de la aplicación configurada. 4. Verifica la integridad de los datos (ID del dispositivo, coordenadas GPS, nivel de batería, etc.). 5. Si la carga útil es válida, el servidor LoRaWAN reenvía los datos procesados en formato JSON al Servidor Central del sistema usando Webhook o MQTT. 6. El sistema central recibe los datos y los procesa según el flujo establecido (ej.

	crear una alerta en la base de datos).

Caso de uso	CUS005 - Procesar Alerta en Servidor
Actores	El Sistema (Backend)
Propósito	Centralizar la recepción, procesamiento y despacho de alertas.
Tipo	Principal
Descripción	El Servidor Central de Monitoreo (Backend) recibe los datos reenviados por el Servidor LoRaWAN, los decodifica, los asocia a una víctima, identifica la patrulla más cercana, guarda la alerta en la base de datos y la despacha.
Precondición	El Servidor LoRaWAN ha reenviado los datos de alerta al Servidor Central.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema (app)**
	1. **Acción del Sistema:** El Servidor Central recibe el POST request del Webhook de TTS. 2. El Backend decodifica la carga útil del mensaje (payload) y valida que

	contenga los campos requeridos (ID, coordenadas, batería). 3. El Backend consulta la base de datos para correlacionar el ID del dispositivo con el perfil de la Víctima. 4. Simultáneamente, el Backend obtiene las ubicaciones en tiempo real de todas las patrullas activas desde la base de datos. 5. El Backend ejecuta un algoritmo de proximidad para identificar la patrulla más cercana a la ubicación de la alerta. 6. El Backend genera un nuevo registro de alerta en la base de datos, incluyendo la información de la Víctima, la ubicación, la patrulla asignada, la hora y el estado inicial ("Despachada"). 7. La creación del registro en la base de datos activa el caso de uso (Despachar Alerta a Unidad).

Caso de uso	CUS006 - Despachar Alerta a Unidad
Actores	El Sistema (Backend)
Propósito	Enviar una notificación a la patrulla asignada y al dashboard del Operador en tiempo real.
Tipo	Incluido

Descripción	Este caso de uso es activado por el Servidor Central una vez que ha procesado la alerta. El sistema genera y envía una notificación a la aplicación móvil del Patrullero asignado y actualiza el dashboard del Operador.
Precondición	El caso de uso (Procesar Alerta en Servidor) se ha completado.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema**
	1. **Acción del Sistema:** El Backend identifica la patrulla asignada a la alerta. 2. El sistema prepara una notificación con un resumen de la alerta (ID, ubicación, nombre de la víctima). 3. El sistema envía la notificación a la Aplicación Móvil de esa Patrulla. 4. El sistema actualiza el dashboard del Operador con la nueva alerta y la asignación, mostrando un aviso visual o sonoro. 5. El Patrullero y el Operador reciben la alerta en sus respectivas interfaces en un plazo de 5 segundos.

Caso de uso	CUS007 - Iniciar Sesión App
Actores	Patrullero

Propósito	Autenticar al Patrullero para que pueda acceder a las funciones de la aplicación móvil de monitoreo y respuesta.
Tipo	Principal
Descripción	El Patrullero ingresa su usuario y contraseña en la aplicación. El sistema valida las credenciales y, si son correctas, le otorga acceso a la interfaz principal de la aplicación.
Precondición	El Patrullero tiene una cuenta de usuario válida. El dispositivo móvil del Patrullero tiene conexión a internet.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema (app)**
1. **Acción del Actor:** El Patrullero abre la aplicación e ingresa su nombre de usuario y contraseña en los campos correspondientes.	2. **Acción del Sistema:** La aplicación móvil envía la solicitud de autenticación al Backend a través de un canal seguro (ej., HTTPS). 3. El Backend valida las credenciales contra la base de datos de usuarios. 4. Si las credenciales son correctas, el Backend devuelve un token de sesión. 5. La aplicación móvil guarda el token y redirige al Patrullero a la pantalla principal de alertas. 6. Si las credenciales son incorrectas, la aplicación muestra un mensaje de error

	y el Patrullero debe reintentar.

Caso de uso	CUS008 - Visualizar Alerta y Gestionar Estado
Actores	Patrullero
Propósito	Permitir al Patrullero ser notificado de una nueva alerta, ver la información crítica y actualizar el estado de la emergencia para coordinar la respuesta.
Tipo	Principal
Descripción	La aplicación móvil del Patrullero recibe una notificación de una alerta asignada. El Patrullero puede ver la ubicación de la víctima en un mapa, acceder a sus detalles y cambiar el estado de la alerta.
Precondición	El Patrullero ha iniciado sesión en la aplicación móvil. Una alerta ha sido despachada a su unidad.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema (app)**
	1. **Acción del Sistema:** La aplicación móvil del Patrullero recibe la

	notificación.
2. **Acción del Actor:** El Patrullero abre la aplicación, que lo dirige a la vista de la alerta.	3. **Acción del Sistema:** La aplicación carga la interfaz de la alerta, mostrando la ubicación de la víctima en un mapa dinámico y un panel con datos resumidos. 4. El sistema en segundo plano sigue ejecutando el caso de uso (Actualizar Ubicación de Patrulla). 5. El Patrullero puede ejecutar el caso de uso (Ver Detalles de Alerta) para ver el perfil completo de la víctima.
6. **Acción del Actor:** El Patrullero interactúa con la interfaz para seleccionar un nuevo estado (ej., "En Ruta").	7. **Acción del Sistema:** La aplicación envía la actualización del estado al Servidor Central. El Backend modifica el estado de la alerta en la base de datos, lo que se refleja en tiempo real en el dashboard del Operador.

Caso de uso	CUS009 - Actualizar Ubicación de Patrulla
Actores	El Sistema (Aplicación Móvil del Patrullero)
Propósito	Enviar periódicamente la ubicación de la patrulla al Servidor Central para el rastreo en tiempo real.
Tipo	Incluido
Descripción	Mientras el Patrullero está "en servicio", la

	aplicación móvil utiliza el GPS del dispositivo para obtener su ubicación y la envía de forma recurrente al Servidor Central.
Precondición	El Patrullero ha iniciado sesión en la aplicación y ha concedido los permisos de ubicación.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema (app)**
	1. **Acción del Sistema:** La aplicación móvil, al estar en primer plano o en modo de servicio, activa el GPS del dispositivo. 2. La aplicación obtiene la ubicación geográfica actual (latitud, longitud). 3. Cada 5 segundos, la aplicación construye un paquete de datos con la ubicación y el ID de la Patrulla y lo envía al Backend. 4. El Backend recibe la ubicación y la actualiza en tiempo real en la base de datos para esa Patrulla específica. 5. La nueva ubicación se sincroniza y es visible inmediatamente en el dashboard del Operador y en los mapas de otras patrullas.

Caso de uso	CUS010 - Iniciar Sesión Dashboard
Actores	Operador de la Central, Administrador del

	Sistema
Propósito	Autenticar y autorizar a un usuario para que acceda a las funciones del dashboard web.
Tipo	Principal
Descripción	El Operador o Administrador ingresa sus credenciales en el formulario de inicio de sesión del dashboard web. El sistema valida las credenciales y, si son correctas, le otorga acceso a la interfaz principal del dashboard.
Precondición	● El usuario tiene una cuenta de usuario válida. ● El dashboard tiene conexión a internet.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema ()**
1. **Acción del Actor:** El usuario ingresa su usuario y contraseña en la página de inicio de sesión del dashboard.	2. **Acción del Sistema:** El dashboard envía la solicitud de autenticación al Backend. 3. El Backend valida las credenciales contra la base de datos de usuarios. 4. Si las credenciales son correctas, el Backend devuelve un token de sesión seguro. 5. El dashboard guarda el token y redirige al usuario a la interfaz principal de su rol. 6. Si las credenciales son incorrectas, el

	dashboard muestra un mensaje de error.

Caso de uso	CUS011 - Monitorear Alertas en la Central
Actores	Operador de la Central
Propósito	Proporcionar al Operador una visión general y en tiempo real de todas las alertas activas y la ubicación de las patrullas.
Tipo	Principal
Descripción	El Operador accede a un dashboard web que funciona como centro de mando. Este dashboard muestra un mapa interactivo con las ubicaciones de todas las alertas activas y de las patrullas en servicio, permitiendo una coordinación eficiente de los recursos.
Precondición	• El Operador ha iniciado sesión exitosamente en el dashboard.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema**
1. **Acción del Actor:** El Operador Central inicia	2. **Acción del Sistema:** El dashboard carga la interfaz principal, mostrando

sesión en el dashboard.	un mapa interactivo y un panel con el listado de alertas activas. 3. El backend establece una conexión en tiempo real con la base de datos para recibir actualizaciones sobre alertas y ubicaciones de patrullas. 4. El dashboard muestra en el mapa las ubicaciones de todas las alertas activas y las posiciones actualizadas en tiempo real de las patrullas. 5. El dashboard muestra notificaciones visuales y/o sonoras cuando llega una nueva alerta
6. **Acción del Actor:** El Operador revisa el listado de alertas, filtrando o priorizando según sea necesario. 7. El Operador puede seleccionar una alerta en el mapa o en el listado para ver sus detalles (ejecutando el caso de uso (Ver Detalles de Alerta).	8. **Acción del Sistema:** El backend mantiene toda la información actualizada en tiempo real a través de la base de datos.

Caso de uso	CUS012 - Ver Ubicación de Patrullas
Actores	Operador de la Central

Propósito	Proveer al Operador una visualización en tiempo real de la ubicación de todas las unidades de respuesta en servicio.
Tipo	Incluido
Descripción	Este caso de uso es parte de la funcionalidad de (Monitorear Alertas en la Central). El dashboard del Operador muestra un mapa con la ubicación actualizada de todas las patrullas activas.
Precondición	● El Operador está monitoreando el sistema. ● Las Patrullas están en servicio y enviando su ubicación.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema**
	1. **Acción del Sistema:** El dashboard del Operador, como parte de la interfaz principal, muestra un mapa interactivo. 2. El Backend consulta la base de datos para obtener las últimas ubicaciones reportadas por todas las patrullas. 3. En el mapa, se visualizan marcadores o íconos que representan la ubicación en tiempo real de cada patrulla en servicio. 4. La ubicación de las patrullas se actualiza constantemente en el mapa a

	medida que las patrullas envían sus datos al sistema.

Caso de uso	CUS013 - Ver Detalles de Alerta
Actores	Patrullero, Operador de la Central
Propósito	Proporcionar acceso rápido y seguro a la información relevante del perfil de la Persona Vulnerable asociada a una alerta.
Tipo	Incluido / Extendido
Descripción	El Patrullero o el Operador pueden seleccionar una alerta activa o una víctima para acceder a su perfil completo. Este perfil contiene datos de contacto, historial de alertas previas y cualquier otra información vital para una intervención efectiva y segura.
Precondición	El Patrullero o el Operador ha iniciado sesión. Hay una alerta activa o una Persona Vulnerable registrada en el sistema.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema ()**

1. **Acción del Actor:** El usuario selecciona una alerta de la lista o hace clic en un marcador en el mapa.	2. **Acción del Sistema:** La interfaz envía una solicitud segura al Backend, solicitando el perfil de la Víctima asociado con la alerta seleccionada. 3. El Backend consulta la base de datos, utilizando el ID del dispositivo (si es desde una alerta) o el ID de la persona vulnerable para recuperar su perfil completo. 4. El Backend aplica las reglas de autorización basadas en el rol del usuario y envía la información del perfil de la Víctima de vuelta a la interfaz. 5. La interfaz (aplicación o dashboard) muestra la información detallada del perfil de la Persona Vulnerable en una ventana emergente o en una vista separada.

