

**Trabajo final de Pregrado**

**Carrera:** Ingeniería en Sistemas

**Título:** Sistema de Alarma Personal Móvil en Smartphones (SECURE-ON)

**Tutor:** Ing. Eduardo Enrique Piray

**Alumno:** Martín, Fernando José

**Declaración de derechos de autor**

Como autor, declaro que este documento es un trabajo original realizado con el acompañamiento tutorial del Ing. Eduardo Enrique Piray, el cual puede ser reproducido y utilizado como base de consulta por el IUA (Instituto Universitario Aeronáutico) y los estudiantes.

La Universidad podrá conservar más de una copia del documento sin alterar su contenido.

Fernando José Martín, Córdoba 10 de octubre de 2025

**Agradecimientos**

Quiero expresar mi más profundo agradecimiento a mi esposa Maria Fernanda, cuyo amor, apoyo incondicional y paciencia infinita han sido el pilar fundamental de mi camino. A mis hijos, Augusto y Marco, quienes con su alegría, su curiosidad y su cariño me inspiran cada día a ser mejor. A mi padre Fernando y a mi madre Susana, por haberme dado la vida, los valores y una educación basada en el esfuerzo y la honestidad. Y a mi tía Graciela, por su cariño siempre presente y sus sabios consejos.

También agradezco muy especialmente a la IUA por haberme brindado la invaluable oportunidad de formarme, por abrirme las puertas al conocimiento y por ser el espacio donde pude desarrollar las herramientas que hoy me definen profesional y personalmente. A todos, mi eterno reconocimiento.

**Dedicatoria**

Este trabajo quiero dedicarlo a mi mujer, Maria Fernanda, a mi hijos Augusto y Marco, que me han dado el soporte emocional y me han tenido la paciencia necesaria para que pudiera terminar esta presentación.

También a mi mama, Susana y a mi tia Graciela que también me han apoyado en todo el trayecto de la Carrera y a mi papa Fernando que aunque ya no este físicamente, me guía desde el cielo

**Resumen**

Secure-On es una aplicación móvil de seguridad personal que opera como una alarma silenciosa en segundo plano, diseñada para responder ante situaciones de robo o agresión física. Su objetivo principal es brindar protección discreta e inmediata mediante la activación de un protocolo de emergencia que se inicia automáticamente al detectar un comando de voz predefinido, un gesto específico o un patrón configurado por el usuario. Una vez activada, la aplicación bloquea temporalmente el dispositivo y, tras una breve ventana de cancelación configurable, envía alertas multicanal a contactos de emergencia y a un Centro de Monitoreo profesional. Estas alertas incluyen la ubicación del usuario y datos del incidente, facilitando una respuesta coordinada.

La aplicación integra funcionalidades avanzadas de captura de evidencias durante la alarma, como grabación de audio ambiental y toma de fotografías con ambas cámaras del dispositivo, siempre que las condiciones de luz lo permitan. Estos datos se transmiten automáticamente al Centro de Monitoreo en tiempo real, priorizando la privacidad y la eficiencia energética. Para garantizar operatividad en condiciones adversas, el sistema incluye mecanismos de resiliencia, como geolocalización por redes celulares ante falta de GPS, almacenamiento local de datos si se pierde conectividad y persistencia del estado de alarma tras reinicios forzados del dispositivo.

Desde la perspectiva del usuario, Secure-On ofrece una experiencia integral que abarca registro inicial, configuración personalizada de contactos y métodos de activación, y un cuestionario post-evento para recabar detalles del incidente. La aplicación es compatible con Android e iOS, desarrollada con un enfoque multiplataforma utilizando tecnologías como Ionic y Capacitor, lo que asegura un rendimiento nativo y acceso a los sensores del dispositivo. Además, incorpora un modo sigiloso que oculta su presencia durante una emergencia, reforzando su carácter discreto.

El Centro de Monitoreo dispone de una plataforma web desarrollada con Angular en el frontend y Spring Boot en el backend, que permite visualizar alertas en tiempo real en un mapa interactivo, gestionar la comunicación con autoridades locales y consultar historiales detallados de incidentes. Esta plataforma facilita la coordinación de respuestas profesionales y el seguimiento documentado de cada activación, asegurando que cada alarma sea atendida de manera eficiente y verificable.

En conjunto, Secure-On constituye una solución autónoma de protección que combina discreción, respuesta inmediata y respaldo profesional. Su arquitectura está diseñada para mantener la operatividad en escenarios críticos, ofreciendo una capa adicional de seguridad tanto para usuarios individuales como para instituciones que requieran monitoreo centralizado. El proyecto sigue una metodología de desarrollo PUDS y se estructura en entregables progresivos (MVP), priorizando funcionalidades básicas de activación, notificación y resiliencia en su primera fase.

# Índice

[2) Glosario 5](#_Toc222620430)

[3) Datos del Negocio 7](#_Toc222620431)

[3.1) Descripción y Posicionamiento de la Empresa 7](#_Toc222620432)

[3.2) Nombre de la Empresa 7](#_Toc222620433)

[3.3) Rubro del Negocio 7](#_Toc222620434)

[3.4) Domicilio de la Empresa 8](#_Toc222620435)

[3.5) Organigrama 9](#_Toc222620436)

[3.6) Misión, Visión, Políticas, Objetivos, Metas y Factores de Éxito 12](#_Toc222620437)

[3.7) Oportunidades de Negocio 13](#_Toc222620438)

[3.8) Entorno de usuarios 14](#_Toc222620439)

[3.9) Necesidades principales de la empresa 15](#_Toc222620440)

[3.10) Alternativas y Competencia 16](#_Toc222620441)

[3.11) Precedencia y Prioridad 17](#_Toc222620442)

[4) Datos del Proyecto 18](#_Toc222620443)

[4.1) Descripción del Proyecto a desarrollar 18](#_Toc222620444)

[4.2) Objetivos y Alcances del Proyecto 19](#_Toc222620445)

[4.3) Características Técnicas del Proyecto 20](#_Toc222620446)

[4.3.1) Arquitectura 20](#_Toc222620447)

[4.3.2) Funcionalidades Clave 21](#_Toc222620448)

[4.3.3) Seguridad y Rendimiento 21](#_Toc222620449)

[4.3.4) Ventajas Técnicas 21](#_Toc222620450)

[4.4) Metodología a utilizar 22](#_Toc222620451)

[4.5) Software de desarrollo 22](#_Toc222620452)

[4.6) Lista y descripción de las funcionalidades que abarca el sistema 22](#_Toc222620453)

[5) Planeamiento 25](#_Toc222620454)

[5.1) Organización del proyecto 25](#_Toc222620455)

[5.1.1) Listado de Roles 25](#_Toc222620456)

[5.2) Lista de Entregables 29](#_Toc222620457)

[5.3) Planifiación 30](#_Toc222620458)

[5.3.1) Iteración I: Núcleo de Seguridad 30](#_Toc222620459)

[5.3.2) Iteración II: Métodos Avanzados & Evidencias 31](#_Toc222620460)

[5.3.3) Iteración III: Resiliencia y Optimización 32](#_Toc222620461)

[5.4) Agenda 34](#_Toc222620462)

[5.4.1) Iteración I 34](#_Toc222620463)

[5.4.2) Iteración II 34](#_Toc222620464)

[5.4.3) Iteración III 35](#_Toc222620465)

[5.5) Lista de Riesgos 35](#_Toc222620466)

[5.5.1) Riesgos Técnicos 35](#_Toc222620467)

[5.5.2) Riesgos de Proyecto 39](#_Toc222620468)

[5.5.3) Riesgos de Seguridad 42](#_Toc222620469)

[5.6) Interfaces de Usuario 44](#_Toc222620470)

[5.6.1) Aplicación Movil 44](#_Toc222620471)

[5.6.2) Centro de Monitoreo 50](#_Toc222620472)

[6) Modelo de Casos de Uso del Negocio 52](#_Toc222620473)

[7) Modelo de Casos de Uso 53](#_Toc222620474)

[7.1) Modelo de Casos de Uso del Sistema 53](#_Toc222620475)

[7.1.1) Módulo de Activación 54](#_Toc222620476)

[7.1.2) Módulo de Notificación 54](#_Toc222620477)

[7.1.3) Módulo de Configuración 55](#_Toc222620478)

[7.1.4) Módulo de Evidencias 55](#_Toc222620479)

[7.1.5) Módulo de Autenticación 56](#_Toc222620480)

[7.1.6) Módulo de Monitoreo 56](#_Toc222620481)

[7.2) Especificación de Casos de Uso 57](#_Toc222620482)

[7.2.1) Módulo Activación 57](#_Toc222620483)

[7.2.2) Modulo Notificación 71](#_Toc222620484)

[7.2.3) Modulo Finalización 83](#_Toc222620485)

[7.2.4) Modulo Configuracion 91](#_Toc222620486)

[7.2.5) Modulo Autenticación 100](#_Toc222620487)

[7.2.6) Modulo Monitoreo 123](#_Toc222620488)

[7.2.7) Modulo Evidencias 134](#_Toc222620489)

[8) Análisis 144](#_Toc222620490)

[8.1) Diagramas de Actividades 144](#_Toc222620491)

[8.1.1) UC-001: Activar Alarma 144](#_Toc222620492)

[8.1.2) UC-002: Activar Manualmente 145](#_Toc222620493)

[8.1.3) UC-006: Bloquear Dispositivo 146](#_Toc222620494)

[8.1.4) UC-007: Mostrar Ventana de Cancelación 147](#_Toc222620495)

[8.1.5) UC-009: Enviar Alarma a Contactos 148](#_Toc222620496)

[8.1.6) UC-010: Transmitir a Centro de Monitoreo 149](#_Toc222620497)

[8.2) Diagramas de Clases de Análisis 150](#_Toc222620498)

[8.2.1) UC-001: Activar Alarma 150](#_Toc222620499)

[8.2.2) UC-002: Activar Manualmente 150](#_Toc222620500)

[8.2.3) UC-006: Bloquear Dispositivo 151](#_Toc222620501)

[8.2.4) UC-007: Mostrar Ventana de Cancelación 151](#_Toc222620502)

[8.3) Diagramas de Colaboración 152](#_Toc222620503)

[8.3.1) UC-001: Activar Alarma 152](#_Toc222620504)

[8.3.2) UC-002: Activar Manualmente 152](#_Toc222620505)

[8.3.3) UC-006: Bloquear Dispositivo 153](#_Toc222620506)

[8.3.4) UC-007: Mostrar Ventana de Cancelación 153](#_Toc222620507)

[9) Diseño 154](#_Toc222620508)

[9.1) Diagramas de Secuencia 154](#_Toc222620509)

[9.1.1) UC-001: Activar Alarma 154](#_Toc222620510)

[9.1.2) UC-002: Activar Manualmente 155](#_Toc222620511)

[9.1.3) UC-006: Bloquear Dispositivo 156](#_Toc222620512)

[9.1.4) UC-007: Mostrar Ventana de Cancelación 157](#_Toc222620513)

[10) Implementación 158](#_Toc222620514)

[10.1) Modelo de Base de Datos 158](#_Toc222620515)

[10.2) Diagrama de Despliegue 159](#_Toc222620516)

[10.3) Versionado del Proyecto 160](#_Toc222620517)

[10.3.1) Lineamientos de Versionado 160](#_Toc222620518)

[10.3.2) Repositorios del Proyecto 161](#_Toc222620519)

[10.4) Lineamientos de Código y Buenas Practicas 162](#_Toc222620520)

[10.4.1) Lineamientos de Código Java 162](#_Toc222620521)

[11) Pruebas 169](#_Toc222620522)

[11.1) Casos de Prueba Unitarios 169](#_Toc222620523)

[11.1.1) UC-001: ACTIVAR ALARMA 169](#_Toc222620524)

[11.1.2) UC-002: ACTIVAR MANUALMENTE 172](#_Toc222620525)

[11.1.3) UC-006: BLOQUEAR DISPOSITIVO 175](#_Toc222620526)

[11.1.4) UC-007: MOSTRAR VENTANA DE CANCELACIÓN 177](#_Toc222620527)

[12) Bibliografía 182](#_Toc222620528)

# Glosario

**API:** Acronimo del inglés “Application Programming Interface” que traducido significa Interfaz de Programación de Aplicaciones, son un conjunto de definiciones que permiten que dos aplicaciones o componentes de software se comuniquen entre sí.

**App:** Abreviatura del inglés “Application” que traducido significa aplicación, es un programa de software diseñado para realizar un grupo específico de funciones, tareas o actividades para el beneficio del usuario.

**Auth:** Abreviatura del inglés “Authentication” que significa autenticación, es el proceso de verificar la identidad de un usuario, sistema o entidad.

**CdM:** Abreviatura de “Centro de Monitoreo”, es el área encargada de la supervisión y gestión de las situaciones de emergencia, donde se encuentran los usuarios, dando soporte tanto a usuarios como a autoridades competentes, notificando y coordinando las acciones conjuntas para socorrer al usuario en situaciones de peligro.

**GPS:** Acrónimo del inglés “Global Positioning System” que traducido significa Sistema de Posicionamiento Global, este es un sistema de navegación por satélite que proporciona información sobre ubicación, velocidad y hora sincronizada en cualquier punto de la Tierra.

**I+D+I:** Significa “Investigación, Desarrollo e Innovación”, es la designación del área del organigrama, responsable de aumentar el conocimiento en la empresa, aplicar ese conocimiento en nuevos productos o procesos, y lograr la introducción exitosa de novedades en el mercado.

**IMEI:** Acrónimo del inglés “International Mobile Equipment” y que se traduce como Identidad Internacional de Equipo Móvil, es un número único de 15 dígitos que identifica a cada dispositivo móvil a nivel mundial.

**PIN:** Acrónimo del inglés “Personal Identification Number” que se traduce como Número de Identificación Personal, este es un código numérico secreto, corto, utilizado para autenticar a un usuario en un sistema

**SO:** Abreviatura de Sistema Operativo, es el software principal que gestiona el hardware de un ordenador o dispositivo móvil.

**Timeout:** Palabra del inglés que se traduce como Tiempo de Espera Agotado, es un evento que ocurre cuando un proceso o solicitud se detiene porque ha pasado un período de tiempo predeterminado sin recibir una respuesta. Se utiliza para evitar que los sistemas queden eternamente a la espera de una respuesta que podría no llegar.

**Timestamp:** Palabra del inglés que se traduce como Marca de Tiempo, es una secuencia de caracteres que representa la fecha y/o hora. Es crucial para registrar el momento exacto de una transacción, error o cualquier dato, permitiendo auditoría y orden cronológico.

**UI:** Acrónimo del inglés “User Interface” que significa Interfaz de Usuario, y puede ser entendido como el punto de interacción entre un usuario y un dispositivo, aplicación o sitio web. Incluye todos los elementos (pantallas, botones, menús, iconos) que permiten al usuario operar el sistema de manera efectiva e intuitiva.

# Datos del Negocio

## Descripción y Posicionamiento de la Empresa

Securion Argentina es una empresa dedicada a la provisión de servicios de seguridad privada. Opera como una entidad comercial que gestiona recursos humanos (personal de vigilancia, supervisores, técnicos), tecnológicos (sistemas de alarmas, CCTV, control de accesos) y logísticos para brindar soluciones de protección integral a sus clientes.

Opera en todas las provincias Argentinas y cuenta con más de 10000 colaboradores entre sus filas. Entre sus clientes se pueden mencionar Supermercados COTO, empresas de Logística y entidades gubernamentales.

Su posicionamiento estratégico se basa en ser un socio confiable y proactivo, destacándose por la integración de tecnología de punta con personal altamente capacitado y seleccionado.

Busca diferenciarse mediante la calidad del servicio, la capacidad de respuesta, la adaptación a las necesidades específicas de cada cliente (empresas, industrias, instituciones, residencias) y un enfoque preventivo, posicionándose como un referente en innovación y confiabilidad dentro del rubro.

## Nombre de la Empresa

El nombre comercial de la empresa es Securion Argentina.