Caso de uso	CUS014 - Gestionar Usuarios y Roles
Actores	Administrador del Sistema
Propósito	Permitir al Administrador gestionar de forma segura los usuarios que tienen acceso al sistema, incluyendo sus roles, permisos y credenciales.
Tipo	Principal

Descripción	El Administrador utiliza una interfaz dedicada en el dashboard web para realizar tareas de gestión de usuarios. Esto incluye crear nuevas cuentas, modificar sus roles y permisos, o, en caso de ser necesario, desactivar cuentas de Patrulleros y Operadores.
Precondición	El Administrador ha iniciado sesión en el dashboard.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema**
1. **Acción del Actor:** El Administrador navega a la sección de "Gestión de Usuarios".	2. **Acción del Sistema:** El dashboard carga la interfaz de gestión, mostrando una lista de todos los usuarios registrados, sus roles y estados.
3. Acción del Actor: El Administrador selecciona una acción (ej., "Crear Nuevo Usuario", "Editar Usuario" o "Desactivar Cuenta").	**4. Acción del Sistema:** El sistema muestra un formulario o una ventana de confirmación.
5. Acción del Actor: El Administrador completa los datos del formulario (ej., nombre, rol, contraseña) y lo envía.	**6. Acción del Sistema:** El sistema valida los datos y realiza la acción correspondiente en la base de datos (crea un nuevo registro, actualiza un rol o marca una cuenta como inactiva). 7. El sistema muestra una confirmación visual de que la acción se ha

	completado con éxito.

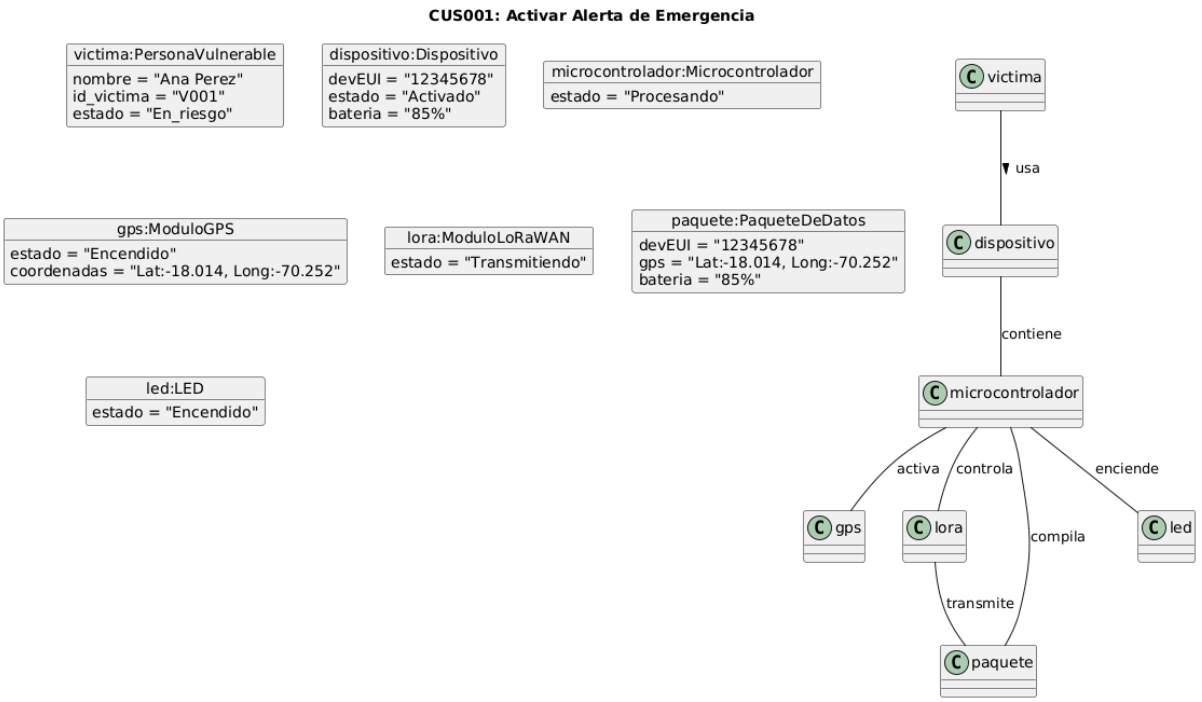
Caso de uso	CUS015 - Registrar Dispositivo/Víctima
Actores	Administrador del Sistema
Propósito	Permitir al Administrador del Sistema registrar y vincular un nuevo dispositivo autónomo con el perfil de una persona vulnerable.
Tipo	Principal
Descripción	El Administrador utiliza el dashboard web para registrar un nuevo dispositivo de alerta. En este proceso, asocia el ID único del dispositivo (DevEUI) con el perfil de la persona vulnerable que lo utilizará, asegurando que el sistema pueda identificar instantáneamente a la víctima cuando se active una alerta.
Precondición	El Administrador ha iniciado sesión en el dashboard. Se tiene acceso al ID único (DevEUI) del nuevo dispositivo.
Curso normal de eventos	
Acciones de actores	**Acciones del sistema ()**

1. **Acción del Actor:** El Administrador navega a la sección de "Registro de Dispositivo/Víctima".	2. **Acción del Sistema:** El dashboard muestra un formulario de registro.
3. **Acción del Actor:** El Administrador ingresa el ID único del dispositivo, el nombre de la víctima, información de contacto, y cualquier otra información relevante.	4. **Acción del Sistema:** El sistema valida que el ID del dispositivo no esté ya en uso y que los datos de la víctima sean válidos. 5. El sistema crea un nuevo registro en la base de datos, que incluye el perfil de la Víctima y la vinculación con el ID del dispositivo. 6. El sistema muestra una confirmación visual de que el dispositivo ha sido registrado y asociado con éxito.

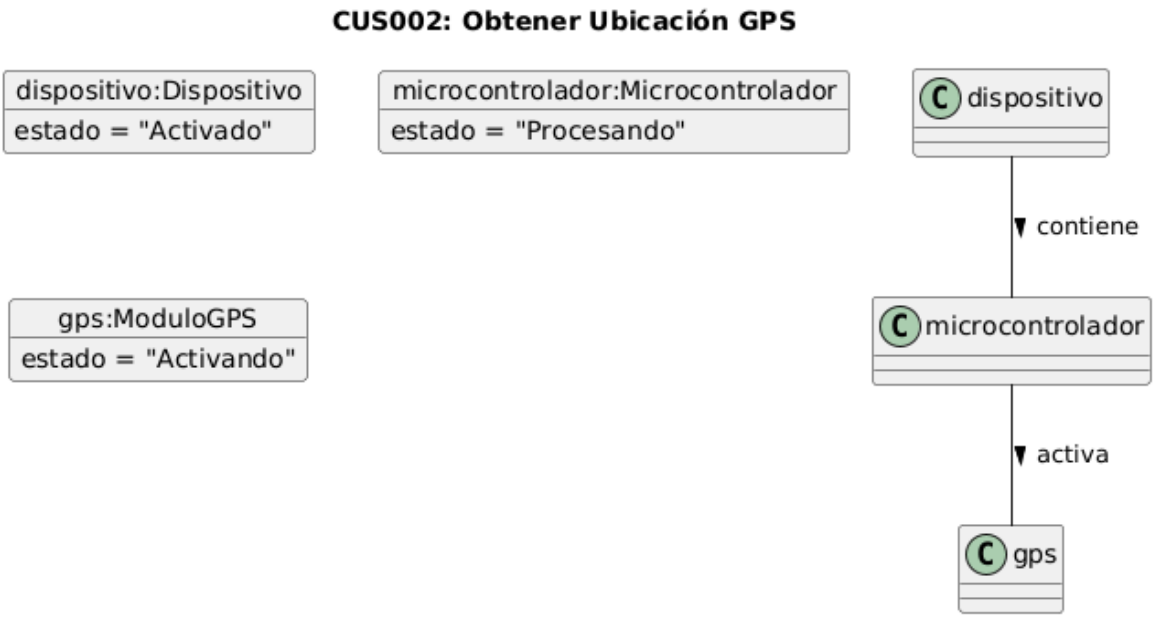
3. Modelo Lógico

   a. Analisis de Objetos

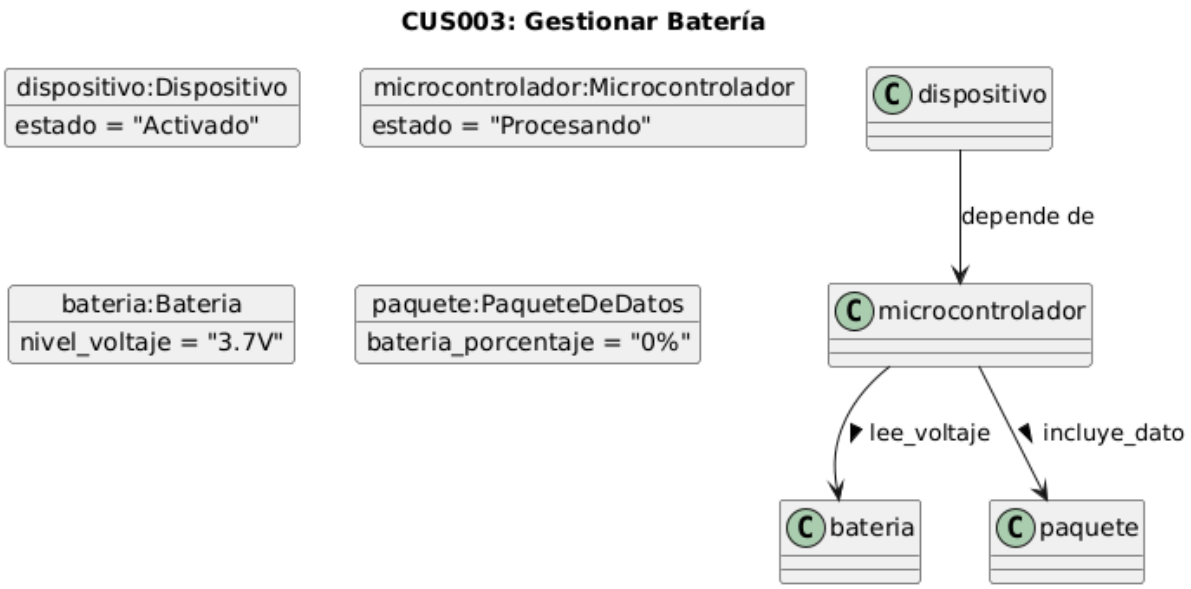
      CUS001 - Activar Alerta de Emergencia



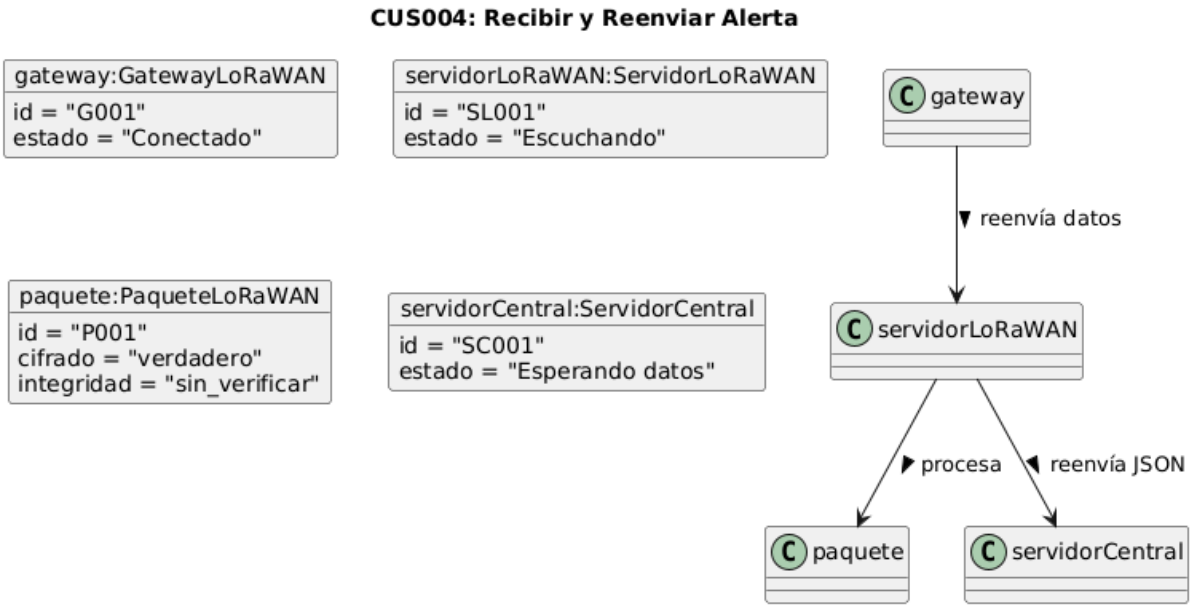
      CUS002 - Obtener Ubicación GPS



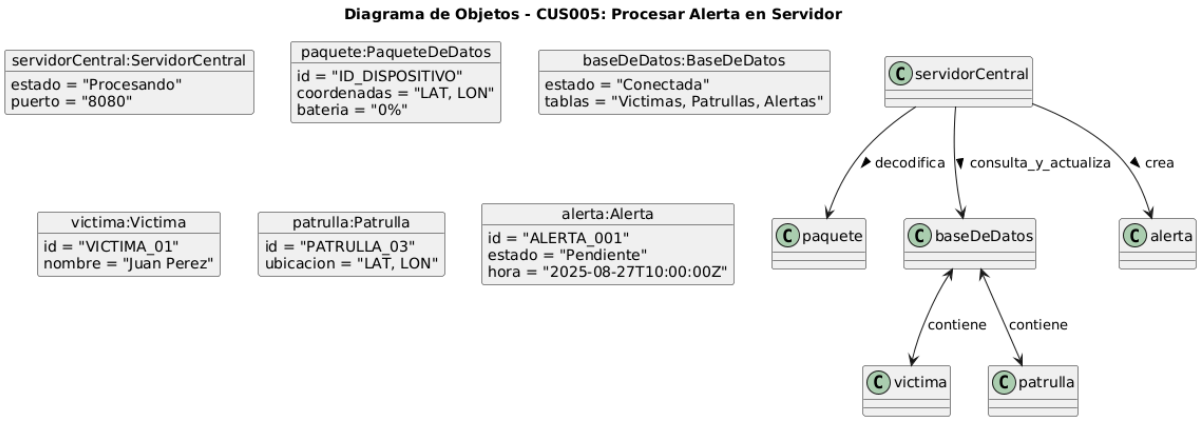
CUS003 - Gestionar Batería



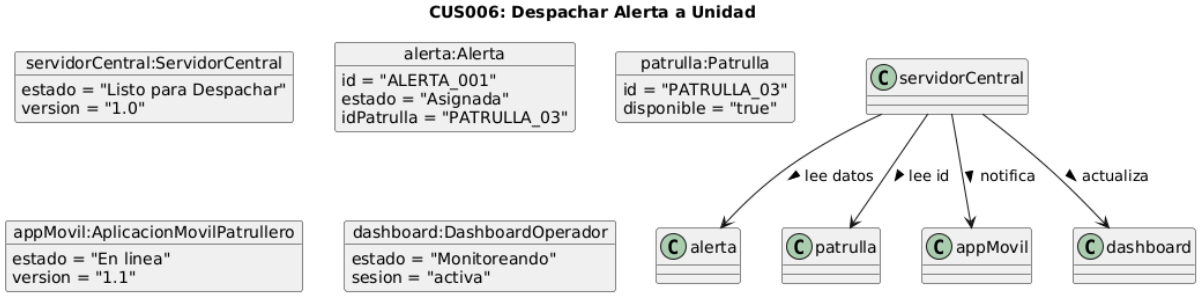
CUS004 - Recibir y Reenviar Alerta



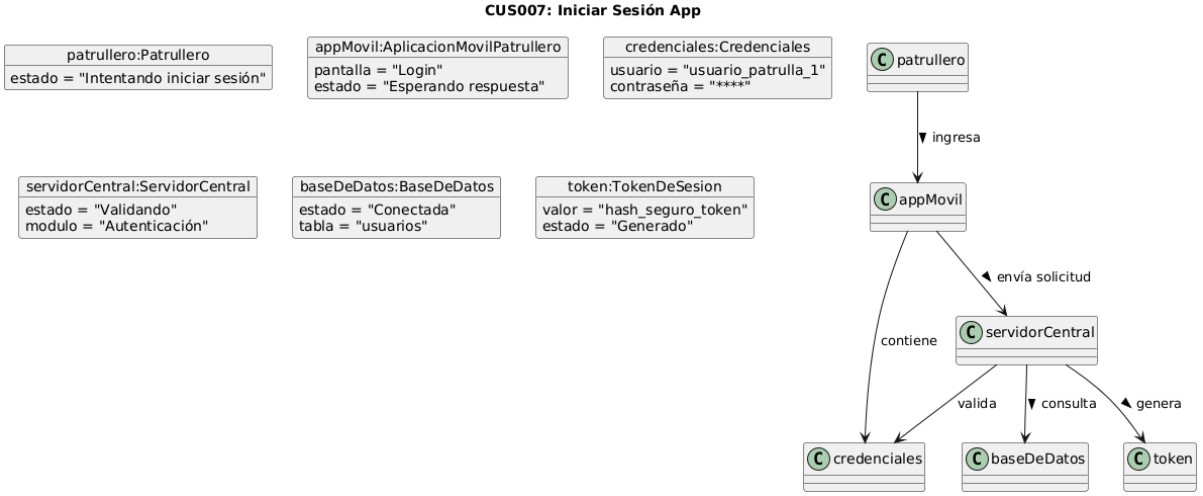
CUS005 - Procesar Alerta en Servidor



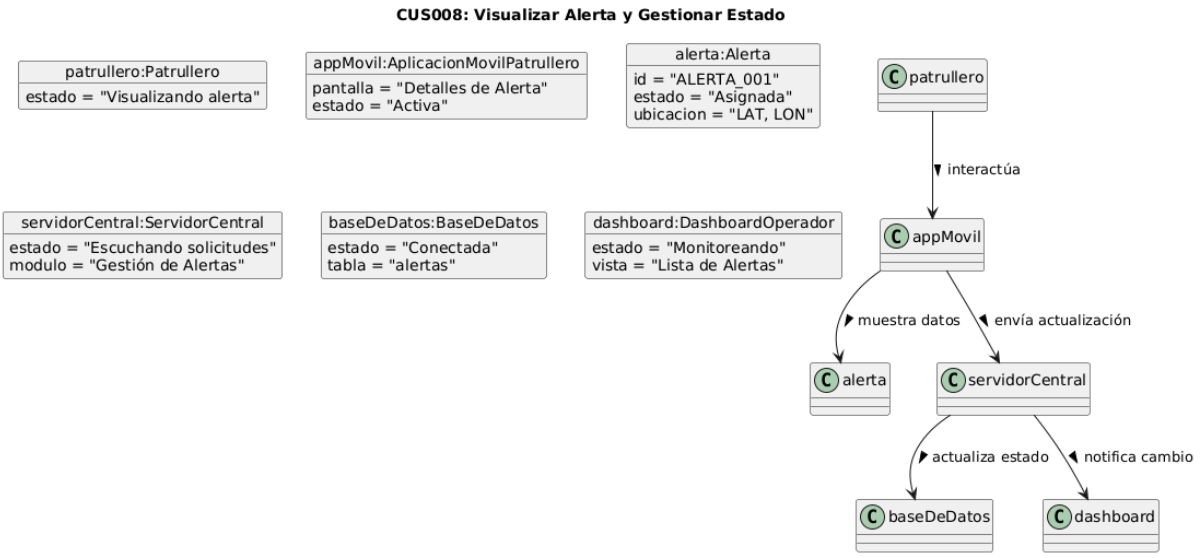
CUS006 - Despachar Alerta a Unidad



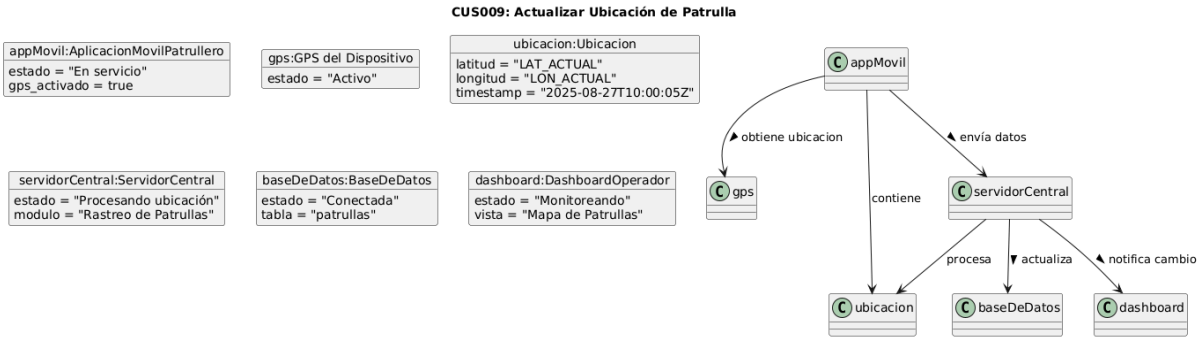
CUS007 - Iniciar Sesión App



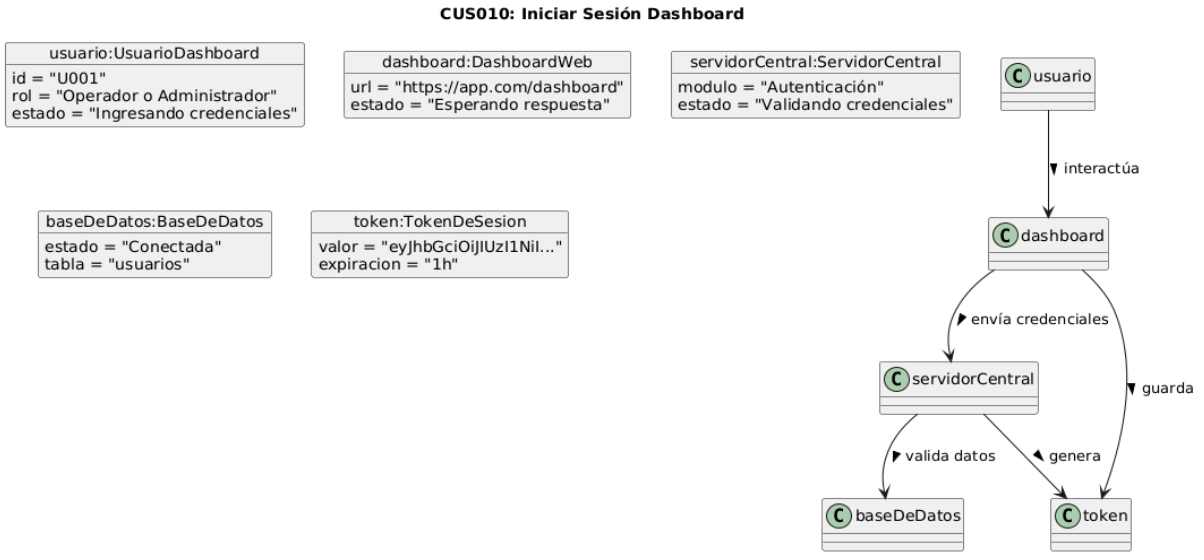
CUS008 - Visualizar Alerta y Gestionar Estado