Se fundó en el año 1995 como filial de Securitas AB (Suecia), y luego del traspaso al Holding SECAR Security Group, paso a llamarse como se la conoce actualmente.

## Rubro del Negocio

La empresa opera dentro del rubro de la Seguridad Privada. Este sector engloba todas las actividades destinadas a proteger personas, bienes muebles e inmuebles, e información, mediante servicios prestados por empresas privadas, complementando o supliendo la seguridad pública.

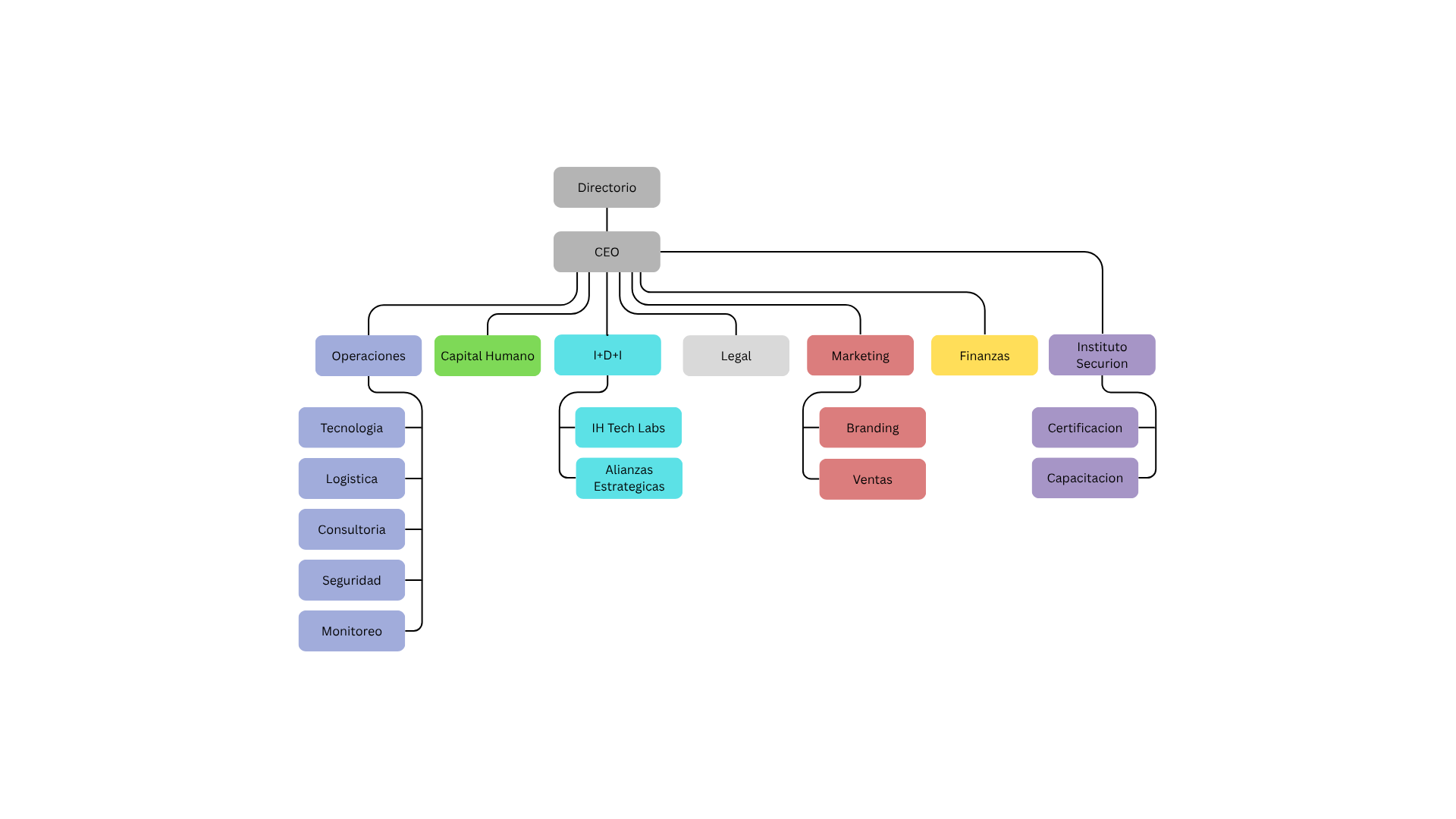
Servicios que brinda la empresa

* *Securion Security: Vigilancia física, custodia de bienes, respuesta armada, monitoreo 24/7.*
* *Securion Technology: Sistemas de CCTV con IA, control de accesos biométricos, seguridad perimetral.*
* *Securion Consult: Auditorías de riesgo, planificación de continuidad operativa, ciberseguridad.*
* *Vigilan Alarmas: Alarmas residenciales/comerciales con app móvil.*
* *Trailback: Logística segura con geolocalización satelital para transporte de valores.*

## Domicilio de la Empresa

* *Casa Central:* Av. Corrientes 2037, Ciudad Autónoma de Buenos Aires.
* *Centros operativos:*
  + *Tecnología:* Parque Industrial Pilar, Buenos Aires.
  + *Monitoreo:* Av. del Libertador 6185, CABA*.*
* *Sede Córdoba:* José Roque Funes 1642. Tel: 0351-4814741

## Organigrama



Imágen 2‑1 Organigrama de Securion

**Descripción de las Áreas de la empresa**

* **CEO:** Define la visión de la empresa, aprueba presupuestos, toma decisiones estratégicas, supervisa a todos los directores.

Se reúne con Alianzas Estratégicas para planificación, con Finanzas para control presupuestario, y con I+D+I para impulsar la innovación.

* **Operaciones**: Coordina guardias, patrullas, respuesta a incidentes, gestiona turnos, supervisa el desempeño en campo.

Recibe reportes de Monitoreo, solicita recursos a Logística, y prueba nuevas tecnologías con I+D+I**.**

* **Capital Humano:** Se encarga de la contratación del personal, gestión de nóminas, beneficios laborales, mejoramiento continuo del clima laboral y resolución de conflictos internos.

Coordina con Capacitaciónpara entrenamientos, con Legalpara temas contractuales, y apoya a todos los departamentos en reclutamiento.

* **I+D+I (Investigación, Desarrollo e Innovación):** Investiga nuevas tecnologías desarrolla prototipos, mejora procesos existentes.

Trabaja con Tecnología para implementar desarrollos, con InstitutoSecuíron para validar métodos, y con Marketing para lanzar innovaciones.

* **Legal**: Redacta contratos con clientes y proveedores, vela por el cumplimiento legal, gestiona riesgos jurídicos.

Asesora al área de Alianzas Estrategicas sobre acuerdos a realizar, apoya a Certificación en normativas, y protege patentes con I+D+I.

* **Marketing**: Diseña campañas publicitarias, gestiona redes sociales, genera leads, investiga mercado.

Colabora con Ventas para estrategias comerciales, con Branding para identidad visual, y con I+D+I para novedades tecnologicas.

* **Finanzas**: Se encarga de la contabilidad general de la empresa, movimiento de flujo de caja, redactar presupuestos, informes financieros y consolidar inversiones.

Proporciona datos a CEO, gestiona cobros con Ventas, y aprueba fondos para I+D+Iy Logística.

* **Instituto Secuíron:** Investiga tendencias en seguridad, diseña programas de formación avanzada, certifica competencias.

Entrena a personal de Operaciones y Seguridad, y desarrolla contenidos con I+D+I.

* **Tecnología**: Desarrolla software de seguridad, gestiona sistemas de comunicación, soporte técnico interno.

Implementa soluciones para Monitoreo, colabora con IT | Tech Labs en infraestructura, y ejecuta proyectos de I+D+I**.**

* **IT | Tech Labs**: Se encarga del manteimiento de servidores, configuración de redes, ciberseguridad interna, prueba hardware/software nuevo.

Depende de Tecnología, da soporte a Certificación y Monitoreo, y prueba equipos para I+D+I**.**

* **Branding**: Desarrolla la identidad de marca, define lineamientos gráficos, supervisa material corporativo.

Alinea estrategias con Marketing, y asegura coherencia en Alianzas Estratégicas.

* **Certificación**: Audita procesos, asegura cumplimiento de normas (ISO, NOM), certifica servicios.
* **Comunicación**: Verifica estándares en Operaciones, valida métodos de I+D+I, y se apoya en Legal para requisitos.
* **Alianzas Estratégicas**: Identifica socios estratégicos, negocia convenios, gestiona relaciones con partners, analiza mercado, planea expansión, evalúa competencia, propone nuevos negocios.

Coordina con Ventas para oportunidades conjuntas, y con Legal para contratos.

* **Ventas**: Prospecta clientes, cierra contratos, da seguimiento post-venta, elabora cotizaciones.

Recibe leads de Marketing, diseña soluciones con Consultoría, e informa a Finanzas de ingresos.

* **Capacitación**: Entrena a guardias y técnicos, evalúa competencias, actualiza cursos.

Se apoya en Instituto Secuíron para contenido avanzado, y coordina con CapitalHumano para onboarding.

* **Logística**: Gestiona inventario, transporte, uniformes, equipos de seguridad, almacenes.

Abastece a Operaciones, coordina con Seguridad para necesidades en campo, y presupuesta con Finanzas.

* **Consultoría**: Asesora clientes en diseño de seguridad, realiza diagnósticos, propone soluciones a medida.

Trabaja con Ventas en propuestas, solicita soporte técnico a I+D+I, y se apoya en Legal para contratos.

* **Seguridad**: Diseña protocolos de actuación, gestiona riesgos, investiga incidentes, supervisa estándares.

Define procedimientos con Operaciones, recibe alertas de Monitoreo, y actualiza métodos con I+D+I.

* **Monitoreo**: Vigila en tiempo real con la ayuda de cámaras y alarmas, reporta incidentes, coordina respuestas con campo.

Notifica a las áreas de Operaciones y Seguridad, reporta fallas a Tecnología, y prueba nuevas herramientas conI+D+I**.**

## Misión, Visión, Políticas, Objetivos, Metas y Factores de Éxito

* **Misión:***“Proteger a las personas, los bienes, los lugares de trabajo y la sociedad”*

Securion se enfoca en garantizar seguridad integral mediante soluciones innovadoras y personalizadas, manteniendo un compromiso con la calidad y la confianza tras más de 30 años de experiencia.

* **Visión**: *“Llevar a la seguridad privada a un modelo de beneficios mutuos para trabajadores, clientes y accionistas”.*

Posicionarse como líder en evolución tecnológica y servicios de seguridad en Argentina, enfrentando futuros desafíos con soluciones adaptadas.

* **Valores Fundamentales**

*Transparencia:* Integridad en procesos y comunicación clara para generar confianza.

*Eficiencia:* Optimización de recursos, uso de tecnología avanzada y capacitación para respuestas efectivas.

*Eficacia:* Diseño de esquemas de protección personalizados, combinando capacidad operativa y competencias técnicas.

* **Políticas Clave**

*Innovación Tecnológica:* Inversión sostenida en IA, robótica y monitoreo predictivo para optimizar respuestas ante emergencias y reducir riesgos operativos, asegurando servicios adaptados a diferentes.

*Capital Humano y Diversidad:* Política de igualdad de oportunidades sin distinción de género, raza o religión, combinada con programas de capacitación técnica y en derechos humanos para todos sus empleados.

*Ética y Cumplimiento:* Adhesión a estándares internacionales (OIT) y certificaciones como ISO 37001 (antisoborno). Operativizada mediante la Línea Ética para denuncias y auditorías externas periódicas.

*Sostenibilidad Ambiental:* Reducción de emisiones de CO₂ en logística, certificaciones IRAM 3501 para prevención de incendios, y alineación con ISO 14001 para minimizar impacto ecológico.

* **Objetivos y Metas**

*Innovación Tecnológica:* Desarrollar soluciones de seguridad electrónica, remota y móvil para adaptarse a necesidades emergentes.

*Expansión de Servicios:* Consolidar portafolios como Protección Contra Incendios, Gestión de Riesgos Corporativos y Seguridad Especializada.

*Capacitación Continua:* Programas de formación para empleados, asegurando altos estándares operativos.

*Satisfacción del Cliente:* Brindar asesoría 24/7 y soluciones a medida mediante Centros de Experiencia.

* **Factores Críticos de Éxito (FCE)**

Tecnología integrada: Uso de IoT e inteligencia artificial para optimizar respuestas y minimizar riesgos.

Talento comprometido: Retención de personal mediante desarrollo profesional y condiciones laborales justas.

Adaptabilidad: Evolución continua frente a cambios regulatorios y demandas del mercado.

Gobernanza ética: Transparencia en la gestión, con auditorías externas y alianzas estratégicas que aseguran confianza a largo plazo.

## Oportunidades de Negocio

* **Oportunidades Estratégicas**: Una aplicación de seguridad móvil le permite a la empresa penetrar mercados móviles desatendidos: trabajadores en riesgo (repartidores, técnicos), grupos vulnerables (mujeres en tránsito, adultos mayores) y turistas. Esto diversifica su negocio más allá de la seguridad estática (hogares/empresas), posicionándolo como protector integral en movilidad. Además, puede en el futuro integrar la aplicación con sus servicios actuales (alarmas, monitoreo 24/7), creando un ecosistema unificado donde clientes residenciales y corporativos extienden su protección “fuera de muros”, fidelizando usuarios y reduciendo rotación.
* **Alianzas y Datos como Ventaja**: La tecnología puede habilitar colaboraciones disruptivas: con municipios para programas de “ciudades seguras” (botones de pánico público), empresas de delivery (seguridad como beneficio laboral) y aseguradoras (pólizas basadas en prevención). Paralelamente, los datos anónimos de incidentes generan mapas de calor del delito, útiles para optimizar patrullas, crear alertas predictivas y vender insights a sectores públicos/privados.
* **Diferenciación Final**: La empresa se distingue al ofrecer respuesta integrada única: activación silenciosa + centro de monitoreo propio + vinculación con autoridades.
* Esto lo posicionaría como líder en seguridad humano-digital, atrayendo clientes que buscan soluciones beyond hardware y transformando su modelo de protección física en cobertura contextual 360°.

## Entorno de usuarios

El sistema de alarma móvil se integra con el tejido operativo de Securion, estableciendo relaciones funcionales con diversas áreas del negocio que garantizan su efectividad. Estas interacciones conforman un ecosistema donde cada componente desempeña roles complementarios:

*Interfaces operativas crítica:* La Central de Monitoreo 24/7 constituye el núcleo de la respuesta inmediata. Este departamento recibe las alertas validadas, analiza las evidencias multimedia en tiempo real y activa los protocolos de coordinación con las fuerzas de seguridad corrspondiente a la ubicación del hecho.

*Soporte técnico y continuidad:* El Departamento de Tecnología sostiene la infraestructura crítica: administra servidores, garantiza la conectividad entre la aplicación y los sistemas heredados y resuelve incidencias técnicas. Los equipos de Desarrollo y Mantenimiento implementan actualizaciones periódicas, adaptan funcionalidades a normativas cambiantes y optimizan el consumo de recursos móviles, asegurando la evolución del sistema.

*Gestión estratégica y comercial:* El área de Marketing posiciona la solución en el mercado, diseñando paquetes integrados para clientes residenciales y corporativos. La Gerencia de Producto define su hoja de ruta, equilibrando innovación con rentabilidad, mientras Legal y Cumplimiento vela por la adhesión a la Ley 25.326 de Protección de Datos, particularmente en el manejo de evidencias sensibles y geolocalización.

*Vinculaciones externas esenciales:* El sistema se extiende fuera de la organización al conectar con fuerzas policiales y de emergencia, que reciben alertas validadas para movilización operativa. Clientes corporativos , pueden incorporan la solución en sus esquemas de protección laboral, mientras los usuarios finales son los protagonistas del ciclo de seguridad, activando alertas y recibiendo asistencia.

## Necesidades principales de la empresa

La decisión de Securion de desarrollar una app de seguridad móvil responde a una combinación de necesidades estratégicas, evoluciones del mercado y oportunidades tecnológicas.

*Adaptación a nuevas demandas del mercado:* Los usuarios ya no buscan solo seguridad en sus hogares, sino protección en su movilidad (calles, transporte, viajes).

*Competencia en un mercado saturado*: Diferenciarse de empresas locales de seguridad tradicionales y de nuevas startups tecnológicas.

*Fidelización de clientes existentes:* Reducir la tasa de abandono de clientes que buscan soluciones más integrales.

*Presión por innovación tecnológica:* Mantener relevancia en un sector donde la IA, el IoT y el 5G están revolucionando la seguridad.

*Alianzas estratégicas con el sector público:* Posicionarse como un actor clave en seguridad pública para acceder a contratos estatales.

## Alternativas y Competencia

*Alternativas básicas y limitadas:* Las aplicaciones antirrobo tradicionales son tenidas en cuenta por el usuario como alternativas inmediatas, pero estas alternativas fallan por su falta de discreción: emiten sonidos fuertes que alertan al agresor y carecen de funciones críticas como notificación a la policía y/o contactos o captura de evidencias multimedia. Su principal ventaja es la simplicidad y bajo consumo de recursos, pero resultan insuficientes en emergencias físicas donde la discreción es vital.

*Soluciones comunitarias y botones de pánico:* Plataformas como SOSAFE o Botón de Auxilio ofrecen redes de apoyo mediante geolocalización y alertas manuales. Sin embargo, su dependencia de acciones visibles limita su utilidad en situaciones de agresión súbita. Los usuarios valoran su enfoque colaborativo, pero señalan debilidades clave: imposibilidad de activación por gestos/voz, cobertura irregular sin internet y ausencia de comunicación automática con centros de monitoreo profesional.

*Sistemas con hardware costoso:* Alternativas como ALARA (joyas inteligentes) o servicios de monitoreo (Medical Guardian) atraen por su portabilidad física y detección de caídas, pero no son económicas para los usuarios (hasta $40/mes) y dependencia de dispositivos adicionales. Aunque percibidos como robustos, no resuelven necesidades centrales: falta integración policial automática, no capturan evidencias (audio/fotos) y su alcance se restringe a quienes pueden costearlos.

*Vacío competitivo y ventaja de Securion:* Frente a estas alternativas, los usuarios identifican un vacío: soluciones accesibles (sin hardware), con activación discreta (voz/gestos), resiliencia offline (SMS, almacenamiento local) y respuesta coordinada con autoridades. Esta aplicacion destaca al unir cuatro elementos ausentes en competidores:

* Activación silenciosa por patrones personalizados
* Evidencias multimedia automáticas (fotos/audio)
* Funcionamiento sin internet/localización
* Protocolos post-emergencia (encuestas), todo sin costos adicionales

posicionándose como una solución integral y económicamente accesible.

## Precedencia y Prioridad

*Precedencia del Proyecto:* Securion identifica una necesidad crítica en seguridad móvil, ya que su oferta actual se limita a protección física en hogares y empresas. El aumento de incidentes en espacios públicos (robos a repartidores, violencia de género) y la falta de competidores locales con respuesta integrada (app + vigilancia física) crean la oportunidad perfecta para desarrollar esta solución. La empresa cuenta con ventajas clave: infraestructura de monitoreo subutilizada, red de vigilantes operativa y certificaciones legales, pero carece de una plataforma digital que conecte estos recursos con usuarios en movimiento.

*Prioridad Estratégica:* El proyecto es de alta urgencia (12-18 meses) para evitar que competidores globales dominen el mercado argentino. Representa una triple ganancia para Securion:

Diversifica ingresos con suscripciones de usuarios finales y clientes corporativos

Optimiza recursos existentes, aumentando el uso de su centro de monitoreo

Posiciona la marca como innovadora al ofrecer el primer servicio de protección física-digital del país.

Su implementación debe comenzar con un piloto en CABA y Córdoba para validar el modelo antes del escalamiento nacional.

# Datos del Proyecto

## Descripción del Proyecto a desarrollar

El proyecto a realizar es una aplicación móvil de seguridad personal para smartphones, que opera como una alarma silenciosa -en segundo plano-, diseñada para responder ante situaciones de robo o agresión física.

El modo de alarma se activa mediante un comando de voz predefinido, un gesto específico o un patrón configurado por el usuario. Tras la activación, el sistema bloquea temporalmente el dispositivo y, después de un intervalo de quince segundos —permitiendo al usuario cancelar en caso de falsa activación—, emite notificaciones a los contactos designados a través de aplicaciones de mensajería (WhatsApp, Telegram, SMS u otras) o redes sociales. Estas notificaciones alertan sobre la situación de riesgo e incluyen la última ubicación registrada del usuario.

Simultáneamente, el sistema envía una notificación al Centro de Monitoreo, que recibe los datos del usuario y la ubicación en tiempo real del dispositivo, facilitando el aviso a las autoridades competentes. Durante el estado de alarma, la aplicación captura audio ambiental en segundo plano y toma fotografías con las cámaras delantera y trasera —siempre que exista un mínimo de luz ambiental—, transmitiendo estos datos al Centro de Monitoreo mientras el nivel de batería no supere un umbral mínimo configurable.

En escenarios sin conectividad a internet o con la geolocalización deshabilitada, el sistema recurrirá a la triangulación mediante redes móviles para localizar el dispositivo y enviar un SMS al Centro de Monitoreo y/o al destacamento policial más cercano a la última ubicación conocida. Si la transmisión inmediata no es posible, los datos se almacenan localmente y se envían automáticamente al restablecerse la conexión.

El modo de alerta permanecerá activo hasta que el usuario desbloquee el dispositivo manualmente. Al desbloquear el teléfono, se presentará un cuestionario para recabar detalles sobre el incidente: motivo de la alarma, estado de la persona y respuesta de las autoridades.

La aplicación debe ser compatible con sistemas operativos Android e iOS.

Durante el primer uso, el usuario debe registrarse y proporcionar información personal (nombre, dirección) y de contactos de emergencia (nombre, número telefónico y aplicación de mensajería preferida). Adicionalmente, si el dispositivo se apaga durante el estado de alarma, al reiniciarse se restablece automáticamente el modo de alarma y la conexión con el Centro de Monitoreo, manteniendo este estado hasta que el usuario desbloquee el teléfono.

El Centro de Monitoreo dispondrá de una plataforma web para visualizar alarmas en tiempo real, consultar su historial (origen, hora de activación, finalización, estado) y verificar la notificación a autoridades, así como los motivos reportados.

Este sistema constituye una solución autónoma de protección que integra discreción, respuesta inmediata y respaldo profesional, manteniendo operatividad en condiciones adversas como falta de conectividad, batería crítica o reinicios forzados.

## Objetivos y Alcances del Proyecto

*Objetivos del Proyecto:* El proyecto busca desarrollar una aplicación móvil de seguridad personal para complementar los servicios actuales de Securion, permitiendo a usuarios activar alertas discretas ante emergencias mediante comandos de voz, gestos o patrones.

Sus objetivos específicos incluyen:

* Integrarse con la central de monitoreo existente,
* Garantizar funcionamiento offline mediante SMS,
* Recolectar evidencias digitales (audio/fotos cuando sea posible) y cumplir con la normativa de protección de datos.
* Además, se enfoca en ser escalable para su adopción por empresas y gobiernos como parte de programas de seguridad.

*Alcance del Proyecto:* El desarrollo abarca una app nativa para Android e iOS con geolocalización en tiempo real, alertas a contactos y autoridades, y un panel web de gestión. Sin embargo, excluye hardware adicional (como wearables), ampliación de infraestructura física o garantías de respuesta policial (dependiente de terceros). La primera fase se centrará en un MVP con funciones básicas, pilotado en CABA y Córdoba, dejando para etapas posteriores integraciones avanzadas como heatmaps de riesgo o IA predictiva.

*Enfoque y Prioridades:* El equilibrio entre innovación y factibilidad es clave: se prioriza el funcionamiento en segundo plano y el cumplimiento legal de privacidad. El proyecto apunta a cerrar la brecha de seguridad móvil de Securion, aprovechando su infraestructura actual sin sobrecargar operaciones. El éxito se medirá mediante pruebas piloto, con escalamiento según resultados, posicionando a Securion como líder en protección física-digital integrada.

*Jusitificacion del proyecto:* Para la empresa de seguridad, este proyecto no es solo el desarrollo de una aplicación móvil. Es un proyecto estratégico de transformación digital que le permite:

1. Diversificar su cartera de servicios hacia un mercado no explotado (seguridad personal).
2. Añadir un valor diferencial alto que justifique precios premium.
3. Modernizar su infraestructura de monitoreo.
4. Fidelizar a su clientela actual y atraer nueva con un servicio integral.
5. Optimizar sus operacionesy reducir costos asociados a falsas alarmas.
6. Abrir flujos de ingresos recurrentes adicionales y sostenibles.

La inversión en el desarrollo de este sistema se justifica plenamente por su potencial para consolidar el liderazgo de la empresa en el sector de la seguridad y asegurar su crecimiento futuro en la era digital.

## Características Técnicas del Proyecto

### Arquitectura

El sistema empleara una arquitectura de microservicios para garantizar escalabilidad y resiliencia. El frontend móvil (Angular/Ionic) se comunicará con un backend modularizado en Spring Boot, donde servicios autónomos gestionaran funciones críticas:

* *Alert-Gateway*: Punto único de entrada con autenticación OAuth2.
* Geo-Locator: Geolocalización GPS/triangulación celular vía OpenCellID.
* *Evidence-Processor*: Cifrado de datos (AES-256) y almacenamiento de evidencias.
* *Comms-Orchestrator:* Manejo de notificaciones multicanal (SMS, WhatsApp, Telegram, etc).

### Funcionalidades Clave

* Activación silenciosa: Por voz, gestos o patrones con bloqueo temporal.
* Evidencias multimedia: Captura automática de audio/fotos.
* Persistencia tras reinicios.
* Comunicación redundante:
* *Online:* WebSockets para tracking en tiempo real.
* *Offline*: SMS con triangulación OpenCellID y sincronización diferida.
* Panel de monitoreo: Visualización de alertas en mapas y gestión de incidentes.

### Seguridad y Rendimiento

* Protección de datos:
  + Cifrado TLS 1.3 (tránsito) y AES-256 (almacenamiento).
  + Cumplimiento Ley 25.326 (consentimientos explícitos y auditorías).
* Rendimiento garantizado:
  + Procesamiento de alertas menor a 3 segundos.
  + Escalado automático con Kubernetes.
* Operación en Entornos Adversos
  + Batería baja: Funciones esenciales operan hasta 15% de carga.
  + Sin conexión: Almacenamiento local cifrado y envío diferido..

### Ventajas Técnicas

* *Alta disponibilidad:* Los microservicios al estar aislados evitan fallos en cascada.
* *Actualizaciones continuas:* Posibilidad de despliegues independientes sin necesidad de bajar los servicios.
* *Escalabilidad económica*: Servicios como Comms-Orchestrator pueden escalar según demanda.

## Metodología a utilizar

La metodología a utilizar será el *Proceso Unificado de Desarrollo de Software* (PUDS), en un desarrollo iterativo e incremental, entregando un MVP al final de cada iteración.

Esta metodología se adopta por su idoneidad técnica para sistemas de alta criticidad como esta alarma personal, donde la precisión en la gestión de riesgos, la documentación auditable y la integración rigurosa con sistemas heredados son determinantes.

## Software de desarrollo

* Frontend: Angular + Ionic, Capacitor, RxJS. Permite el desarrollo híbrido (iOS/Android) con acceso nativo a sensores.
* Backend: Spring Boot (java), Spring Data JPA, Spring Security.
* Base de datos: PostgreSQL + PostGIS. Escalabilidad, seguridad y manejo eficiente de concurrencia. (Server-side). SQLite (nativa del front-end)
* Comunicación: REST API (JSON), WebSockets. Para tener una mayor sincronización en tiempo real para tracking.
* Infraestructura Dev/Ops: Docker, GitHub, Kubernetes
* APIs/Servicios Externos: OpenCellId (Triangulacion de redes mobiles), Google Cloud Speech-to-text (para convertir audio a texto), Google Maps (para la UI)

## Lista y descripción de las funcionalidades que abarca el sistema

* *Activación de Alarma mediante Palabra Clave:* Reconocimiento de voz en segundo plano para activar la alarma al detectar una frase predefinida por el usuario.
* *Activación de Alarma mediante Gestos o Movimientos:* Detección de movimientos bruscos (ej. sacudida violenta) o gestos personalizados (ej. triple toque en la pantalla).
* *Activación mediante Patrón Personalizado:* Configuración de un patrón táctil secreto en pantalla bloqueada para activar el modo de emergencia.
* *Bloqueo Automático del Teléfono al Activar la Alarma:* Inhabilitación temporal del desbloqueo del dispositivo tras la activación de la alarma.
* *Ventana de Cancelación de 5 Segundos:* Permite al usuario desactivar la alarma mediante autenticación biométrica, contraseña o patrón, antes de enviar alertas.
* *Notificación Multicanal a Contactos de Emergencia:* Envío automático de mensajes (WhatsApp, SMS, Telegram, etc.) a contactos designados, incluyendo ubicación y mensaje predefinido.
* *Alerta en Tiempo Real al Centro de Monitoreo:* Transmisión de datos del usuario (nombre, dirección) y ubicación GPS en tiempo real al centro de monitoreo.
* *Grabación de Audio en Segundo Plano:* Captura continua de audio ambiental durante la alarma, con almacenamiento en la nube o envío al centro de monitoreo.
* *Captura Automática de Fotos con Cámaras Frontal/Trasera:* Toma de fotos periódicas mientras haya luz suficiente, priorizando el ahorro de batería.
* *Gestión de Batería Baja:* Parámetros configurables para suspender funciones intensivas (ej. Fotos, audio) si la batería cae bajo un umbral definido.
* *Geolocalización por Red Celular (sin GPS):* Estimación de ubicación mediante torres de telefonía o Wi-Fi si el GPS está desactivado o no hay conexión a internet.
* *Envío de SMS de Emergencia a Autoridades:* Envío automático de SMS a números de emergencia cercanos (ej. destacamento policial) si no hay internet.
* *Almacenamiento Local y Reintento de Envío:* Guardado de datos (audio, fotos, ubicación) en LocalStorage cuando no hay conexión, con reenvío automático al recuperarla.
* Persistencia de la Alarma tras Reinicio: Reanudación del modo de emergencia al reiniciar el teléfono, evitando que el atacante detenga la alarma apagando el dispositivo.
* Cuestionario Post-Alarma: Encuesta post-evento para registrar motivo de activación, estado del usuario, intervención de autoridades, etc.
* Registro y Autenticación de Usuario: Flujo de registro/login inicial con validación de identidad (correo, teléfono, o redes sociales).
* Gestión de Perfil y Contactos de Emergencia: Configuración de datos personales (nombre, dirección) y selección de contactos con preferencias de comunicación.
* Dashboard Web para el Centro de Monitoreo: Plataforma web con mapa interactivo, historial de alertas, estado en tiempo real, y registro de acciones tomadas (ej. aviso a policía).
* Compatibilidad Multiplataforma (Android/iOS): Desarrollo nativo o con frameworks cross-platform para garantizar funcionalidad equivalente en ambos sistemas operativos.
* Notificación a Autoridades: Protocolo automatizado para que el centro de monitoreo contacte a policía.
* Modo Sigiloso: Ocultar ícono de la app y desactivar notificaciones visibles durante la alarma.
* Historial de Alarmas para el Usuario: Acceso a un registro local/remoto de activaciones pasadas y respuestas.

# Planeamiento

## Organización del proyecto

Dado que se trata de un proyecto llevado a cabo por una única persona, esta se convierte en un profesional multidisciplinar, debiendo desempeñar las tareas y asumir las responsabilidades de diversos puestos. La esencia, en este caso, no son las etiquetas de los roles, sino el cumplimiento efectivo de la totalidad de sus funciones.