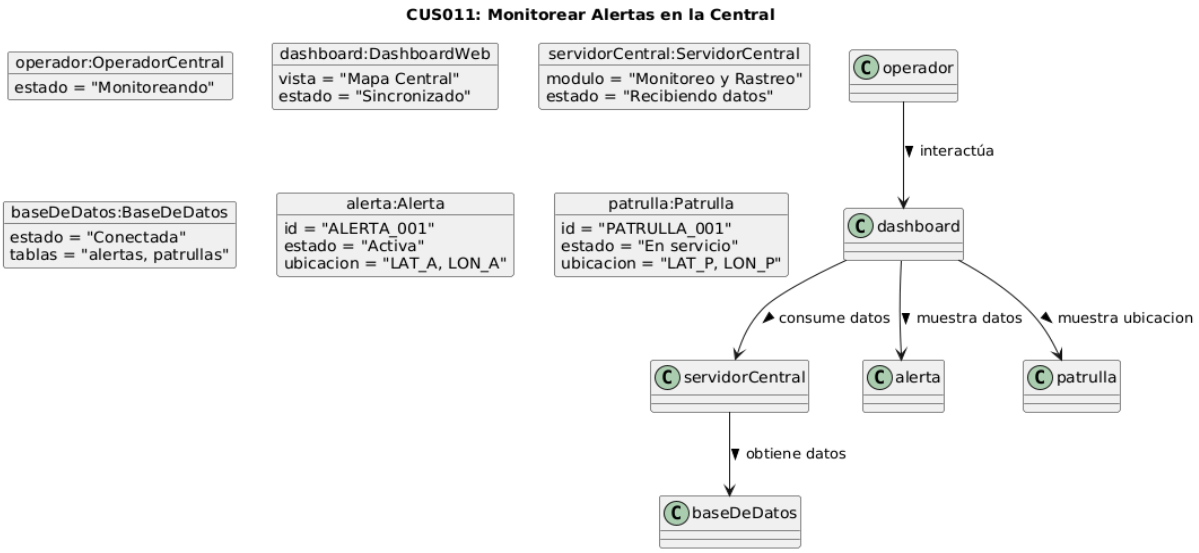
CUS009 - Actualizar Ubicación de Patrulla



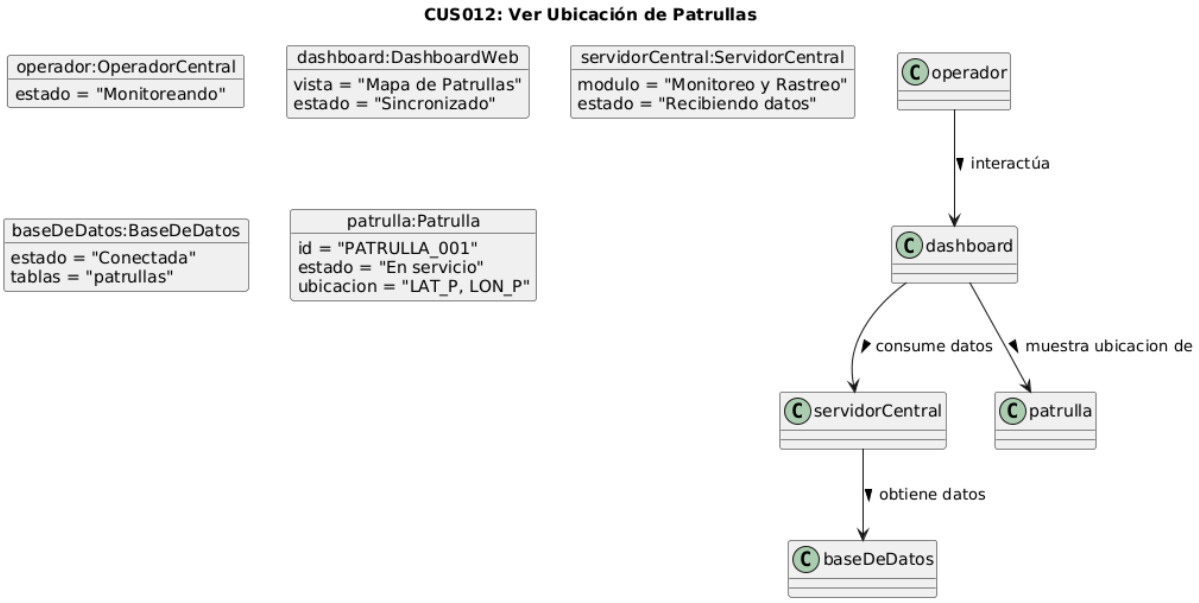
CUS010 - Iniciar Sesión Dashboard



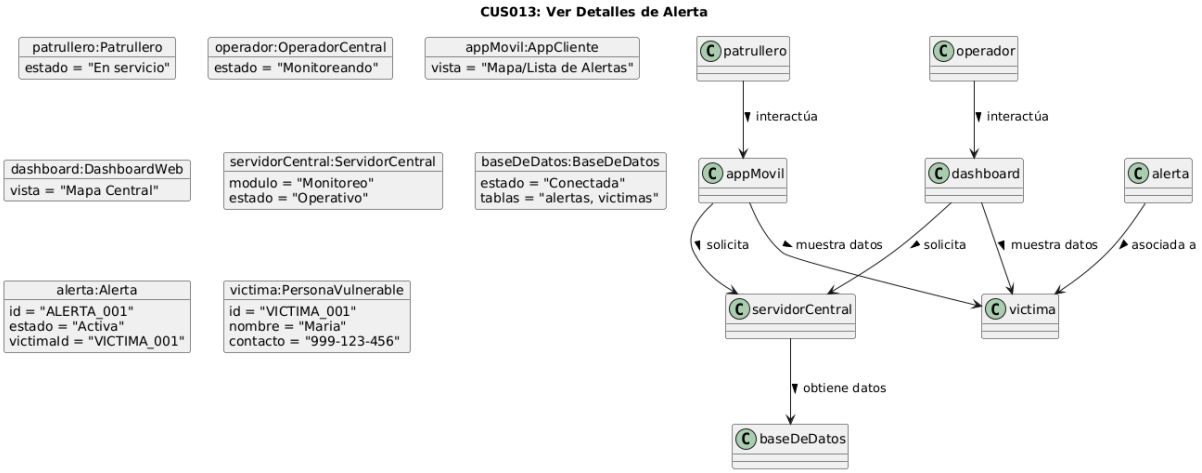
CUS011 - Monitorear Alertas en la Central