### Listado de Roles

|  |  |
| --- | --- |
| **Jefe de Proyecto** | |
| **Responsabilidades** | **Actividades** |
| * Planificación general y control del proyecto * Gestión de riesgos y toma de decisiones * Coordinación entre roles técnicos * Seguimiento de cronograma y entregables | * Definir plan de proyecto y cronograma PUDS * Gestionar entregables por iteración * Monitorear avance según matriz de casos de uso * Coordinar integración entre módulos * Gestionar cambios en alcance |

|  |  |
| --- | --- |
| **Arquitecto de Software** | |
| **Responsabilidades** | **Actividades** |
| * Diseño de arquitectura del sistema * Selección de tecnologías y patrones * Garantizar coherencia técnica * Definir estándares de desarrollo | * Diseñar arquitectura por módulos * Especificar integración entre componentes * Definir estrategias de persistencia y comunicación * Establecer patrones de seguridad * Validar viabilidad técnica de casos de uso |

|  |  |
| --- | --- |
| **Analista de Requerimientos** | |
| **Responsabilidades** | **Actividades** |
| * Especificación y documentación de requerimientos * Validación de completitud funcional * Traducción de necesidades a especificaciones técnicas | * Elaborar y mantener matriz de casos de uso * Especificar detalles de cada Caso de Uso * Validar cobertura de Caso de Uso de Negocio por Caso de Uso * Documentar reglas de negocio * Priorizar requerimientos por iteración |

|  |  |
| --- | --- |
| **Diseñador de Software** | |
| **Responsabilidades** | **Actividades** |
| * Diseño detallado de componentes * Especificación de interfaces * Modelado de datos y procesos | * Diseñar componentes por módulo * Modelar esquema de base de datos * Especificar APIs y contratos de servicio * Diseñar interfaces de usuario * Documentar diseños técnicos |

|  |  |
| --- | --- |
| **Desarrollador de Software** | |
| **Responsabilidades** | **Actividades** |
| * Implementación de componentes según diseño * Pruebas unitarias y documentación de código * Resolución de problemas técnicos | * Implementar casos de uso según especificación * Desarrollar frontend móvil y web * Programar servicios backend * Integrar APIs externas * Realizar pruebas unitarias |

|  |  |
| --- | --- |
| **QA & Tester** | |
| **Responsabilidades** | **Actividades** |
| * Verificación de calidad del software * Validación de cumplimiento de requerimientos * Detección y reporte de defectos | * Elaborar plan de pruebas por caso de uso * Ejecutar pruebas funcionales e integrales * Validar cumplimiento de requerimientos * Reportar y seguir defectos * Validar performance y usabilidad |

|  |  |
| --- | --- |
| **Documentador** | |
| **Responsabilidades** | **Actividades** |
| * Elaboración de documentación técnica y de usuario * Mantenimiento de artefactos del proyecto * Gestión de conocimiento | * Documentar arquitectura y diseño * Elaborar manuales de usuario * Mantener matriz de casos de uso actualizada * Gestionar repositorio de documentación * Preparar entregables formales |

|  |  |
| --- | --- |
| **Administrador de Configuración** | |
| **Responsabilidades** | **Actividades** |
| * Gestión de versiones y entornos * Control de cambios * Garantizar trazabilidad | * Gestionar control de versiones * Administrar entornos de desarrollo y pruebas * Controlar cambios en requerimientos * Mantener trazabilidad UCN-UC * Gestionar releases y versiones |

|  |  |
| --- | --- |
| **Administrador de Configuración** | |
| **Responsabilidades** | **Actividades** |
| * Instalación y configuración en producción * Capacitación a usuarios finales * Soporte post-implementación | * Planificar estrategia de despliegue * Configurar ambientes productivos * Capacitar usuarios y operadores * Dar soporte inicial post-implementación * Monitorear operación inicial |

## Lista de Entregables

**MVP 1 - Núcleo de Seguridad (Meses 1-2)**

**Objetivo:** Sistema básico de activación y notificación

**Entregable MVP 1:**

* App móvil con activación manual básica
* Notificaciones SMS a contactos
* Backend con API REST funcional
* Dashboard web mínimo para visualizar alarmas entrantes
* Base de datos PostgreSQL básica

**MVP 2 - Métodos Avanzados & Evidencias (Meses 3-4)**

**Objetivo:** Ampliar métodos de activación y captura de evidencias

* Entregable MVP 2:
* Activación por voz y patrón
* Captura de audio y fotos
* Dashboard CdM operativo
* Sistema de autenticación completo

**MVP 3 - Resiliencia & Optimización (Meses 5-6)**

**Objetivo:** Robustez y características avanzadas

**Entregable MVP 3:**

* Persistencia tras reinicio
* Optimización de batería
* Geolocalización por red celular
* Sistema completo de gestión CdM

## Planifiación

### Iteración I: Núcleo de Seguridad

* **Objetivo:** Sistema básico de activación, bloqueo y notificación.
* **Tiempo estimado:** 8 semanas (semana 1 a 18)

1. **Relevamiento & Análisis** 
   * Definir alcance MVP1 con UC priorizados.
   * Análisis de APIs: SMS, Google Maps.
   * Análisis de permisos móviles críticos (GPS, background)
   * Documento de Especificaciones Técnicas v1.
2. **Diseño** 
   * Wireframes: pantallas de registro, configuración, activación.
   * Diseño base de datos: tablas Usuarios, Alarmas, Contactos.
   * Diseño API REST para alertas y usuarios.
   * Prototipo de UI en Figma. Diagrama ER. Esquema de APIs.
3. **Implementación** 
   * Backend: Desarrollo Spring Boot con APIs de Usuario, Alarma.
   * App: Pantallas de registro y configuración.
   * Funcionalidad Core: Lógica de activación por presión manual, bloqueo, ventana de cancelación.
   * Integración: Servicio de ubicación GPS y envío de SMS.
   * Código fuente funcional.
   * App instalable en Alpha.
   * APIs desplegadas.
4. **Pruebas** 
   * Pruebas unitarias.
   * Pruebas de integración: Flujo completo de alarma.
   * Pruebas en dispositivo real: consumo de batería, permisos.
   * Informe de pruebas.
   * App Beta estable.
5. **Despliegue & Retro** 
   * Despliegue backend en entorno de pruebas
   * Publicación de app en canal Beta.
   * Recopilación de feedback inicial.
   * MVP 1 Operativo: Sistema básico funcionando.

### Iteración II: Métodos Avanzados & Evidencias

* **Objetivo:** Ampliar métodos de activación e iniciar captura de evidencias.
* **Tiempo estimado:** 8 semanas (semana 9 a 16)

1. **Relevamiento & Análisis** 
   * Análisis de APIs de voz (Google Speech) y cámara.
   * Diseño de flujos de encuesta post-alarma y dashboard CdM.
   * Especificaciones Técnicas v2.
2. **Diseño** 
   * Wireframes: Dashboard web CdM, encuesta post-alarma
   * Diseño de módulo de autenticación JWT.
   * Modelado de datos para evidencias (Audio, Foto).
   * Prototipo Dashboard Web. Diseño de módulos.
3. **Implementación**
   * Backend: APIs para gestión de evidencias y autenticación.
   * Dashboard Web: Desarrollo con Angular para visualizar alertas
   * App: Activación por voz y patrón, grabación de audio.
   * Funcionalidad: Encuesta post-alarma
   * Código del Dashboard.
   * App con métodos de activación avanzados.
4. **Pruebas** 
   * Pruebas de reconocimiento de voz en diferentes ambientes.
   * Pruebas de rendimiento del dashboard web.
   * Pruebas de seguridad (autenticación JWT).
   * Informe de pruebas MVP2.
5. **Despliegue & Retro** 
   * Despliegue del dashboard web.
   * Actualización de la app en canales Beta.
   * Feedback de usuarios y operadores CdM simulados.
   * MVP2 Operativo: Sistema con evidencias y dashboard.

### Iteración III: Resiliencia y Optimización

* **Objetivo:** Robustez ante condiciones adversas y características avanzadas.
* **Tiempo estimado:** 8 semanas (semana 17 a 24)

1. **Relevamiento & Análisis**
   * Análisis de geolocalización por red celular (OpenCellID).
   * Estudio de BroadcastReceiver y servicios foreground para persistencia
   * Especificaciones Técnicas v3.
2. **Diseño**
   * Diseño de la arquitectura de reintentos y colas offline.
   * Diseño del módulo de gestión de batería.
   * Diagrama de secuencia para resiliencia.
3. **Implementación**
   * Backend: Lógica para asignación de operadores e historiales.
   * App: Activación por movimiento, reactivación tras reinicio, geolocalización offline.
   * Optimización: Lógica de gestión de batería y almacenamiento local inteligente.
   * Código de características de resiliencia.
   * App optimizada.
4. **Pruebas**
   * Pruebas de estrés: sin conexión, batería baja.
   * Pruebas de persistencia: reinicios forzados.
   * Pruebas de usabilidad final.
   * Informe final de pruebas.
   * App Release Candidate.
5. **Despliegue & Retro** 
   * Preparación para lanzamiento en tiendas (políticas de privacidad, etc.).
   * Lanzamiento oficial de la aplicación Secure-On.
   * Documentación final del proyecto.
   * PROYECTO COMPLETO: Aplicación lista para producción.

## Agenda

### Iteración I

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FASE** | **SEMANAS** | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Relevamiento |  |  |  |  |  |  |  |  |
| Análisis |  |  |  |  |  |  |  |  |
| Diseño |  |  |  |  |  |  |  |  |
| Implementación |  |  |  |  |  |  |  |  |
| Pruebas |  |  |  |  |  |  |  |  |
| Despliegue |  |  |  |  |  |  |  |  |

### Iteración II

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FASE** | **SEMANAS** | | | | | | | |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Relevamiento |  |  |  |  |  |  |  |  |
| Análisis |  |  |  |  |  |  |  |  |
| Diseño |  |  |  |  |  |  |  |  |
| Implementación |  |  |  |  |  |  |  |  |
| Pruebas |  |  |  |  |  |  |  |  |
| Despliegue |  |  |  |  |  |  |  |  |

### Iteración III

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FASE** | **SEMANAS** | | | | | | | |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| Relevamiento |  |  |  |  |  |  |  |  |
| Análisis |  |  |  |  |  |  |  |  |
| Diseño |  |  |  |  |  |  |  |  |
| Implementación |  |  |  |  |  |  |  |  |
| Pruebas |  |  |  |  |  |  |  |  |
| Despliegue |  |  |  |  |  |  |  |  |

## Lista de Riesgos

### Riesgos Técnicos

**R-01: Permisos de background en iOS**

* **Descripción:** Dificultad para obtener y mantener los permisos necesarios para que la aplicación ejecute tareas en segundo plano (como grabación de audio o geolocalización) en dispositivos iOS, debido a las estrictas políticas y limitaciones técnicas del sistema operativo.
* **Impacto:** Alto. Impacta la funcionalidad central de la aplicación, la experiencia del usuario, y la viabilidad técnica del proyecto en el ecosistema iOS.
* **Indicadores:** Alta probabilidad. Indicado por el rechazo inicial de la app durante la revisión de App Store, la imposibilidad de implementar características clave en iOS, o el cierre forzado de la aplicación por el sistema operativo durante su uso en segundo plano.
* **Estrategias de Mitigación:** Investigar en profundidad los Background Modes de Apple y las APIs permitidas (PushKit, BackgroundTasks). Diseñar la funcionalidad para alinearse estrictamente con los casos de uso aprobados por Apple y documentar su necesidad.
* **Plan de Contingencia:** Implementar un mecanismo alternativo usando notificaciones silenciosas (PushKit) para reactivar la aplicación de manera limitada, o replantear la funcionalidad para iOS como un sistema de activación manual/consciente en lugar de totalmente automático en segundo plano.

**R-02: Consumo excesivo de batería**

* **Descripción:** Las operaciones en segundo plano (micrófono, GPS, procesamiento) pueden drenar la batería del dispositivo de manera significativa, leading a una mala experiencia de usuario y a que el sistema operativo termine la aplicación.
* **Impacto:** Alto. Impacta directamente la satisfacción del usuario, la tasa de adopción y retención, y la percepción pública de la aplicación.
* **Indicadores:** Probabilidad Media. Indicado por reportes de usuarios sobre baja duración de batería, métricas anómalas de consumo en las herramientas de desarrollo, o advertencias del sistema operativo.
* **Estrategias de Mitigación:** Implementar optimizaciones agresivas: uso eficiente de WorkManager (Android) / BackgroundTasks (iOS), intervalos de muestreo adaptativos, desactivación de sensores cuando no sean estrictamente necesarios y uso de hardware de baja energía cuando esté disponible.
* **Plan de Contingencia:** Introducir un "modo de bajo consumo" configurable por el usuario que reduzca la frecuencia de monitoreo o desactive características no críticas. Ofrecer recomendaciones claras de uso al usuario.

**R-03: Reconocimiento de voz en ruido**

* **Descripción:** El algoritmo de detección de palabras clave o sonidos de alerta puede fallar en entornos ruidosos, generando falsos negativos (no detectar una emergencia) o falsos positivos (activarse por error).
* **Impacto:** Medio. Impacta la confiabilidad y precisión del sistema, pudiendo comprometer su propósito principal en situaciones críticas.
* **Indicadores:** Probabilidad Media. Indicado por pruebas en entornos ruidosos con alta tasa de error, reportes de usuarios sobre activaciones fallidas o erróneas en lugares públicos.
* **Estrategias de Mitigación:** Usar filtros de audio (reducción de ruido) y técnicas de procesamiento de señal. Combinar el reconocimiento de voz con otros métodos de activación (botón físico, detección de movimiento brusco) para crear un sistema de verificación múltiple.
* **Plan de Contingencia:** Permitir que el usuario calibre el nivel de sensibilidad del micrófono y priorizar explícitamente la activación manual como método principal, dejando la voz como un método secundario o de respaldo.

**R-04: Geolocalización sin GPS**

* **Descripción:** En interiores o zonas con mala señal, el GPS puede ser inexacto o no funcionar, impidiendo enviar la ubicación precisa del usuario en una emergencia.
* **Impacto:** Medio. Impacta la efectividad de la respuesta ante una emergencia, ya que los servicios de auxilio podrían no encontrar al usuario rápidamente.
* **Indicadores:** Probabilidad Media. Indicado por lecturas de GPS con alta desviación (alto margen de error) o la incapacidad del dispositivo para obtener una fijación satelital en pruebas de interior.
* **Estrategias de Mitigación:** Implementar un proveedor de ubicación híbrido que combine GPS, redes móviles (triangulación con torres celulares usando servicios como OpenCellId) y escaneo de redes WiFi para obtener una ubicación aproximada cuando el GPS falle.
* **Plan de Contingencia:** Enviar la última ubicación conocida con buena precisión junto con una estimación basada en red celular/WiFi. Incluir la dirección manual ingresada por el usuario en su perfil como respaldo.

**R-05: Almacenamiento de evidencias grande**

* **Descripción:** Los archivos de evidencia (audio, video, foto) pueden ocupar un espacio significativo en el dispositivo del usuario o en el servidor, aumentando costos y afectando el rendimiento.
* **Impacto:** Medio. Impacta la capacidad de almacenamiento del dispositivo del usuario, los costos operativos de almacenamiento en la nube y la velocidad de subida/descarga de datos.
* **Indicadores:** Probabilidad Baja. Indicado por un crecimiento rápido del uso de almacenamiento local o en la nube durante las pruebas, o quejas de usuarios sobre espacio en disco.
* **Estrategias de Mitigación:** Implementar compresión en tiempo real (ej., audio Opus, video H.265). Usar almacenamiento temporal y eliminar archivos antiguos después de un tiempo o después de ser procesados/validados. Ofrecer calidad ajustable.
* **Plan de Contingencia:** Limitar automáticamente la duración de las grabaciones. Dar prioridad al almacenamiento en el servidor y solo guardar en el dispositivo de manera temporal. Implementar una política de retención clara.

**R-06: Compatibilidad entre dispositivos**

* **Descripción:** La aplicación puede comportarse de manera inconsistente o presentar errores en diferentes modelos de Android, versiones de iOS o navegadores web, debido a la fragmentación del ecosistema.
* **Impacto:** Alto. Impacta la estabilidad de la aplicación, la calidad percibida y la capacidad de llegar a toda la base de usuarios objetivo.
* **Indicadores:** Probabilidad Media. Indicado por errores reportados solo en dispositivos específicos durante las pruebas, o por inconsistencias visuales/funcionales entre plataformas.
* **Estrategias de Mitigación:** Realizar testing temprano y continuo en un conjunto diverso de dispositivos físicos y emuladores. Utilizar plugins oficiales de Capacitor/Ionic y evitar APIs nativas no estandarizadas.
* **Plan de Contingencia:** Implementar detección de características (feature detection) y fallbacks elegantes. Establecer un conjunto mínimo de requisitos del sistema (versión de SO, capacidades hardware) y comunicarlos claramente.

### Riesgos de Proyecto

**R-07: Complejidad del desarrollo en solitario**

* **Descripción:** Un solo desarrollador debe gestionar y ejecutar todas las fases del proyecto (frontend, backend, móvil, seguridad, despliegue), lo que puede llevar a sobrecarga, cuellos de botella y fatiga.
* **Impacto:** Alto. Impacta la velocidad de desarrollo, la calidad del código, la salud del desarrollador y la capacidad de cumplir con los plazos.
* **Indicadores:** Alta probabilidad. Indicado por incumplimiento de hitos internos, acumulación de tareas pendientes en diferentes áreas, y aumento de errores por falta de revisión de código.
* **Estrategias de Mitigación:** Priorizar un MVP extremadamente estricto. Usar componentes de código abierto probados y frameworks de alto nivel (como Ionic/Capacitor) para reducir código personalizado. Externalizar o utilizar servicios gestionados (BaaS) cuando sea posible.
* **Plan de Contingencia:** Extender el cronograma del proyecto. Postergar o eliminar características no esenciales del MVP. Considerar la incorporación de un colaborador para áreas críticas específicas (ej., diseño de UI/UX).

**R-08: Costo de APIs y servicios externos**

* **Descripción:** Los costos asociados a APIs de terceros (geolocalización, SMS, voz, cloud) pueden escalar inesperadamente con el uso, afectando la sostenibilidad económica del proyecto.
* **Impacto:** Medio. Impacta la viabilidad financiera a largo plazo, especialmente en una fase inicial sin ingresos.
* **Indicadores:** Probabilidad Media. Indicado por estimaciones de costos que se acercan o superan el presupuesto disponible, o un crecimiento no anticipado en el número de usuarios durante las pruebas.
* **Estrategias de Mitigación:** Utilizar planes gratuitos o de bajo costo durante el desarrollo y lanzamiento inicial. Implementar mecanismos de "fallback" manual o con servicios alternativos más baratos (ej., email en lugar de SMS).
* **Plan de Contingencia:** Implementar un límite estricto de uso (rate limiting) en la aplicación para controlar costos. Migrar a proveedores más económicos o considerar un modelo freemium donde características de alto costo sean de pago.

**R-09: Requisitos legales de grabación**

* **Descripción:** Las leyes sobre consentimiento para la grabación de audio/video varían por país y región. Realizar grabaciones sin cumplir estos requisitos puede acarrear consecuencias legales.
* **Impacto:** Alto. Impacta la legalidad de la aplicación, pudiendo resultar en demandas, multas o la prohibición de la aplicación en ciertas jurisdicciones.
* **Indicadores:** Probabilidad Baja (si se investiga), pero de impacto severo. Indicado por cambios en legislaciones locales, consultas legales que revelan requisitos no considerados, o quejas de usuarios sobre privacidad.
* **Estrategias de Mitigación:** Investigar a fondo las leyes locales de todos los mercados objetivo. Implementar notificaciones claras y consentimiento explícito (no solo implícito) antes de iniciar cualquier grabación. Almacenar el registro del consentimiento.
* **Plan de Contingencia:** Restringir la disponibilidad de la aplicación a países con legislación favorable y clara. Cambiar el modelo de la aplicación para que solo grabe tras una confirmación explícita en el momento de la emergencia (botón de "sí, grabar").

**R-10: Rechazo en App Stores**

* **Descripción:** La aplicación puede ser rechazada durante el proceso de revisión de Apple App Store o Google Play Store por incumplir sus políticas (privacidad, background, funcionalidad).
* **Impacto:** Alto. Impacta la distribución masiva de la aplicación y el acceso a los usuarios, bloqueando completamente el lanzamiento en una plataforma.
* **Indicadores:** Probabilidad Media. Indicado por un rechazo inicial con comentarios específicos de los revisores, o por el uso de APIs o funcionalidades que históricamente son problemáticas (ej., background audio, acceso a contactos).
* **Estrategias de Mitigación:** Estudiar y seguir estrictamente las Human Interface Guidelines de Apple y las Policy Guidelines de Google. Probar la aplicación con las herramientas de pre-revisión (ej., App Store Connect). Ser transparente en las descripciones de los permisos.
* **Plan de Contingencia:** Responder rápidamente a los comentarios del revisor, modificando la aplicación según sus indicaciones. Tener listo un plan de lanzamiento progresivo (TestFlight/TestFairy) para obtener feedback antes del envío formal. Considerar la distribución alternativa solo para usuarios objetivo si el rechazo persiste.

**R-11: Escalabilidad del backend**

* **Descripción:** La arquitectura del servidor backend puede no soportar un crecimiento repentino en el número de usuarios o eventos concurrentes, leading a caídas del servicio en momentos críticos.
* **Impacto:** Medio. Impacta la disponibilidad y confiabilidad del servicio, especialmente durante una emergencia real donde la falla sería inaceptable.
* **Indicadores:** Probabilidad Baja en etapas iniciales. Indicado por tiempos de respuesta lentos bajo carga simulada, caídas durante pruebas de estrés, o alto uso de recursos en el servidor con pocos usuarios.
* **Estrategias de Mitigación:** Diseñar una arquitectura modular y sin estado (stateless) desde el inicio. Utilizar servicios cloud escalables (como AWS Lambda, Firebase Functions, bases de datos gestionadas) que ajusten capacidad automáticamente.
* **Plan de Contingencia:** Implementar un sistema de colas (message queue) para manejar picos de solicitudes. Tener un plan de escalamiento manual rápido con el proveedor cloud. Introducir una página de estado del servicio (status page).

### Riesgos de Seguridad

**R-12: Filtración de datos sensibles**

* **Descripción:** Información personal, ubicación en tiempo real, archivos de evidencia o credenciales podrían ser interceptados o accedidos por actores no autorizados debido a fallos en la seguridad.
* **Impacto:** Alto. Impacta la privacidad y seguridad física de los usuarios, la reputación de la aplicación y conlleva riesgos legales por violación de datos.
* **Indicadores:** Probabilidad Media. Indicado por vulnerabilidades identificadas en auditorías de código o pentesting, tráfico no encriptado detectado, o brechas de seguridad reportadas en servicios de terceros utilizados.
* **Estrategias de Mitigación:** Implementar encriptación end-to-end (E2EE) para datos sensibles. Minimizar el almacenamiento local de datos críticos. Usar conexiones seguras (HTTPS, TLS) y almacenar credenciales de manera segura (Keychain/Keystore).
* **Plan de Contingencia:** Tener un protocolo de respuesta a incidentes: notificación a usuarios afectados, revocación de tokens de acceso, y análisis forense para identificar la brecha. Realizar backups seguros y cifrados.

**R-13: Falsas alarmas intencionales**

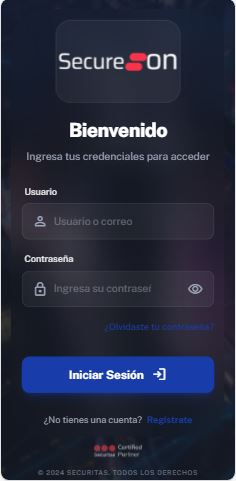
* Descripció**n:** Usuarios malintencionados podrían activar el sistema de emergencia repetidamente sin una razón real, saturando los recursos del centro de monitoreo y desacreditando el servicio.
* **Impacto:** Medio. Impacta la operación del centro de monitoreo, genera costos innecesarios y puede provocar que se ignore una alerta real.
* **Indicadores:** Probabilidad Baja. Indicado por un número anormalmente alto de activaciones desde una misma cuenta en un periodo corto, o reportes de centros de monitoreo sobre alarmas falsas.
* **Estrategias de Mitigación:** Implementar mecanismos de verificación (ej., llamada de confirmación automatizada antes de escalar). Establecer límites de uso por usuario. Requerir un proceso de registro verificado para cuentas.
* **Plan de Contingencia:** Suspender temporalmente las cuentas con patrones sospechosos de actividad. Introducir un sistema de reputación para usuarios. Tener un protocolo manual para que el centro de monitoreo verifique rápidamente una alerta antes de movilizar recursos externos.

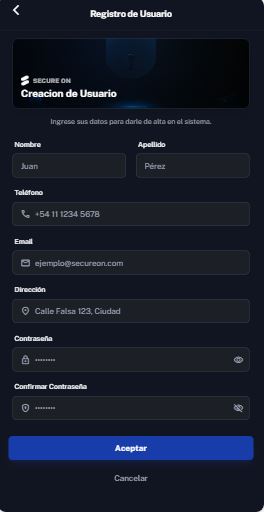
**R-14: Ataques al centro de monitoreo**

* **Descripción:** La plataforma web del centro de monitoreo podría ser objetivo de ataques DDoS, inyección SQL o intentos de acceso no autorizado, comprometiendo su operación.
* **Impacto:** Alto. Impacta la disponibilidad del servicio para todos los usuarios en un momento crítico y puede exponer datos sensibles de múltiples usuarios.
* **Indicadores:** Probabilidad Baja. Indicado por picos de tráfico malicioso detectados, múltiples intentos de login fallidos desde distintas IPs, o comportamientos anómalos en los logs de la aplicación.
* **Estrategias de Mitigación:** Implementar un backend robusto con Spring Security, incluyendo rate limiting, protección contra CSRF y SQL injection. Usar un Web Application Firewall (WAF). Mantener todas las dependencias actualizadas.
* **Plan de Contingencia:** Tener un plan de mitigación de DDoS con el proveedor de hosting/hosting. Realizar backups diarios y tener un entorno de recuperación ante desastres. Monitorear el tráfico y tener alertas automáticas para actividad sospechosa.

## Interfaces de Usuario

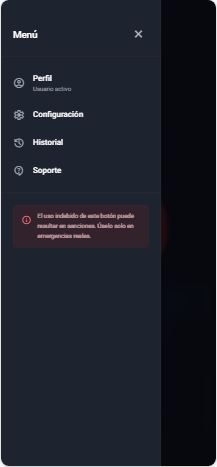
### Aplicación Movil





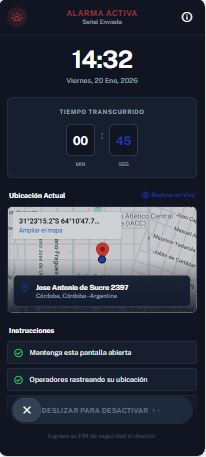
Imágen 4‑1 Interfaz de Inicio de Sesion

Imágen 4‑2 Interfaz de Registro de Usuario



Imágen 4‑3 Interfaz de Menu Principal

Imágen 4‑4 Interfaz de Pantalla Principal



Imágen 4‑5 Interfaz de Ventana e Cancelacion

Imágen 4‑6 Interfaz de Bloqueo de Dispositivo



Imagen 4‑7 Interfaz de Confirmación de Finalización de Alarma con PIN

Imagen 4‑8 Interfaz de Confirmación de Finalización de Alarma con Contraseña

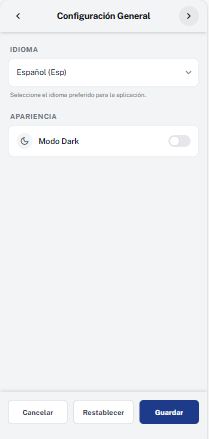


Imagen 4‑9 Interfaz de Configuracion General

Imagen 4‑10 Interfaz de Configuracion de Seguridad

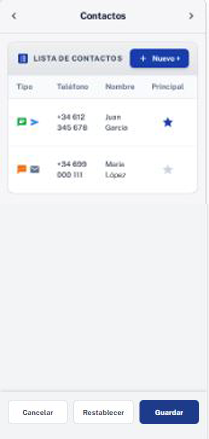


Imagen 4‑12 Interfaz de Configuracion de Contactos

Imagen 4‑11 Interfaz de Configuracion de Contactos

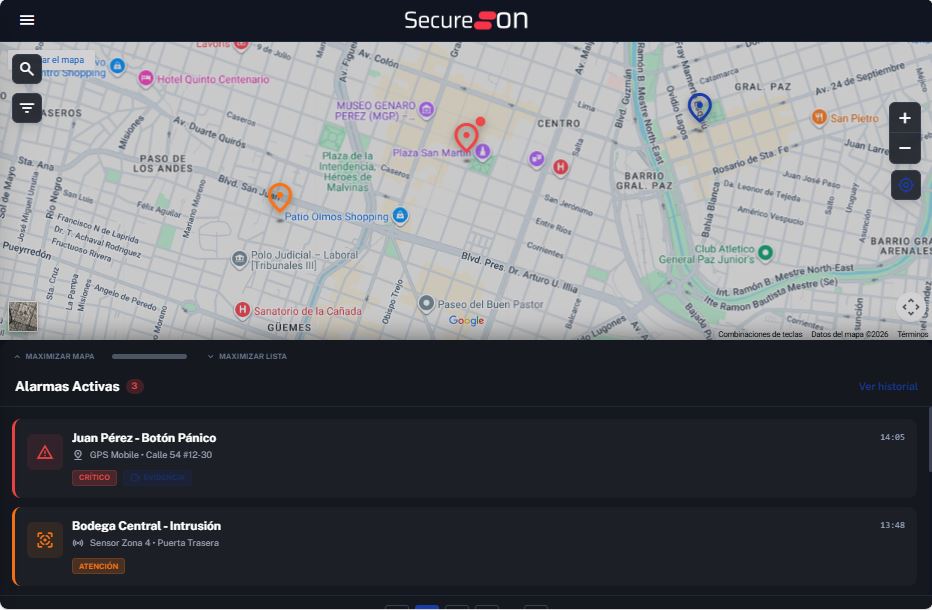
### Centro de Monitoreo



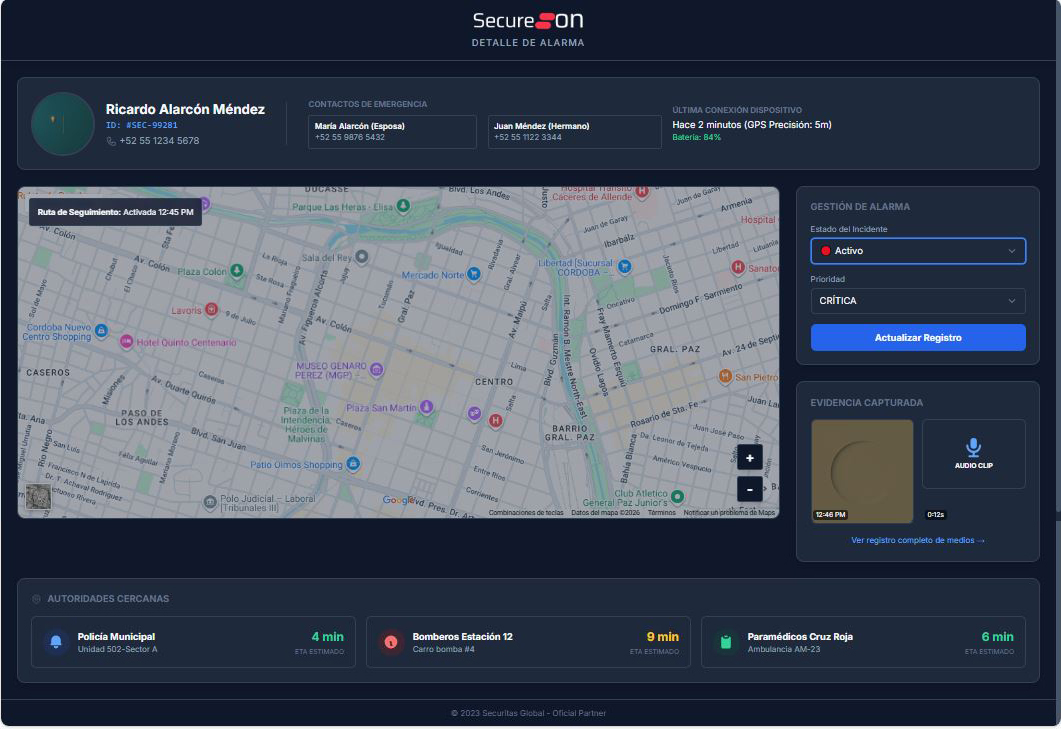
Imágen 4‑13 Interfaz de Inicio de Sesion en el CdM