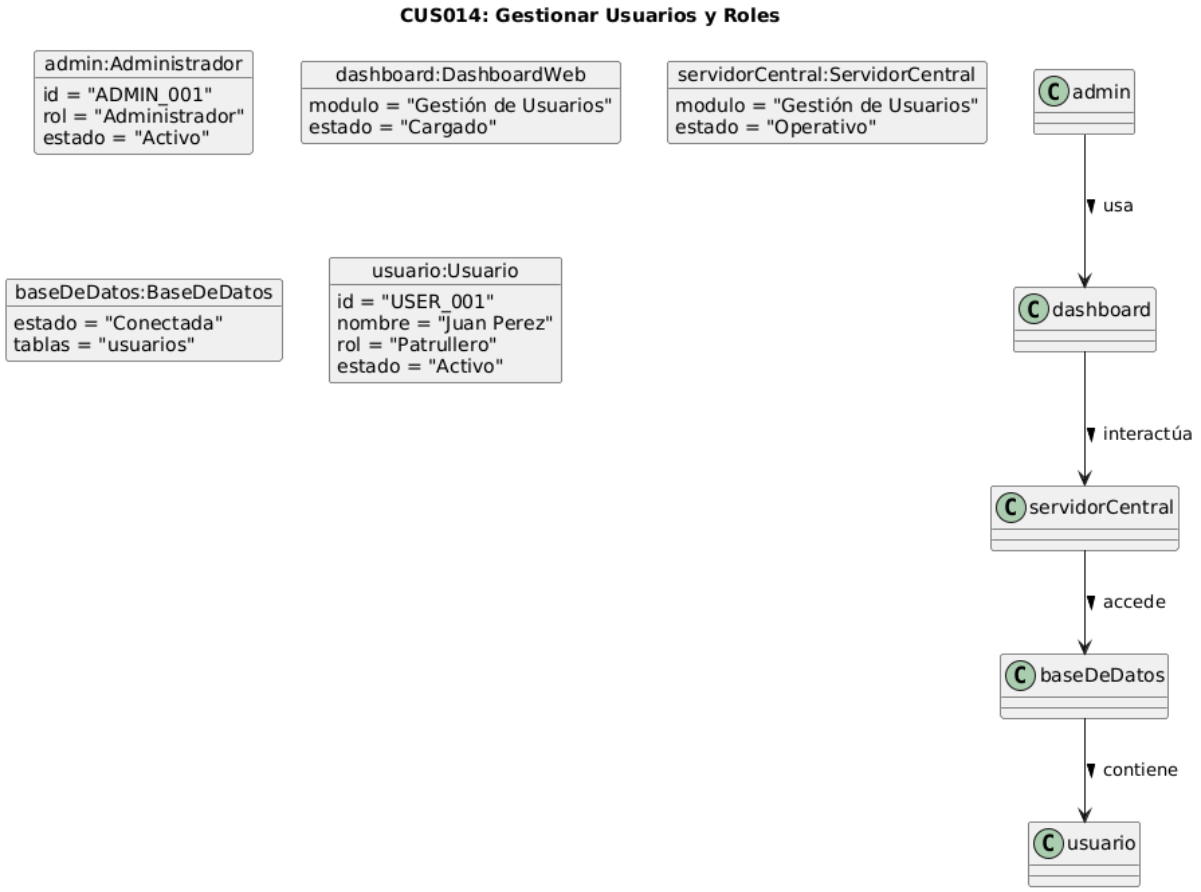
CUS012 - Ver Ubicación de Patrullas



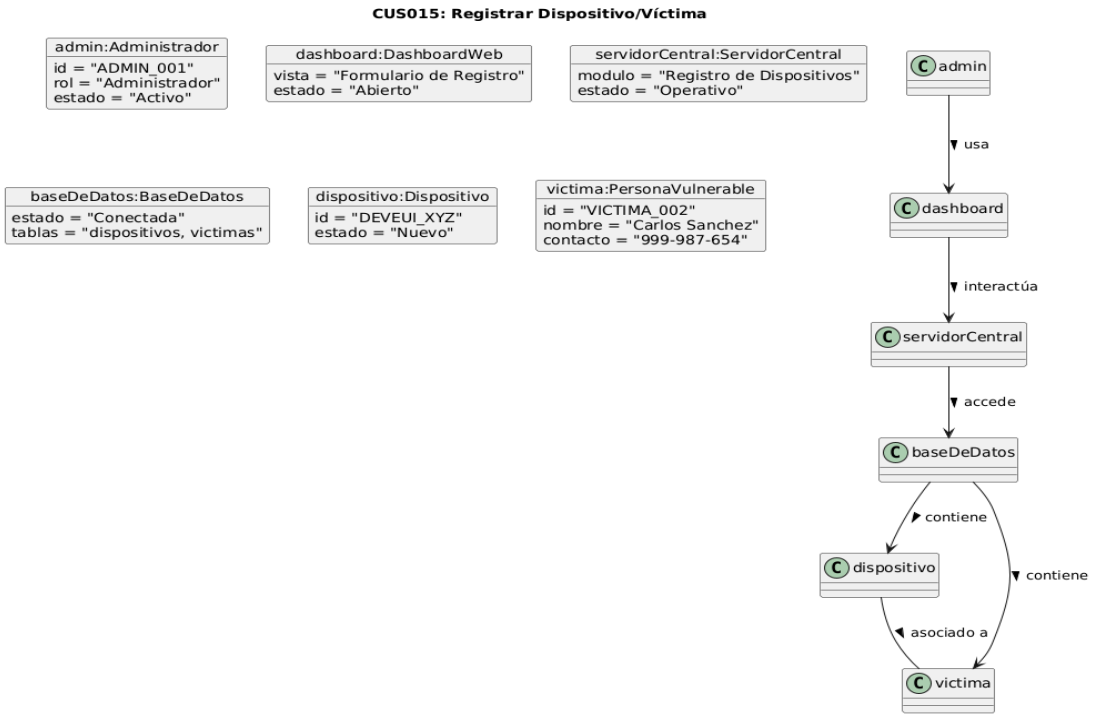
CUS013 - Ver Detalles de Alerta



CUS014 - Gestionar Usuarios y Roles

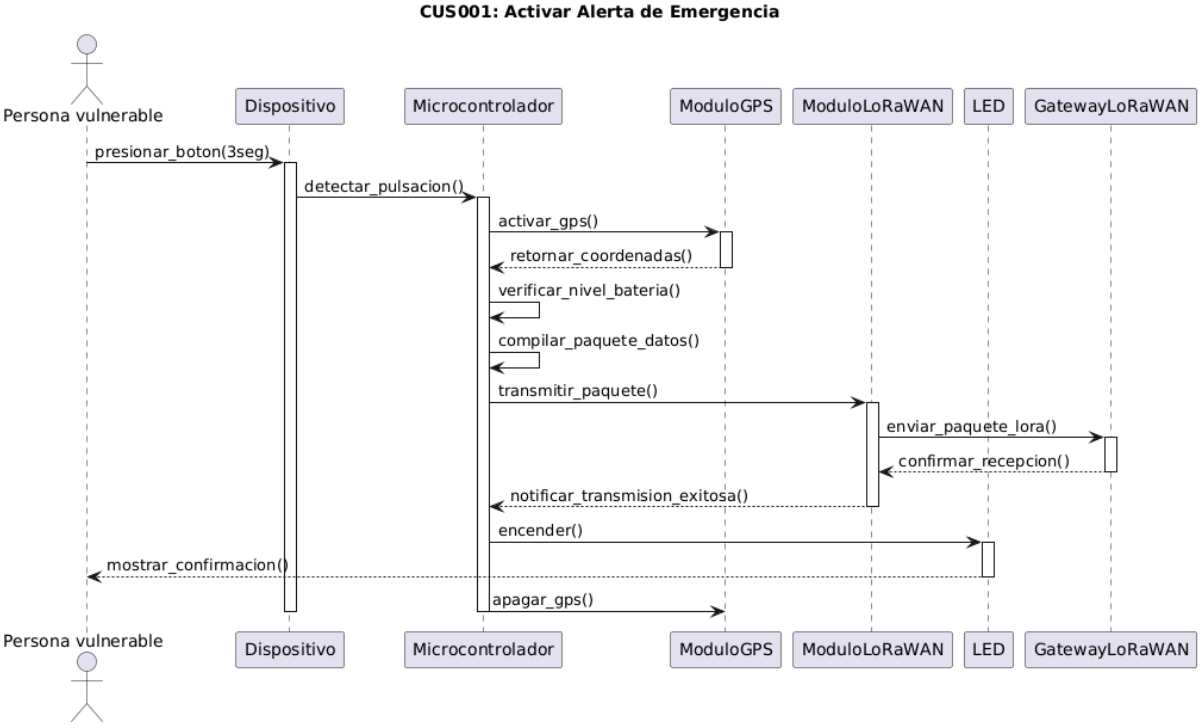


CUS015 - Registrar Dispositivo/Víctima

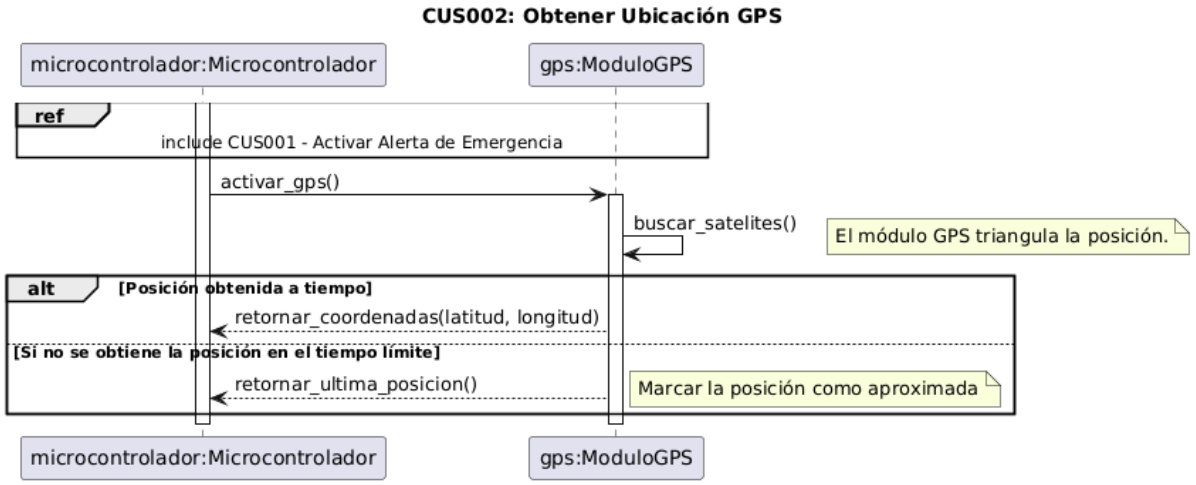


b. Diagrama de Secuencia