aa

Imágen 4‑14 Interfaz del Registro de Operador



Imágen 4‑15 Interfaz del Dashboard del Centro de Monitoreo



Imágen 4‑16 Interfaz de Gestion de Alarma

# Modelo de Casos de Uso del Negocio

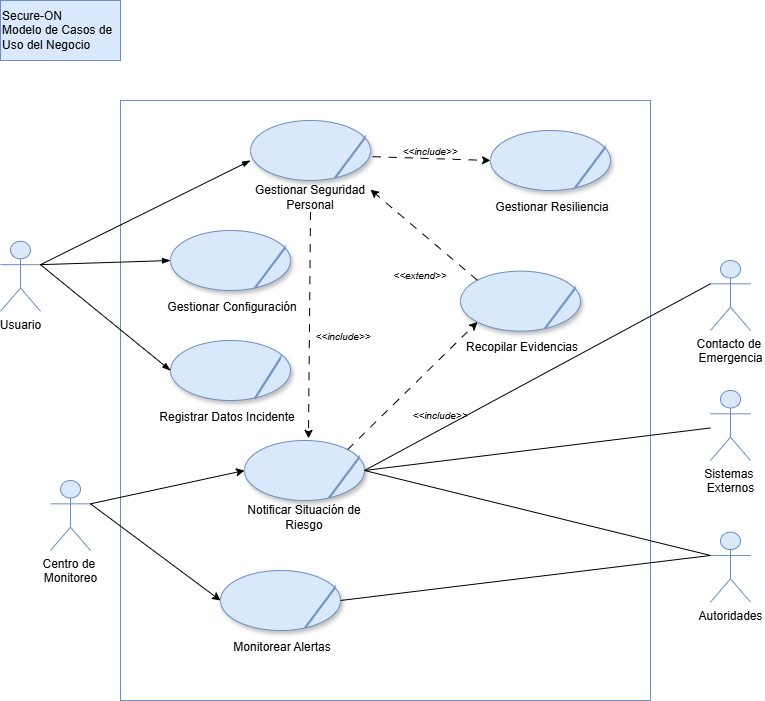
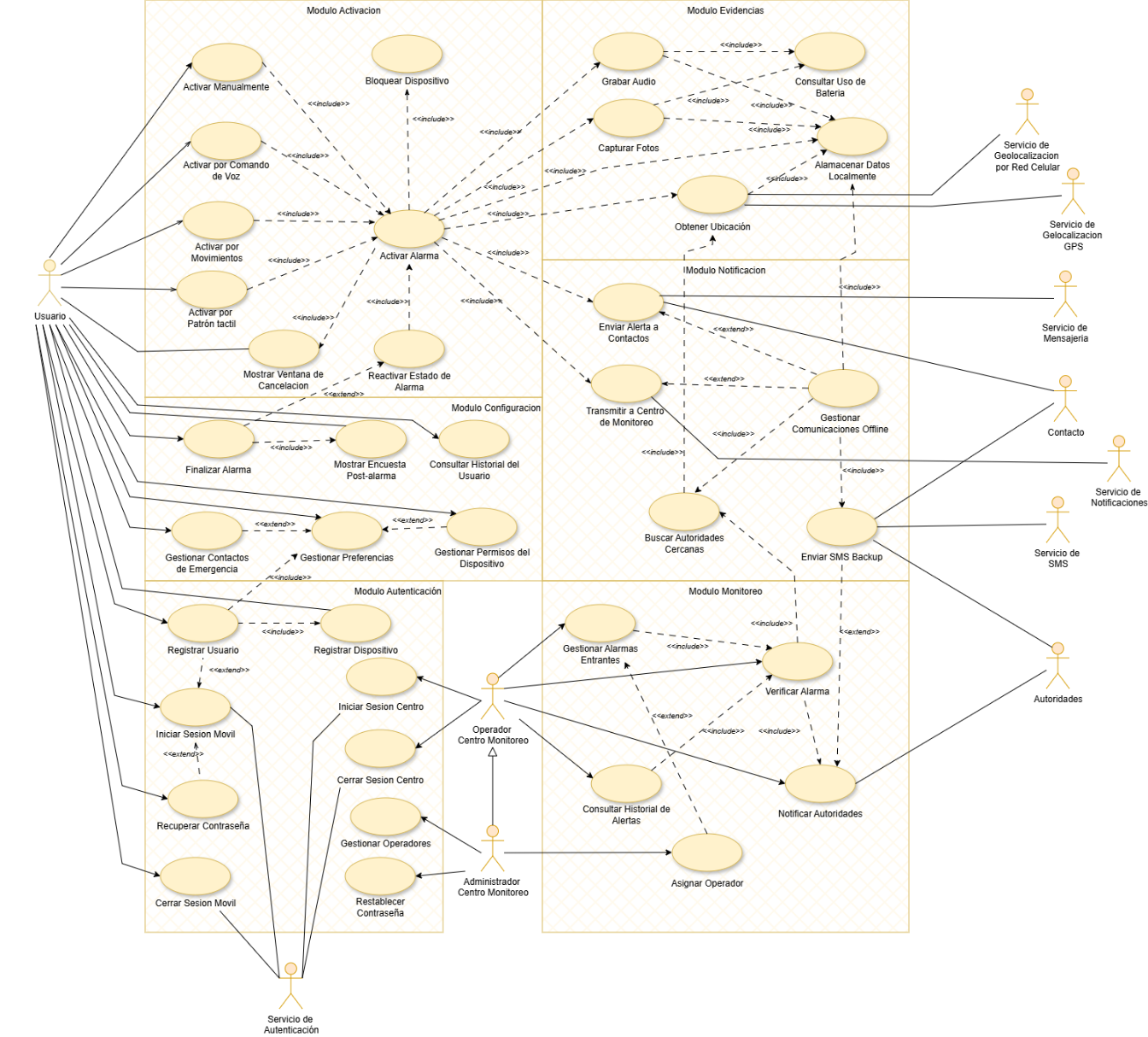


Imagen 5-1 Diagrama de Casos de Uso del Negocio

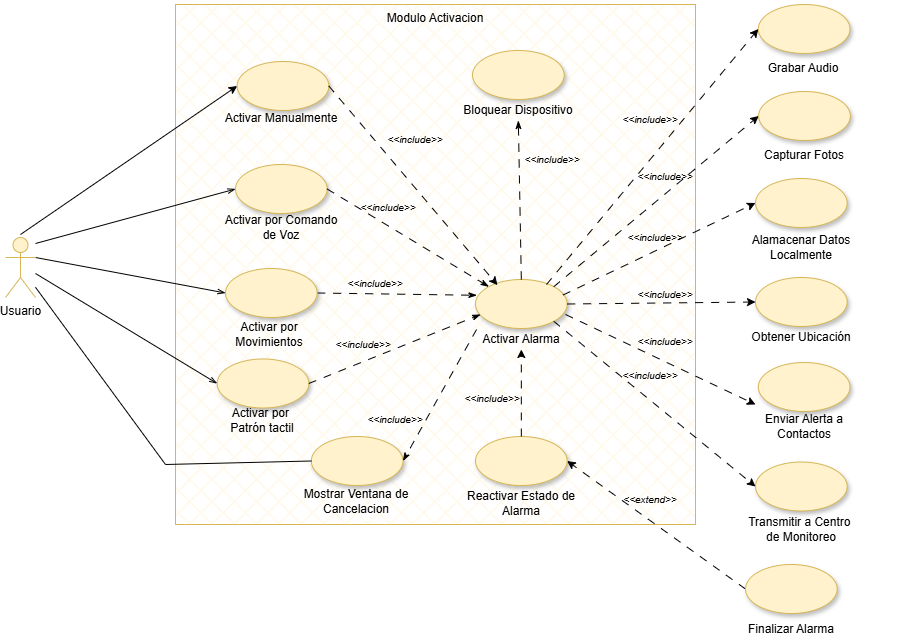
# Modelo de Casos de Uso

## Modelo de Casos de Uso del Sistema



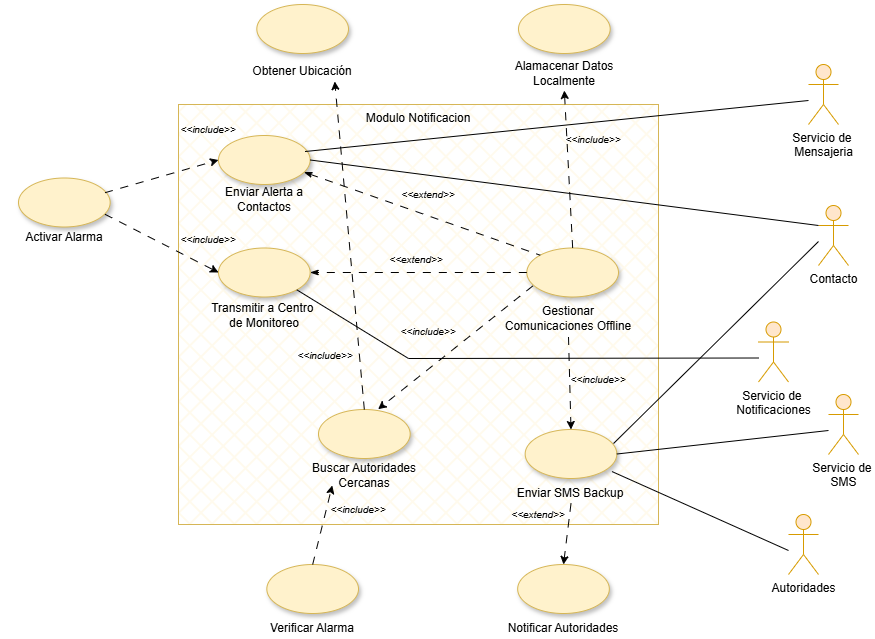
*Imagen 6-1 Diagrama de Casos de Uso del Sistema Completo*

### Módulo de Activación



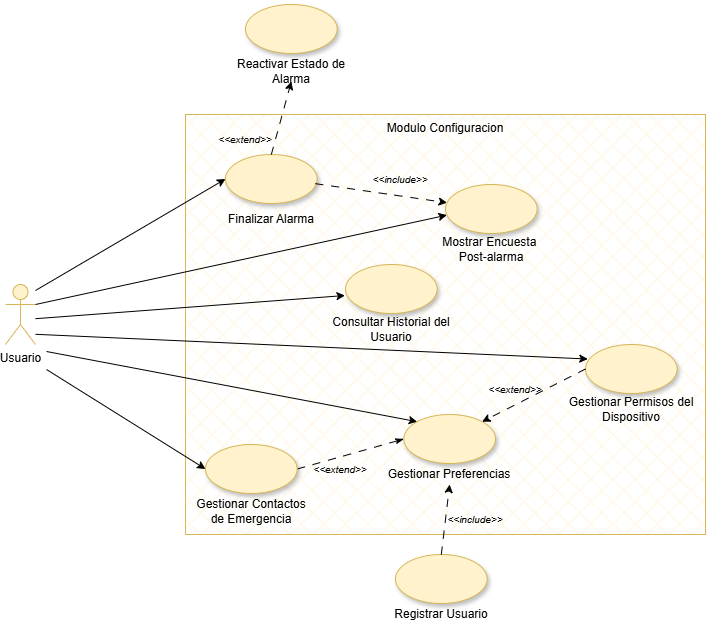
*Imagen 6-2 Diagrama de UC del Módulo de Activación*

### Módulo de Notificación



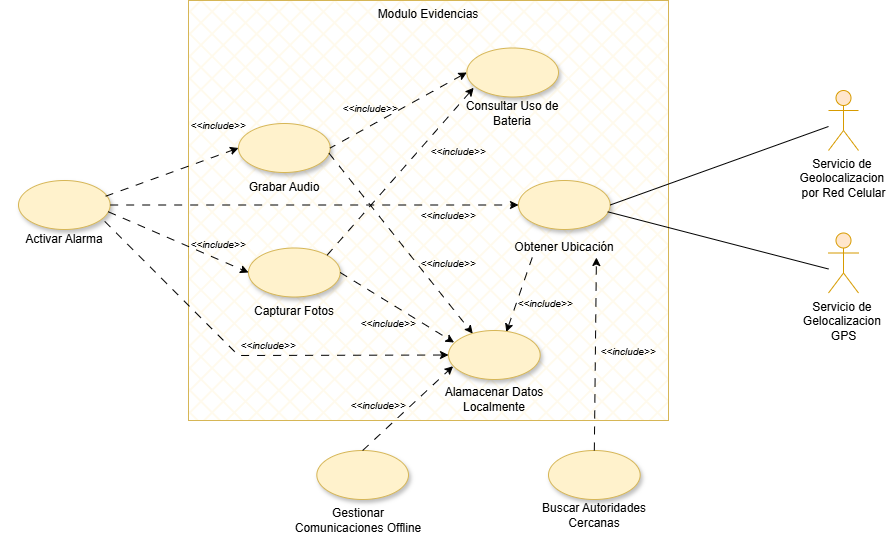
*Imagen 6-3 Diagrama de UC del Módulo de Notificación*

### Módulo de Configuración



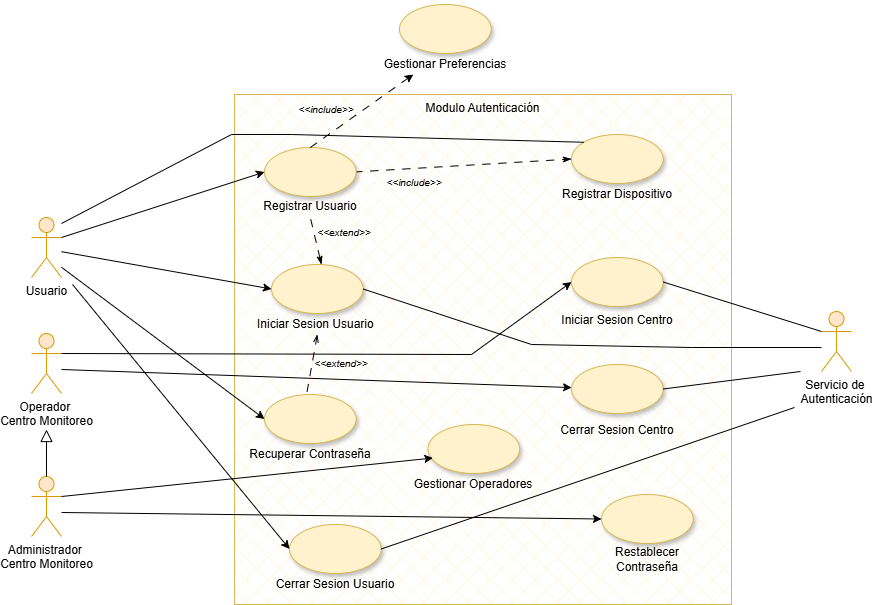
*Imagen 6-4 Diagrama de UC del Módulo Configuración*