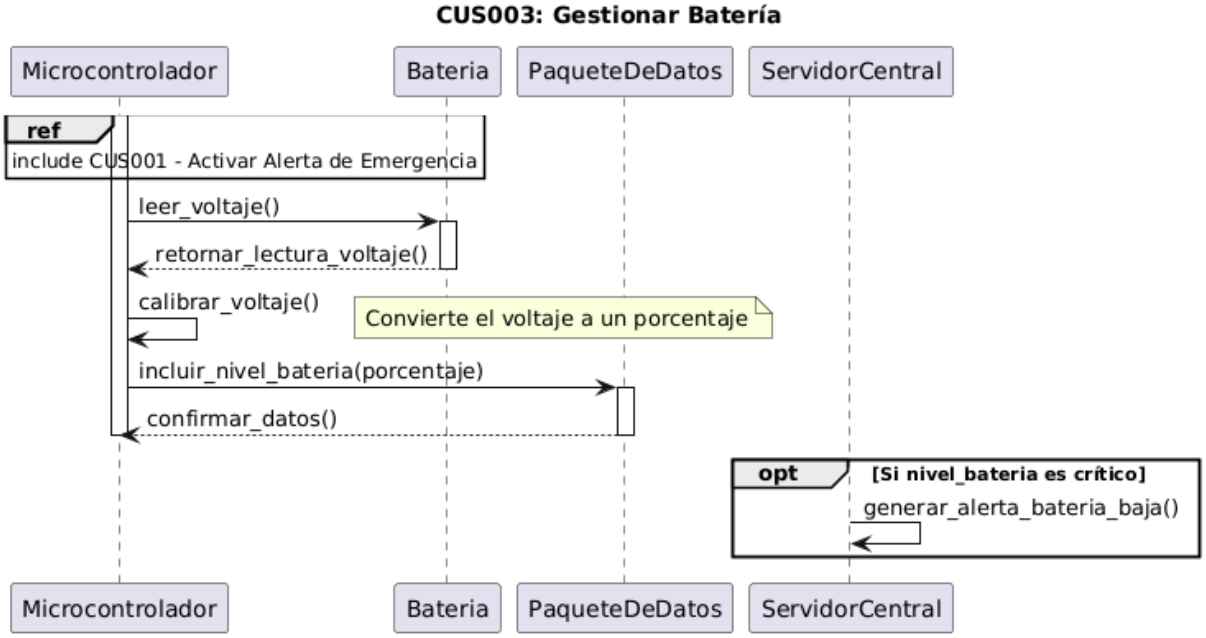
CUS001 - Activar Alerta de Emergencia



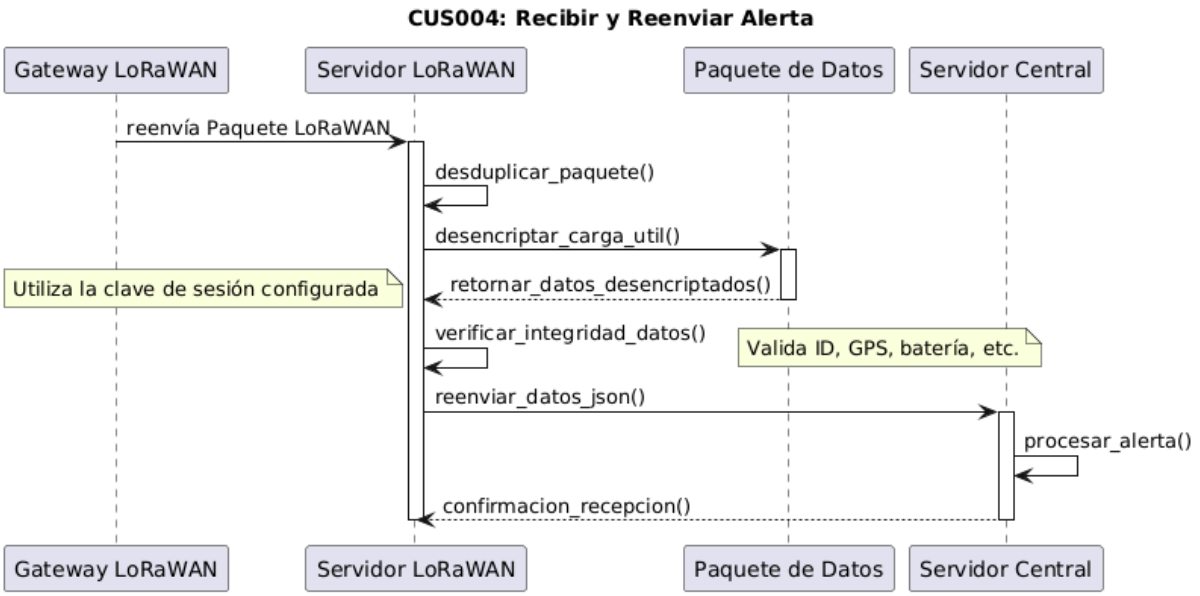
CUS002 - Obtener Ubicación GPS



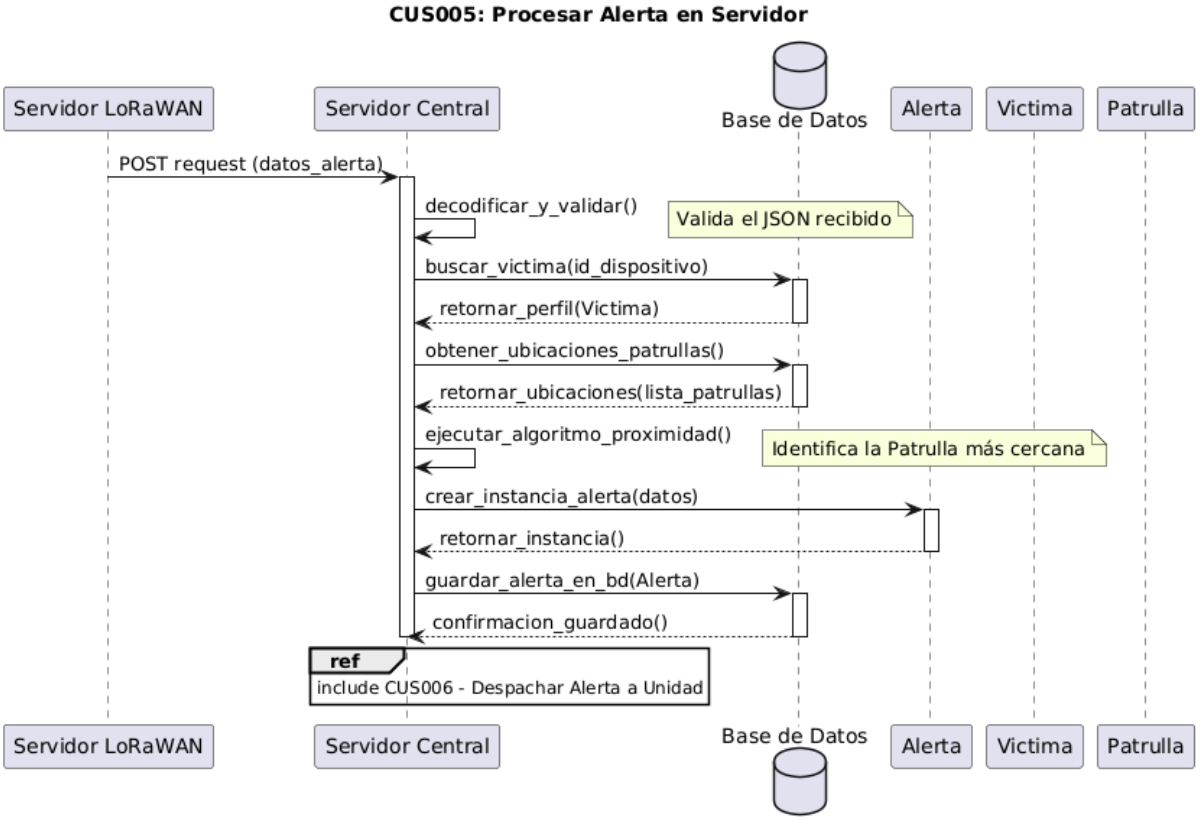
CUS003 - Gestionar Batería



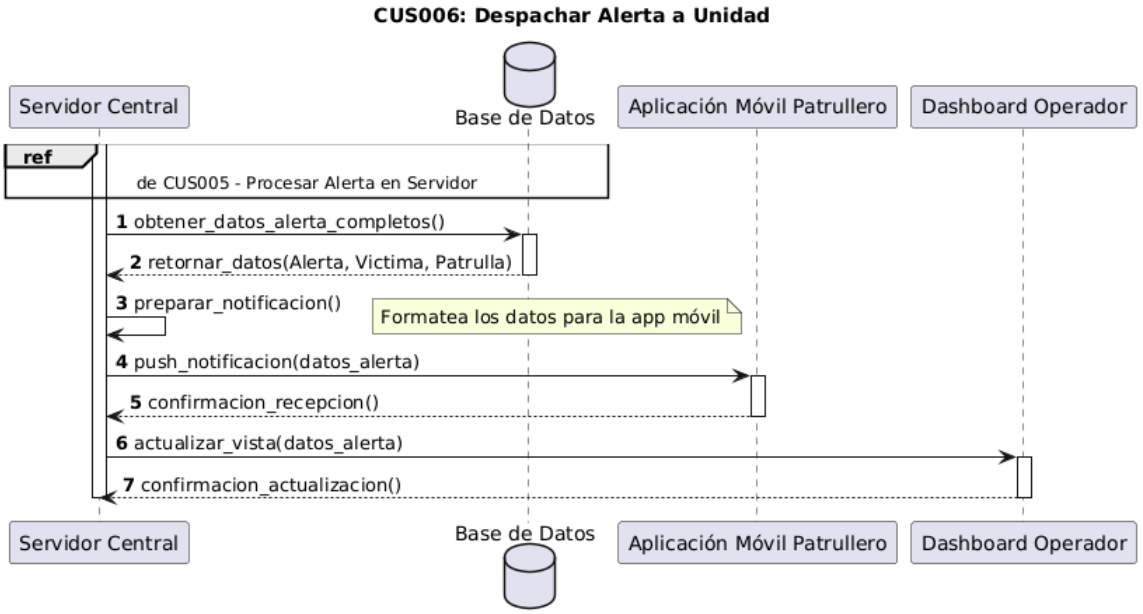
CUS004 - Recibir y Reenviar Alerta



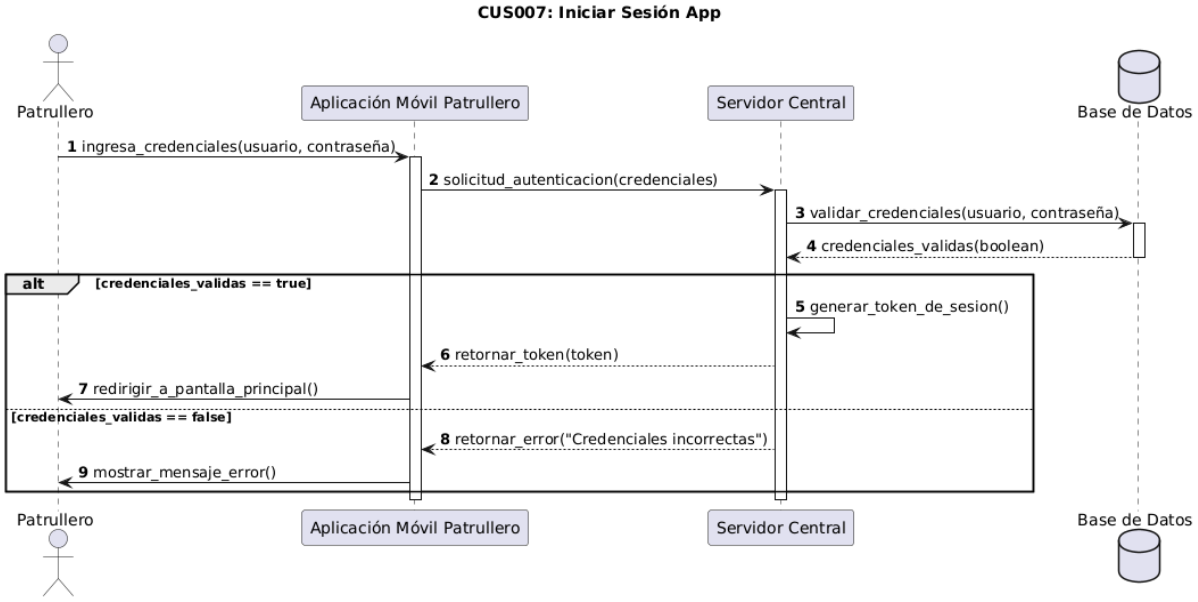