### Módulo de Evidencias



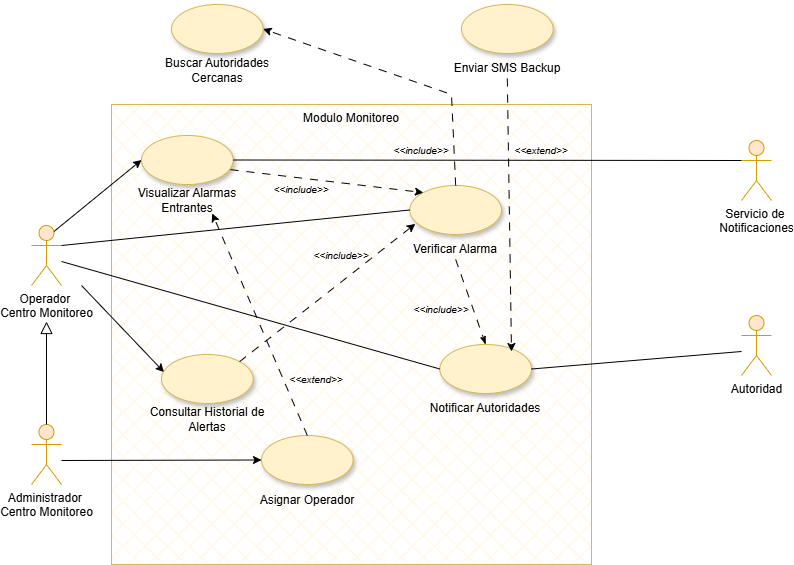
*Imagen 6-5 Diagrama de UC del Módulo de Evidencias*

### Módulo de Autenticación



*Imagen 6-6 Diagrama de UC del Módulo de Autenticación*

### Módulo de Monitoreo



*Imagen 6-7 Diagrama de UC del Módulo de Monitoreo*

## Especificación de Casos de Uso

### Módulo Activación

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-001** | **Activar Alarma** | | |
| Descripción | Coordina el protocolo completo de emergencia al ser invocado por métodos específicos, orquestando bloqueo, notificaciones y recolección de evidencias. | | |
| Objetivo | Activar la alarma de manera inmediata, coordinando todas las acciones de seguridad de manera integral. | | |
| Actor | n/a | Actores Sec. | n/a |
| Complejidad | Muy Alta | Prioridad | Muy Alta |
| Usa | UC-006, UC-007, UC-008, UC-009, UC-010, UC-034, UC-035, UC-036, UC-037 | Extiende | No |
| Pre-condiciones | Aplicación instalada y configurada correctamente  Usuario con sesión activa  Permisos necesarios concedidos (cámara, micrófono, ubicación)  Nivel de batería suficiente para operación básica  Servicios de localización disponibles | | |
| Post-condiciones | Dispositivo en estado de alarma activa  Protocolo completo de seguridad iniciado  Evidencias en proceso de recolección  Notificaciones programadas para envío  Estado persistido para resiliencia | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema inicia la secuencia de alarma cuando recibe solicitud de activación desde UC-002: activar manualmente, UC-003:activar por patrón táctil, UC-004: activar por comando de voz, UC-005: activar por movimiento y UC-008: reactivar alarma después de reinicio | |  | |
| 2. El sistema procede a bloquear el dispositivo y ejecuta el UC-006: Bloquear Dispositivo | |  | |
| 3. El sistema lanza una pantalla para cancelar la alarma, con un temporizador y ejecuta el UC-007: Mostrar Ventana de Cancelación | | 3.A.1 El sistema detecta que UC-007 retorna cancelación exitosa  3.A.2 El sistema interrumpe todos los procesos de alarma y registra evento de cancelación de alarma  3.A.3 Sistema desbloquea dispositivo y restaura estado normal y va al paso 10 | |
| 4. El sistema procede a obtener la ubicación y ejecuta el UC-034: Obtener Ubicación | |  | |
| 5. El sistema procede a enviar mensajes a los contactos de emergencia configurados y ejecuta UC-009:Enviar alarma a contactos | |  | |
| 6. El sistema procede a enviar notificación al centro de monitoreo y ejecuta UC-010: Transmitir a centro de monitoreo | |  | |
| 7. El sistema procede a capturar el audio ambiente y ejecuta el UC-035: Grabar Audio | |  | |
| 8. El sistema procede a sacar fotos y ejecuta UC-036: Capturar Fotos | |  | |
| 9. El sistema procede a guardar el estado de la alarma en activa y ejecuta el UC-037: Almacenar Datos Locales | |  | |
| 10. Fin del UC | |  | |
| Comentarios | Caso de uso central que orquesta toda la respuesta de emergencia. Tiempo crítico de ejecución <2 segundos | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-002** | **Activar Manualmente** | | |
| Descripción | Permite al usuario activar la alarma mediante un botón prominente en la pantalla principal de la aplicación. Diseñado para activación rápida y explícita cuando el usuario ya se encuentra dentro de la aplicación. | | |
| Objetivo | Ofrecer un método de activación directo, intuitivo y sin ambigüedades incorporada en la interfaz. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Baja | Prioridad | Alta |
| Usa | UC-001 | Extiende | No |
| Pre-condiciones | Aplicación abierta y en primer plano  Usuario en pantalla principal de la app  Usuario autenticado y con sesión activa  Botón de activación visible y habilitado  No hay otra alarma activa en el momento | | |
| Post-condiciones | La activación se alarma se ha invocado exitosamente UC-001  Protocolo completo de seguridad iniciado  Evento de activación registrado en historial con origen en activación Manual | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario navega a pantalla principal | |  | |
| 2. El sistema renderiza dentro de la pantalla principal un botón rojo con la Leyenda Activar Alarma, si el estado de la alarma no esta activa | | 2.A.1. Si ya hay una alarma previamente activada, el botón se mostrara deshabilitado | |
| 3. El usuario presiona por más de 3 segundos el botón de activar alarma | | 3.A.1. El usuario realiza una presión leve y/o insuficiente en el tiempo  3.A.2. El sistema presenta dialogo de confirmación para activar la alarma.  3.A.3.A.1. El usuario selecciona Activar, sigue en el paso 4  3.A.3.B.1. El usuario selecciona Cancelar, sigue en el paso 5 | |
| 4. El sistema procede a iniciar la activación de la alarma y ejecuta UC-001, con modo de activación manual | |  | |
| 5. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-003** | **Activar por Patrón Táctil** | | |
| Descripción | Permite al usuario activar la alarma mediante el dibujo de un patrón preconfigurado en la pantalla bloqueada del dispositivo. El sistema reconoce y valida el patrón táctil contra el almacenado, activando la alarma solo cuando estos coinciden. | | |
| Objetivo | Proporcionar un método discreto y rápido de activación mediante interfaz táctil familiar. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Alta |
| Usa | UC-001 | Extiende | No |
| Pre-condiciones | Dispositivo en estado de pantalla bloqueada  Patrón de activación configurado  Sensor táctil funcionando correctamente  Aplicación con permisos para capturar eventos táctiles en pantalla bloqueada  No hay otra alarma activa en el momento | | |
| Post-condiciones | La activación se alarma se ha invocado exitosamente UC-001  Protocolo completo de seguridad iniciado  Evento de activación registrado en historial con origen en activación por patron tactil | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario dibuja patrón secreto sobre la pantalla bloqueada del dispositivo | |  | |
| 2. El sistema captura secuencia táctil completa (coordenadas, presión, timing) | | 2.A.1 El sistema detecta un patrón incompleto o interrumpido  2.A.2 Sistema descarta captura y reinicia el UC en el paso 1 | |
| 3. El sistema normaliza patrón ingresado compensando variaciones de tamaño y posición | |  | |
| 4. El sistema compara patrón normalizado con patrón de referencia almacenado y calcula porcentaje de coincidencia | |  | |
| 5. El sistema valida que el porcentaje de coincidencia del patrón ingresado es mayor o igual al 85% | | 5.A.1. El sistema detecta coincidencia menor al 85%  5.A.2. El sistema incrementa contador interno de intentos fallidos  5.A.3. Si hay más de 3 intentos fallidos, el sistema bloquea nuevos intentos por 30 segundos y vuelve al paso 1 | |
| 6. El sistema procede a activar el inicio de la alarma y ejecuta UC-001 con modo de activación por patrón táctil | |  | |
| 7. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-004** | **Activar por Comando de Voz** | | |
| Descripción | Permite la posibilidad de activar la alarma mediante el reconocimiento de voz continuo en segundo plano para detectar una frase clave preconfigurada. | | |
| Objetivo | Ofrecer un método activación manos libre mediante comando vocal, ideal para situaciones donde el uso táctil no es posible o seguro. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Muy Alta | Prioridad | Alta |
| Usa | UC-001 | Extiende | No |
| Pre-condiciones | Reconocimiento de voz activado en configuración de aplicación  Frase clave definida y entrenada  Permisos de acceso al micrófono concedidos  Procesamiento de audio en segundo plano permitido por SO  Capacidad de procesamiento suficiente para reconocimiento continuo  No hay otra alarma activa en el momento | | |
| Post-condiciones | La activación se alarma se ha invocado exitosamente UC-001  Protocolo completo de seguridad iniciado  Evento de activación registrado en historial con origen en activación por voz | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario pronuncia las palabras clave de activación | |  | |
| 2. El sistema captura stream de audio y le aplica pre procesamiento (filtrado de ruido) | | 2.A.1. El sistema detecta que la relación señal-ruido (SNR) es menor a 20dB (lo que es lo mismo un audio con mucho ruido de fondo)  2.A.2. El sistema aumenta el umbral de confianza al 90% y aplica filtros adicionales de reducción de ruido  2.A.3 Sistema intensifica análisis espectral para separación voz/ruido y sigue en el paso 3 | |
| 3. El sistema aplica modelo de reconocimiento vocal para conversión audio-texto | |  | |
| 4. El sistema compara texto reconocido con frase clave almacenada y calcula el nivel de confianza del reconocimiento | |  | |
| 5. El sistema valida que el nivel de confianza del reconocimiento es igual o mayor al 80% | | 5.A.1. El sistema detecta que el nivel de confianza esta entre 60-80% (reconocimiento parcial)  5.A.2 El Sistema espera 2 segundos adicionales buscando confirmación audible de forma parcial  5.A.3.A.1. Si recibe confirmación va al paso 6  5.A.3.B.1. Si no recibe confirmación, descarta activación y va al paso 7  5.B.1. El sistema detecta que el nivel de confianza esta por debajo del 60%, descarta la activación y va al paso 7 | |
| 6. El sistema activa el inicio de la alarma llamando al UC-001: activar alarma con modo de activación por comando de voz | |  | |
| 7. Fin del UC | |  | |
| Comentarios | Debe tener una precisión en la detección mayor 95% en condiciones normales, consumo del CPU menor al 5% en modo escucha pasiva y una latencia menor a 1.5 seg. | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-005** | **Activar por Movimiento** | | |
| Descripción | Ofrecer un método de activación automático mediante la detección inteligente de movimientos bruscos, sacudidas o patrones de movimiento específicos asociados a situaciones de peligro mediante sensores del dispositivo como acelerómetros y giroscopios | | |
| Objetivo | Activar alarma automáticamente basado en análisis del movimiento físico del dispositivo, ideal para situaciones donde el usuario no puede activar manualmente pero experimenta movimientos característicos de agresión, caída o robo violento. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Muy Alta | Prioridad | Media |
| Usa | UC-001 | Extiende | No |
| Pre-condiciones | Sensores de movimiento (acelerómetro 3 ejes, giroscopio) disponibles y funcionando  Patrones de movimiento configurados y calibrados para usuario específico  Procesamiento en segundo plano de datos de sensores activo y permitido por SO  Aplicación con permisos para acceder a sensores del dispositivo  Umbrales de sensibilidad configurados según perfil de actividad del usuario  No hay otra alarma activa en el momento | | |
| Post-condiciones | UC-001 invocado exitosamente  Protocolo completo de seguridad iniciado  Evento de activación registrado en historial con origen en activación por movimiento | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario experimenta movimiento brusco o gesto específico configurado como disparador (caída, sacudida violenta, patrón de lucha) | |  | |
| 2. El sistema captura ventana temporal de datos (hasta que termina el evento o hasta un máximo de 8 segs) | |  | |
| 3. El sistema aplica extracción de características: magnitud aceleración, cambio brusco, rotación, altitud | |  | |
| 4. El sistema ejecuta clasificador sobre características extraídas | |  | |
| 5. El sistema valida que el nivel de confianza del clasificador de movimiento tenga un nivel de confianza mayor o igual al 80% | | 5.A.1. El sistema detecta el patrón de movimiento con confianza 60-80% (zona-gris)  5.A.2. El sistema espera movimiento de confirmación específico en ventana de 2 segundos  5.A.3.A.1. Si recibe confirmación va al paso 6  5.A.3.B.1. Si no recibe, descarta como falso positivo y va al paso 7  5.B.1. El sistema detecta el patrón de movimiento con confianza menor al 60%, descarta la alarma como falso positivo y va al paso 7 | |
| 6. El sistema activa el inicio de la alarma llamando al UC-001: activar alarma con modo de activación por movimiento | |  | |
| 7. Fin del UC | |  | |
| Comentarios | Debe tener una precisión en detección de caídas mayor al 90%, y la tasa de falsos positivos ser menor al 2% en uso normal (excluyendo actividades deportivas). El consumo de batería debe ser menor al 3% con monitoreo continuo de movimiento | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-006** | **Bloquear Dispositivo** | | |
| Descripción | Inhabilita todos los mecanismos normales de desbloqueo del dispositivo y muestra interfaz de emergencia personalizada full-screen cuando se activa una alarma. Previene desactivación no autorizada mientras proporciona información clara sobre el estado de emergencia y opciones de cancelación. | | |
| Objetivo | Garantizar que el dispositivo permanezca en estado de alarma activa hasta desactivación legítima, previniendo manipulaciones por atacantes y mostrando información relevante de manera clara incluso en condiciones de estrés. | | |
| Actor | n/a | Actores Sec. | n/a |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | UC-001: activar alarma en proceso de ejecución  Aplicación tiene permisos necesarios  Dispositivo no está actualmente en proceso de apagado forzado | | |
| Post-condiciones | Dispositivo en estado de bloqueo de emergencia con funciones restringidas  Interfaz de alarma visible proporcionando información relevante  Mecanismos nativos de desbloqueo deshabilitados temporalmente  Botones físicos limitados en funcionalidad | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema muestra interfaz de emergencia de la alarma full-screen con: fecha y hora actual, tiempo desde que la alarma se activó, ubicación actual e instrucciones básicas | | 1.A.1. El sistema detecta que está activado el modo sigiloso  1.A.2. El sistema muestra una pantalla oscura y continua al paso 2 | |
| 2. El sistema verifica que el SO del dispositivo permita su bloqueo | | 2.A.1. El sistema detecta restricciones del SO para bloqueo nativo  2.A.2. El sistema implementa bloqueo alternativo por superposición de pantalla persistente | |
| 3. El sistema deshabilita métodos nativos de desbloqueo | | 3.A.1. El sistema detecta restricciones del SO para bloqueo nativo  3.A.2. El sistema implementa bloqueo alternativo por superposición de pantalla persistente y continua al paso 5 | |
| 4. El sistema limita funcionalidad de botones físicos | |  | |
| 5. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-007** | **Mostrar Ventana de Cancelación** | | |
| Descripción | Presenta una interfaz temporal superpuesta que permite al usuario cancelar una alarma activada accidentalmente durante un período de gracia configurable entre 5 y 30 segundos. | | |
| Objetivo | Proveer un mecanismo seguro y accesible para que usuarios legítimos cancelen las alarmas activadas accidentalmente, manteniendo al mismo tiempo seguridad contra desactivaciones no autorizadas por terceros. | | |
| Actor | n/a | Actores Sec. | Usuario |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | El dispositivo ha sido bloqueado exitosamente por el UC-006  Métodos de autenticación del usuario configurados y disponibles  Hardware de pantalla y entrada táctil funcionando correctamente | | |
| Post-condiciones | Si desactiva la alarma: se cancela la continuación de la alarma (UC-001) y el dispositivo se restaura a un estado normal.  Si no desactiva la alarma: continua con el procedimiento de emergencia iniciado en el UC-001 | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema muestra ventana de cancelación superpuesta con temporizador grande y visible, botón “Cancelar Alarma” e instrucciones breves para cancelar la alarma | |  | |
| 2. El sistema inicia cuenta regresiva configurada | |  | |
| 3. El usuario selecciona opción “Cancelar Alarma” dentro del tiempo disponible | | 3.A.1 El sistema valida que el temporizador ha terminado sin tener una acción del usuario  3.A.2 El sistema oculta automáticamente ventana de cancelación y va al paso 7 | |
| 4. El sistema presenta métodos de autenticación disponibles según configuración: huella dactilar, patrón, PIN, contraseña | |  | |
| 5. El usuario selecciona y ejecuta método de autenticación preferido | | 5.A.1. El sistema detecta credenciales de autenticación inválidas  5.A.2. El sistema muestra mensaje de error discreto  5.A.3.A.1. Si el temporizador no ha expirado el sistema permite reintentar la autenticación y retorna al paso 3  5.A.3.B.1. Si el temporizador ya expiró el sistema oculta la ventana de cancelación y va al paso 7  5.B.1. El sistema detecta que el tiempo de cancelación expiro y oculta la ventana de cancelación y va al paso 7 | |
| 6. El sistema cancela la alarma y restaura estado normal del dispositivo | |  | |
| 7. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-008** | **Reactivar Estado de Alarma** | | |
| Descripción | Proceso automático de resiliencia que se ejecuta al iniciarse el sistema operativo del dispositivo, cuando existía una alarma activa y restablece inmediatamente el estado completo de alarma sin intervención del usuario, garantizando la continuidad de la protección. | | |
| Objetivo | Impedir que un atacante pueda detener el sistema de seguridad apagando o reiniciando forzosamente el dispositivo, asegurando que el modo de emergencia persista y se reanude automáticamente, manteniendo la operatividad crítica. | | |
| Actor | n/a | Actores Sec. | n/a |
| Complejidad | Muy Alta | Prioridad | Alta |
| Usa | UC-001 | Extiende | No |
| Pre-condiciones | El dispositivo completa su proceso de arranque del sistema operativo.  La aplicación está configurada para ejecutarse automáticamente al inicio (como servicio o aplicación de arranque).  Existe un mecanismo de persistencia que guardó el estado de alarma activa antes del apagado | | |
| Post-condiciones | Si existía una alarma activa, se restaura por completo el estado de emergencia.  Se invoca el protocolo de activación con los parámetros originales guardados.  El dispositivo se bloquea y muestra la interfaz de emergencia  Las funcionalidades de notificación y recolección de evidencias se reanudan desde el punto donde se interrumpieron.  Si no había alarma activa, la aplicación se inicia en modo normal. | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema detecta que el SO del móvil se está iniciando | |  | |
| 2. El sistema verifica que la bandera de la última alarma sigue activa | | 2.A.1. El sistema verifica que la bandera de la última alarma esta inactiva y continua en el paso 6 | |
| 3. El sistema verifica que no se haya intentado finalizar la alarma desde el CdM | | 3.A.1. El sistema detecta que la alarma tuvo un pedido de finalización de CdM, que no se cursó por estar el dispositivo apagado y llama al UC-014: finalizar alarma y continua en el paso 6 | |
| 4. El sistema recupera los datos contextuales de la alarma | |  | |
| 5. El sistema activa el inicio de la alarma llamando al UC-001: activar alarma con modo de activación por reinicio | |  | |
| 6. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