CUS005 - Procesar Alerta en Servidor



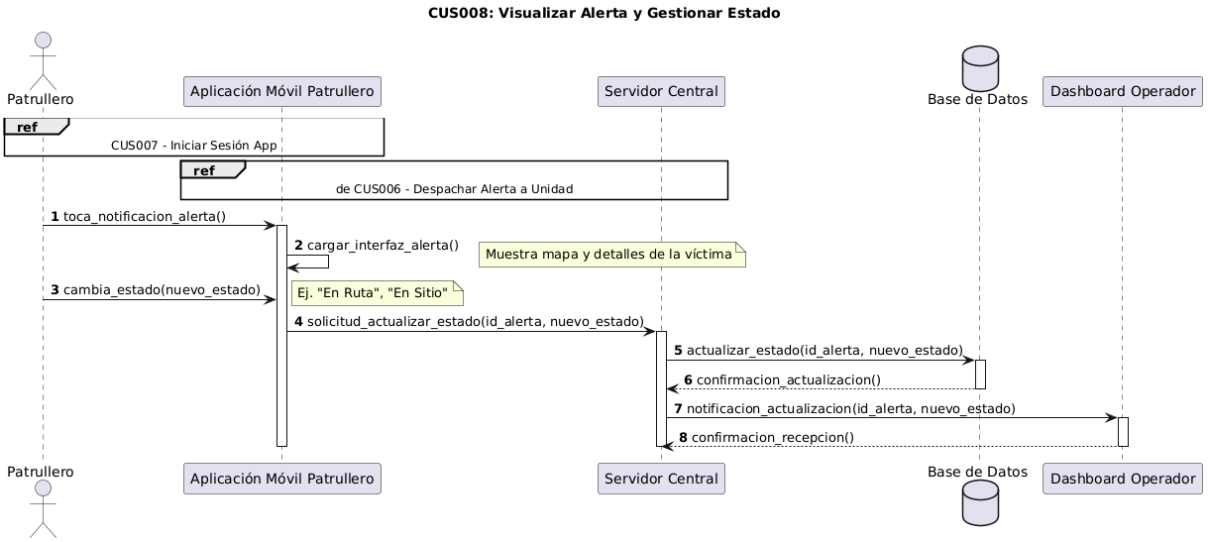
CUS006 - Despachar Alerta a Unidad



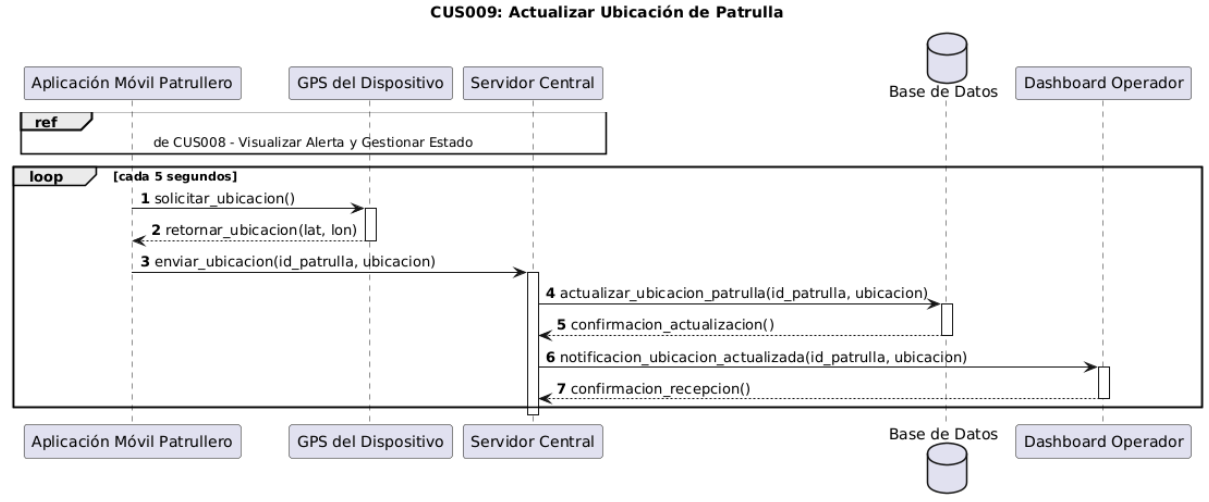
CUS007 - Iniciar Sesión App



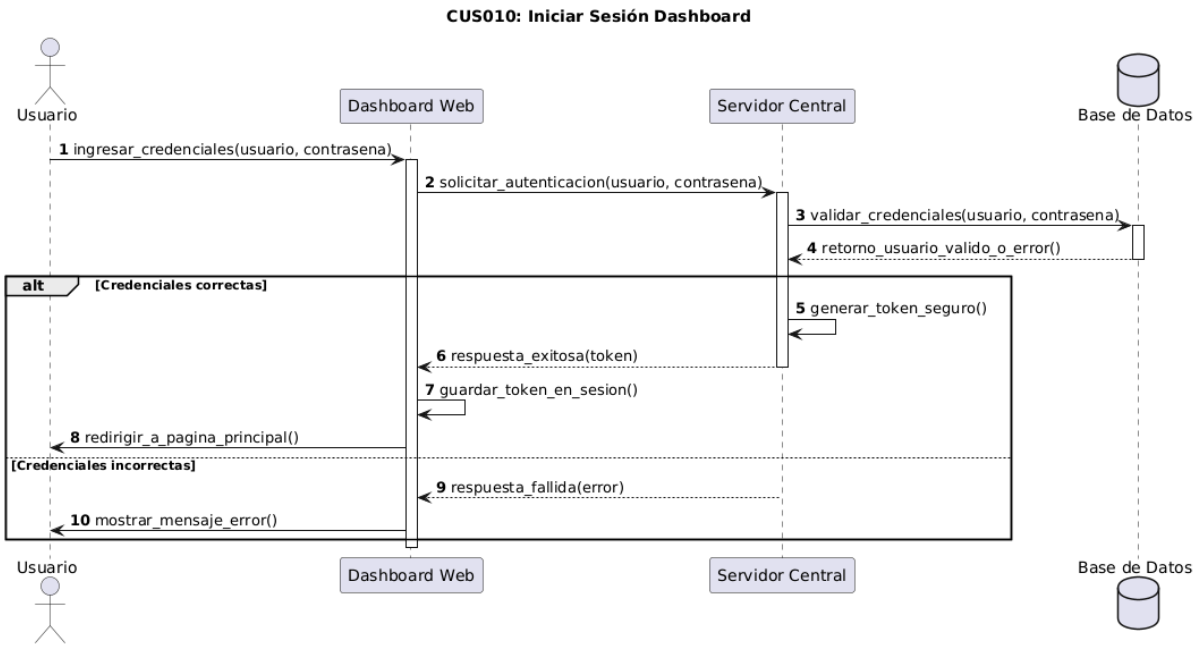
CUS008 - Visualizar Alerta y Gestionar Estado



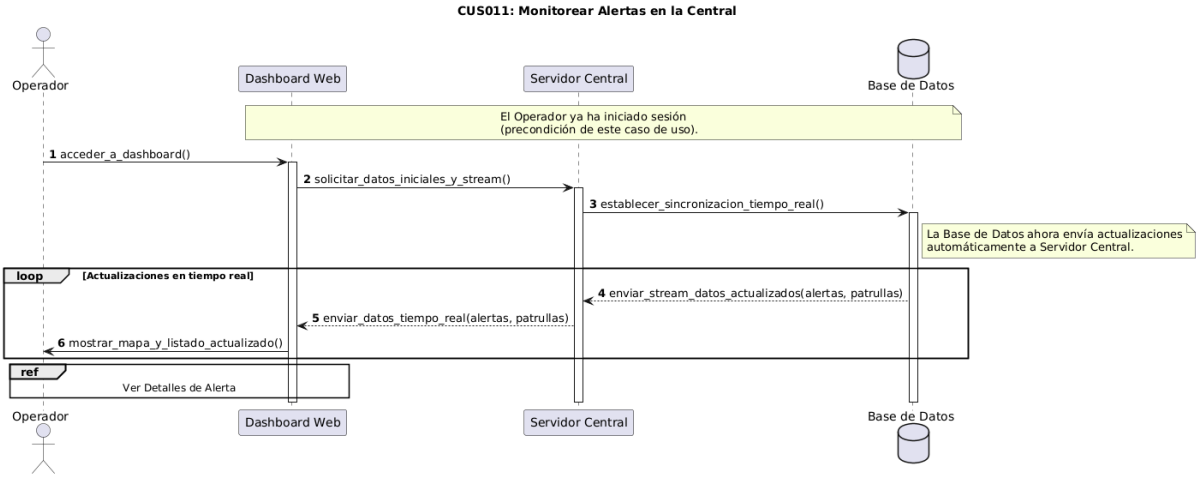
CUS009 - Actualizar Ubicación de Patrulla



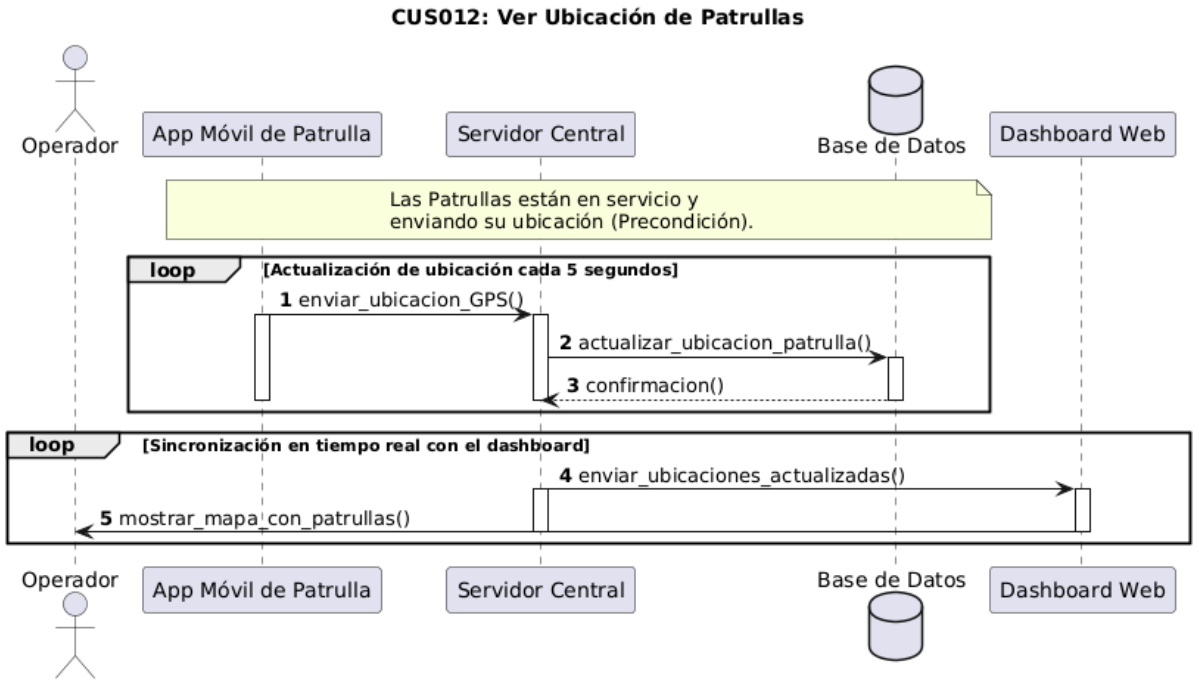
CUS010 - Iniciar Sesión Dashboard



CUS011 - Monitorear Alertas en la Central

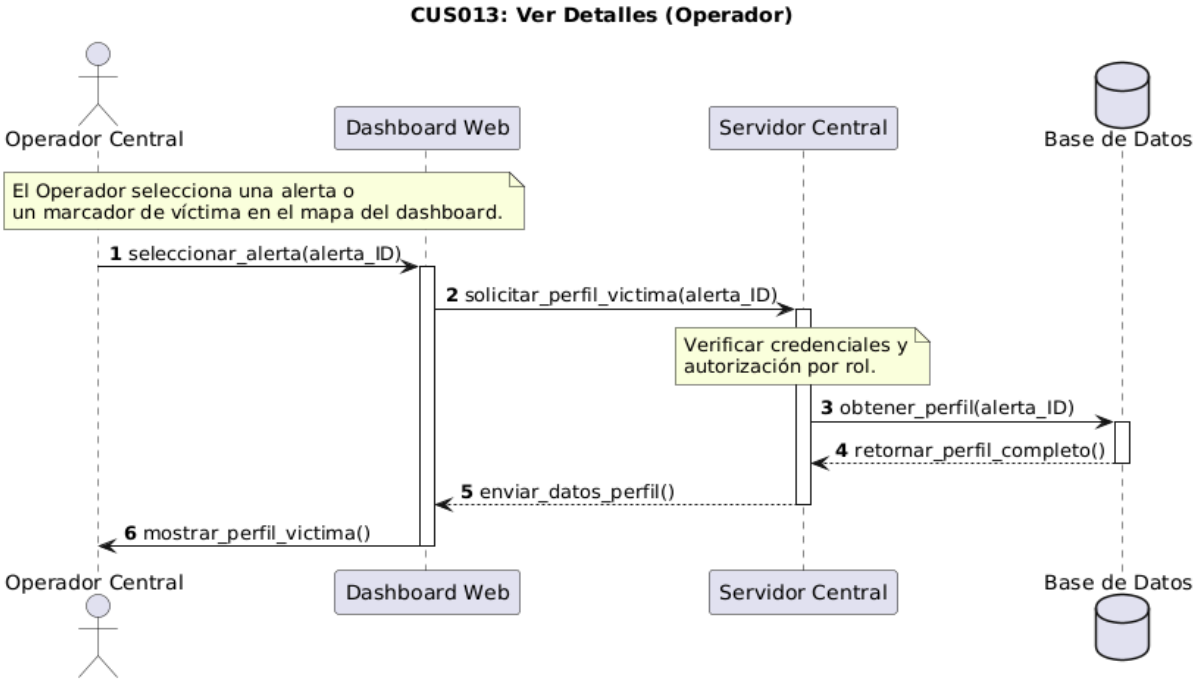


CUS012 - Ver Ubicación de Patrullas

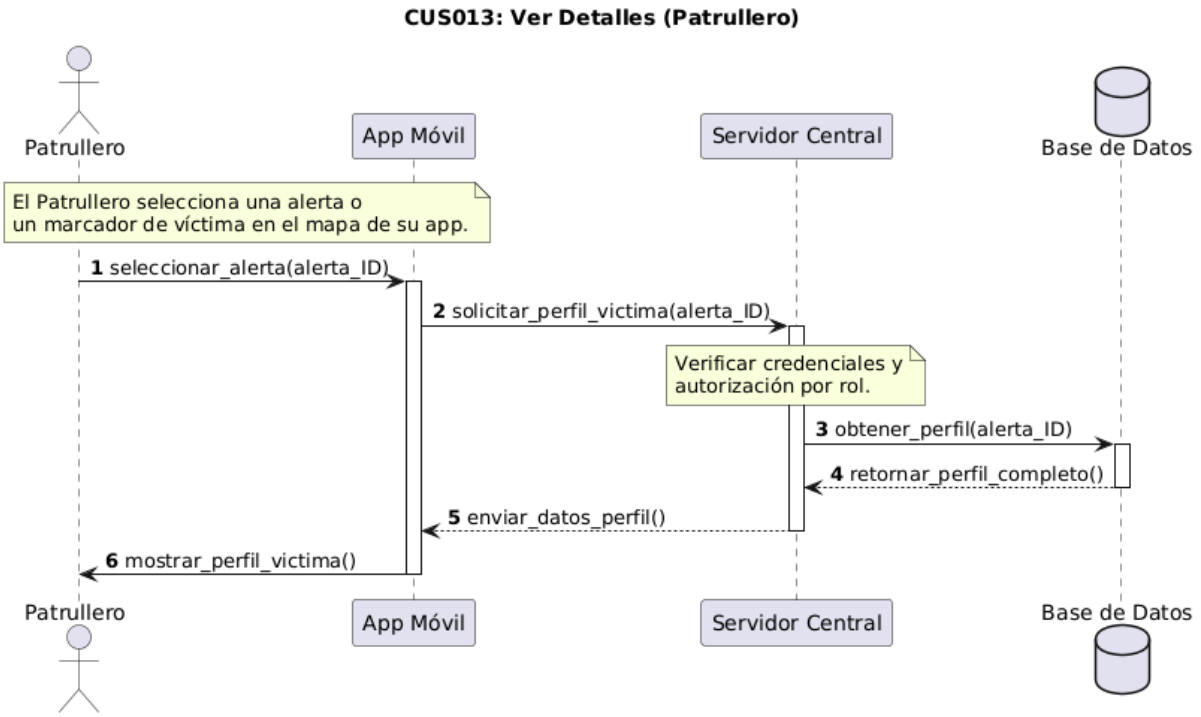


CUS013 - Ver Detalles de Alerta

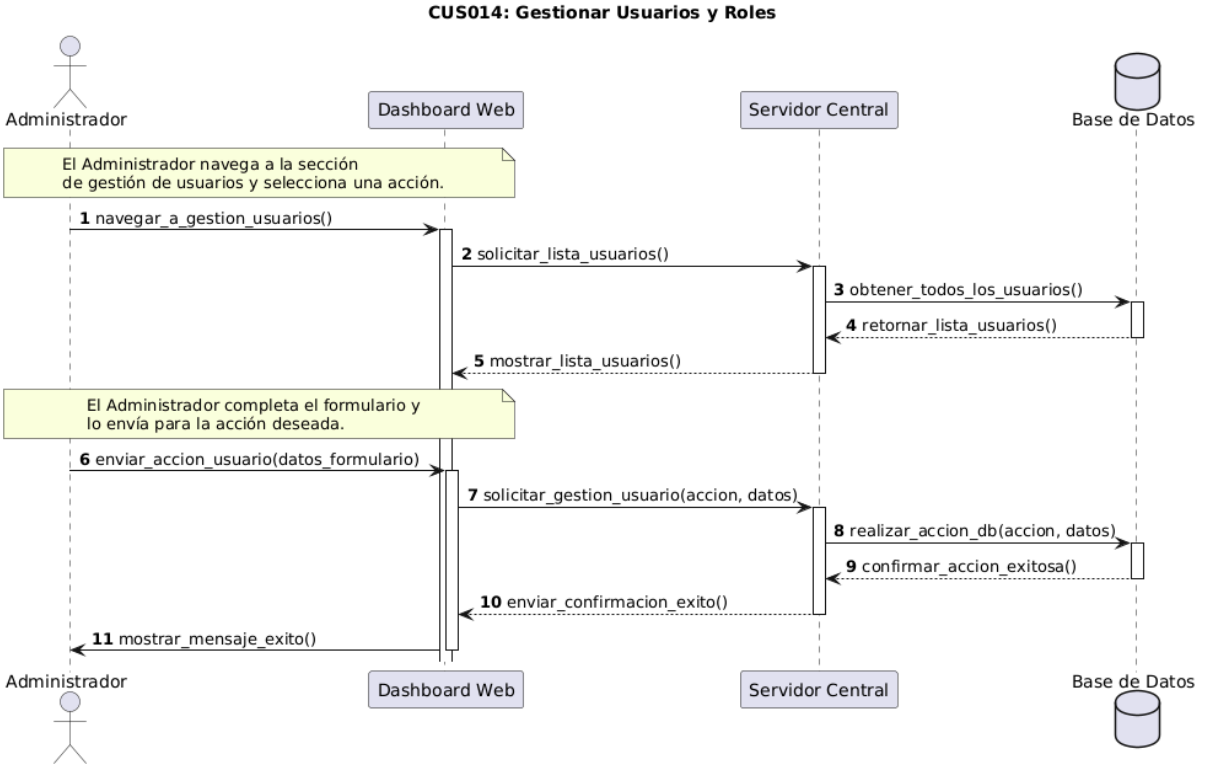
Operador



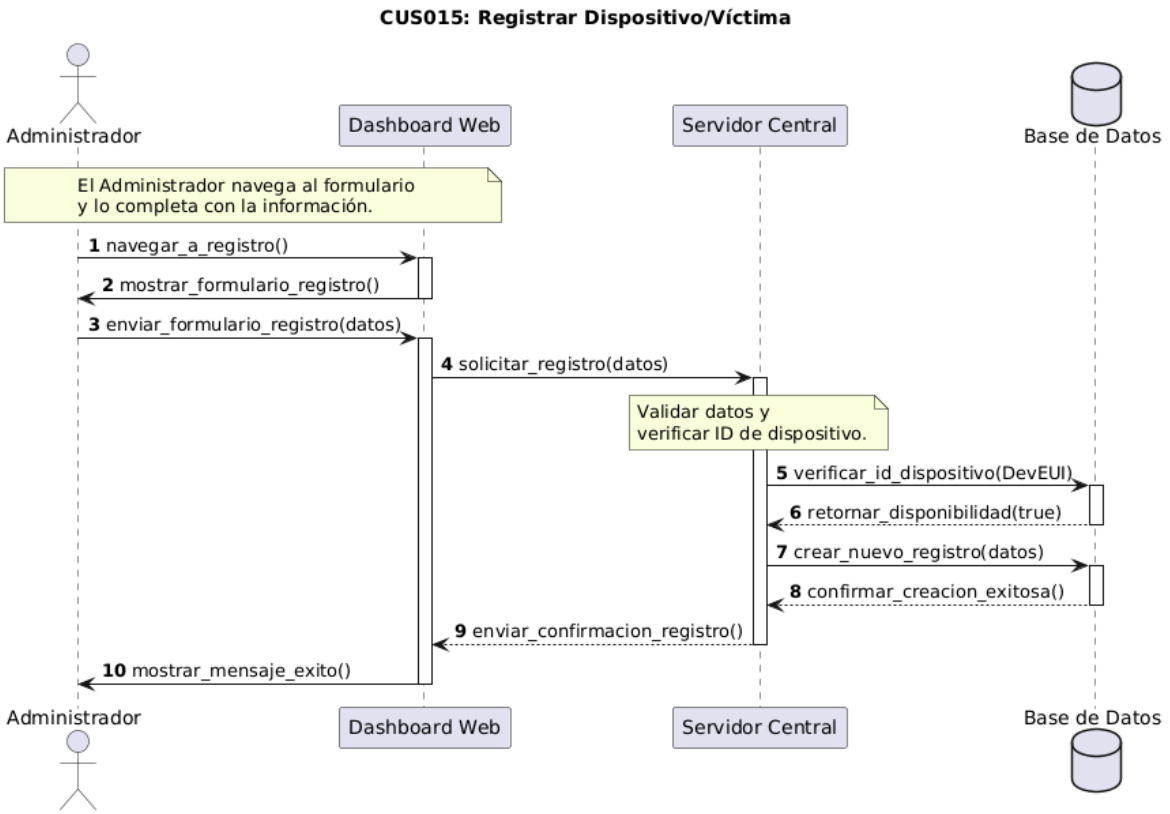
Patrullero



CUS014 - Gestionar Usuarios y Roles



CUS015 - Registrar Dispositivo/Víctima



c. Diagrama de Clases

CONCLUSIONES

El desarrollo del sistema de alerta personal basado en tecnología LoRa y dispositivos ESP32 ha permitido demostrar la viabilidad de una solución eficiente, de bajo costo y bajo consumo energético para situaciones de emergencia. La integración de módulos GPS y la comunicación LoRaWAN aseguran la transmisión de alertas incluso en áreas con baja cobertura celular, brindando mayor seguridad a las personas vulnerables.

La arquitectura modular del sistema, soportada por un backend en la nube (Firebase) y clientes multiplataforma (aplicación móvil y dashboard web), facilita la escalabilidad y el monitoreo en tiempo real de las alertas y recursos. El uso de servicios externos como Google Maps API mejora la experiencia de usuario al proporcionar visualización geoespacial precisa de las incidencias y patrullas en servicio.

En la etapa de pruebas, el sistema mostró un desempeño adecuado, con tiempos de respuesta bajos y una transmisión confiable de las alertas. La documentación y los diagramas arquitectónicos generados aseguran que el sistema sea comprensible y mantenible para futuras mejoras.

RECOMENDACIONES

Para fortalecer y garantizar la sostenibilidad del sistema de alerta personal desarrollado, se recomienda profundizar en la optimización energética del dispositivo autónomo. Es fundamental investigar e implementar técnicas avanzadas de ahorro de energía, tales como el uso de modos de suspensión profunda y la optimización de la transmisión de datos GPS, con el objetivo de maximizar la autonomía de la batería y reducir la frecuencia de recargas o reemplazos.

Asimismo, es importante priorizar la protección física del hardware. Se aconseja utilizar cajas resistentes y selladas que permitan resguardar los componentes electrónicos frente a condiciones ambientales adversas, tales como humedad, polvo o golpes, especialmente si el uso del dispositivo será en exteriores o situaciones de riesgo.

De cara a un despliegue a mayor escala, se recomienda preparar la infraestructura en la nube para soportar un mayor número de dispositivos y usuarios. Esto incluye la correcta configuración de recursos cloud, así como la implementación de mecanismos de balanceo de carga y redundancia en el backend, para asegurar tanto la disponibilidad como la escalabilidad del sistema ante un crecimiento de la demanda.

En materia de seguridad, es fundamental reforzar los mecanismos de autenticación y cifrado de datos en todas las etapas de comunicación, desde la transmisión LoRaWAN

hasta la interacción con Firebase y APIs externas. Esto ayudará a proteger la integridad y confidencialidad de la información transmitida y almacenada en el sistema.

Se sugiere igualmente la realización periódica de pruebas en campo, tanto en escenarios controlados como en situaciones reales. Estas pruebas permitirán ajustar parámetros críticos del sistema, como la sensibilidad de activación, los rangos de cobertura y la experiencia de usuario final, asegurando así la eficacia y usabilidad del sistema en condiciones reales.

Para mantener la seguridad y funcionalidad del sistema a lo largo del tiempo, es recomendable actualizar regularmente el firmware de los dispositivos, así como las dependencias de software de las aplicaciones móviles y web. Esto permitirá la incorporación de mejoras, correcciones de errores y parches de seguridad.

Finalmente, se debe verificar en todo momento el cumplimiento de la normativa legal vigente respecto al uso de frecuencias LoRa en la región de operación, así como asegurar la protección y manejo responsable de los datos personales de los usuarios, cumpliendo con las leyes y estándares de privacidad aplicables.

REFERENCIAS

Ministerio de la Mujer y Poblaciones Vulnerables (MIMP). (s. f.). *Estadísticas – MIMP*. Recuperado de https://www.mimp.gob.pe/omep/resumenes-departamentales.php

PlatformIO. (s. f.). *TTGO T-Beam — PlatformIO latest documentation*. Recuperado de https://docs.platformio.org/en/latest/boards/espressif32/ttgo-t-beam.html

Microsoft. (s. f.). *Common web application architectures*. En *Microsoft Learn*. Recuperado de https://learn.microsoft.com/es-es/dotnet/architecture/modern-web-apps-azure/common-web-application-architectures

The Things Industries. (s. f.). *API Concepts*. Recuperado de https://www.thethingsindustries.com/docs/api/concepts/

The Things Network Forum. (2021). *Register device – The Things Stack V3 API*. Recuperado de

https://www.thethingsnetwork.org/forum/t/register-device-the-things-stack-v3-api/51816/3

The Things Industries. (s. f.). *API Reference – HTTP Routes*. Recuperado de https://www.thethingsindustries.com/docs/api/reference/http/routes/