### Modulo Notificación

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-009** | **Enviar Alarma a Contactos** | | |
| Descripción | Envía notificaciones multicanal (WhatsApp, Telegram, SMS, etc.) a los contactos de emergencia configurados por el usuario, incluyendo mensaje predefinido y ubicación. | | |
| Objetivo | Notificar rápidamente a los contactos de emergencia configurados, sobre la situación de alarma utilizando múltiples canales para maximizar la probabilidad de recepción. | | |
| Actor | n/a | Actores Sec. | Servicios de mensajería, Contactos de emergencia |
| Complejidad | Alta | Prioridad | Muy Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | La alarma ha sido activada (UC-001 ejecutado)  Ha finalizado la ventana de cancelación sin intervención del usuario  Existe al menos un contacto de emergencia configurado  Los permisos necesarios para mensajería están concedidos | | |
| Post-condiciones | Se han enviado alarmas a todos los contactos configurados por sus canales preferidos  Se registra en el historial el envío de cada notificación  Si algún envío falló, se programa reintento automático | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema recupera la lista de contactos de emergencia configurados del perfil del usuario | |  | |
| 2. El sistema obtiene el canal de comunicación preferido por cada contacto | | 2.A.1. El sistema no obtiene el canal de comunicación para el contacto  2.A.2. El sistema selecciona por defecto enviar SMS | |
| 3. El sistema construye el mensaje con: nombre del usuario, mensaje de emergencia predefinido, nombre del contacto, última ubicación y hora del evento | |  | |
| 4. El sistema verifica conexión a internet y envía el mensaje a través del canal correspondiente usando la API del Servicio de Mensajería Externo correspondiente | | 4.A.1. El sistema detecta falla en la conexión a internet  4.A.2. El sistema llama en paralelo al UC-011 en modo falloCTO y libera la ejecución para continuar en el paso 6  4.B.1. El sistema detecta que el contacto es envío por SMS  4.B.2. El sistema llama en paralelo al UC-011 en modo falloCTO y libera la ejecución para continuar en el paso 6  4.C.1. El sistema recibe error de la API del Servicio de Mensajería  4.C.2. El sistema llama en paralelo al UC-011 en modo falloCTO y libera la ejecución para continuar en el paso 6 | |
| 5. El sistema recibe la confirmación de la API del servicio de mensajería y registra el envío exitoso del mensaje | |  | |
| 6. El sistema verifica que no existen más contactos | | 6.A.1. El sistema verifica que hay más contactos a enviar y continua en el paso 2 | |
| 7. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-010** | **Transmitir a Centro de Monitoreo** | | |
| Descripción | Establece comunicación con el servidor del CdM, enviando datos del usuario, ubicación en tiempo real, y facilitando el streaming de evidencias (audio/fotos). Mantiene canal persistente durante la emergencia. | | |
| Objetivo | Notificar al CdM para activar protocolos de respuesta coordinada y proporcionar datos en tiempo real para toma de decisiones. | | |
| Actor | n/a | Actores Sec. | Servicio de Notificaciones |
| Complejidad | Muy Alta | Prioridad | Muy Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | El usuario tiene una cuenta registrada y activa en el sistema  El dispositivo tiene conectividad a internet estable  El CdM está operativo y accesible | | |
| Post-condiciones | El CdM ha recibido la alarma y puede visualizarla en el tablero  Se establece un canal de comunicación persistente mientras dure la alarma  El sistema inicia la transmisión periódica de ubicación y evidencias  Se recibe confirmación del servidor con ID de caso asignado | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema establece conexión con el servidor del CdM | | 1.A.1. El sistema falla en la conexión con el servidor del CdM y ejecuta el UC-011 en modo falloCdM y continua en el paso 6 | |
| 2. El sistema valida que el UC está siendo llamado en modo activación y envía paquete inicial con: datos del usuario, ubicación actual, timestamp de activación y método de activación utilizado | | 2.A.1. El sistema valida que el UC está siendo llamado en otro modo y tiene id asignado, procede a enviar paquete con: ID de alarma, estado de alarma, ubicación actual, y timestamp de evento | |
| 3. El sistema recibe confirmación del servidor del CdM con: ID de alarma, operador asignado e instrucciones específicas (si las hay) | | 3.A.1 El sistema no recibe confirmación del CdM en 5 segundos  3.A.2.A.1 El sistema valida que el número de intento es igual o menor a 3  3.A.2.A.2 El sistema espera 5 segundos para reintentar conexión y vuelve al paso 2.  3.A.2.B.1 El sistema valida que el número de intento es mayor a 3  3.A.2.B.2 El sistema ejecuta el UC-011 en modo falloCdM y continua en el paso 7 | |
| 4. El sistema inicia transmisión periódica de ubicación en lapsos preconfigurables (de 30 segundos por defecto) | | 4.A.1. El sistema detecta pérdida de conexión durante transmisión  4.A.2. El sistema Almacena datos en buffer local y reintenta reconexión automáticamente tras 5 segundos  4.A.3.A.1. El sistema detecta que se reconecto y sincroniza todos los datos pendientes  4.A.3.B.1. El sistema no detecta una reconexión y es el intento igual o menor a 3, vuelve al paso 4  4.A.3.C.1. El sistema no detecta una reconexión y es el intento mayor a 3, llama al UC-011 en modo falloGPS y continua en el paso 7 | |
| 5. El sistema comienza a enviar evidencias según disponibilidad en la cola de evidencias pendientes de envio | | 5.A.1. El sistema detecta pérdida de conexión durante transmisión y reintenta reconexión automáticamente tras 5 segundos  5.A.2.A.1. El sistema detecta que se reconecto y sincroniza todos los datos pendientes  5.A.2.B.1. El sistema no detecta una reconexión y es el intento igual o menor a 3, vuelve al paso 5  5.A.3.C.1. El sistema no detecta una reconexión y es el intento mayor a 3, llama al UC-011 en modo falloEVD y continua en el paso 7 | |
| 6. El sistema marca como enviadas las evidencias para su posterior eliminación del almacenamiento local | |  | |
| 7. El sistema verifica que el estado de la alarma está finalizado para cerrar la conexión al CdM | | 7.A.1. El sistema verifica que el estado de alarma está activo y continua en el paso 4 | |
| 8. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-011** | **Gestionar Comunicaciones Offline** | | |
| Descripción | Maneja el escenario donde no hay conectividad a internet, activando protocolos alternativos de comunicación y almacenamiento local de datos. | | |
| Objetivo | Garantizar continuidad operativa y evitar la pérdida de datos críticos en condiciones de conectividad limitada o intermitente. | | |
| Actor | n/a | Actores Sec. | Usuario |
| Complejidad | Alta | Prioridad | Alta |
| Usa | UC-012, UC-013 | Extiende | No |
| Pre-condiciones | Se ha detectado falta de conectividad a internet o intermitencias en la conexión  El modo y los datos de llamada están definidos  La alarma está activa y no ha sido cancelada | | |
| Post-condiciones | Se han activado los mecanismos de comunicación alternativos  Los datos se están almacenando localmente  El sistema monitorea continuamente el estado de conectividad  Se programa reintento automático de conexión periódico | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema detecta se invoca el UC en modo de ejecución falloCdM | | 1.A.1. El sistema detecta que el modo de ejecución es falloCTO y continua en el paso 2  1.B.1. El sistema detecta que el modo de ejecución es falloGPS y continua en el paso 3  1.C.1. El sistema detecta que el modo de ejecución es falloEVD y continua en el paso 6 | |
| 2. El sistema envía el texto del mensaje original por SMS al número de contacto y llama al UC-012 enviar SMS backup | | 2.A.1. El sistema no logra enviar el mensaje por no tener cobertura de red celular  2.A.2. El sistema llama al UC-037 para guardar el mensaje  2.A.3. El sistema monitorea si vuelve algún tipo de conexión a la red.  2.A.4.A.1. El sistema detecta que volvió la conexión a internet, sin que antes haya vuelto la red celular  2.A.4.A.2. El sistema reintenta envío del mensaje por el canal original del mensaje  2.A.4.B.1. El sistema detecta que volvió la conexión a la red celular, sin que antes haya vuelto la conexión a internet  2.A.4.A.2. El sistema reintenta envío del mensaje por SMS UC-012  2.B.1. El sistema detecta que es modo de ejecución falloCTO y va al paso 8 | |
| 3. El sistema busca el número de contacto de las Autoridades Locales más cercanas a la última ubicación conocida y llama al UC-013 | |  | |
| 4. El sistema llama al UC-012 y envía mensaje SMS a las autoridades más cercanas: con datos del usuario, mensaje predefinido, ultima ubicación y hora del evento | | 4.A.1. El sistema no logra enviar el mensaje por no tener cobertura de red celular  4.A.2. El sistema llama al UC-037 para guardar el mensaje  4.A.3. El sistema monitorea si vuelve algún tipo de conexión a la red.  4.A.4.A.1. El sistema detecta que volvió la conexión a internet  4.A.4.A.2. El sistema cancela el envío del mensaje (el CdM se encarga de la conexión con las autoridades)  4.A.4.B.1. El sistema detecta que volvió la conexión a la red celular  4.A.4.B.2. El sistema reintenta envío del mensaje por SMS UC-012 | |
| 5. El sistema monitorea periódicamente cada 60 segundos si vuelve la conexión a internet o red celular hasta que se haya completado el envio. | |  | |
| 6. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-012** | **Enviar SMS Backup** | | |
| Descripción | Envía mensajes SMS de emergencia cuando no hay conectividad a internet, dirigidos a contactos, autoridades cercanas y/o Centro de Monitoreo. Funciona como canal de respaldo crítico. | | |
| Objetivo | Proporcionar notificación básica alternativa cuando fallan todos los canales de internet, utilizando la red celular básica. | | |
| Actor | n/a | Actores Sec. | Servicio SMS, Autoridades locales, Contactos de emergencia |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | UC-031 |
| Pre-condiciones | Modo offline ha sido activado  Existe cobertura de red celular  Hay números de teléfono configurados para notificación por SMS  El dispositivo tiene crédito o plan de SMS activo  Permisos de SMS están concedidos en el dispositivo | | |
| Post-condiciones | Se han enviado SMS a todos los destinatarios configurados para modo offline  Se registra el envío en el historial local con hora y estado  Se notifica al UC-011 del resultado de la operación | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema verifica que recibe el número de contacto | | 1.A.1. El sistema no recibe el número de contacto, registra el error y continua en el paso 6 | |
| 2. El sistema verifica que recibe el mensaje a enviar | | 2.A.1. El sistema no recibe el mensaje a enviar  2.A.2. El sistema arma un mensaje predefinido de máximo de 160 caracteres con el nombre y la ubicación del usuario, y la hora del evento  2.B.1. El sistema detecta que el mensaje supera 160 caracteres  2.B.2. Divide mensaje en múltiples SMS concatenados  2.B.3. Ajusta formato para mantener información crítica en primer SMS  2.B.4. Envía secuencia completa | |
| 3. El sistema envía mensaje SMS utilizando la API nativa del SO del dispositivo | | 3.A.1. El sistema detecta error de sin crédito o servicio no disponible  3.A.2. El sistema Almacena los mensajes en cola local con prioridad alta  3.A.3. El sistema Intenta enviar cuando detecta conexión a internet o red celular | |
| 4. El sistema espera confirmación de envío del sistema operativo | |  | |
| 5. El sistema envía exitosamente el mensaje y notifica resultado de éxito | | 5.A.1. El sistema no logra enviar el mensaje y notifica la causa del fallo | |
| 6. Fin del UC | |  | |
| Comentarios | Manejar permisos de SMS  Considerar costos de SMS en diferentes regiones | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-013** | **Buscar Autoridades Cercanas** | | |
| Descripción | Identifica las autoridades de emergencia más cercanas a la ubicación actual del usuario (policía, bomberos, hospitales) utilizando bases de datos locales o servicios online. | | |
| Objetivo | Proporcionar información de contacto precisa y actualizada de autoridades locales para notificación directa o referencia del Centro de Monitoreo. | | |
| Actor | n/a | Actores Sec. | Usuario |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | UC-034, UC-037 |
| Pre-condiciones | La alarma está activa y no ha sido cancelada  Se necesita notificar a autoridades  Se puede obtener alguna forma de ubicación (GPS, red celular)  Base de datos de autoridades disponible (local u online) | | |
| Post-condiciones | Se tiene lista priorizada de autoridades cercanas con datos de contacto completos  Los datos están disponibles para UC-011 o UC-032  Se registra la búsqueda y resultados en el historial local  Si se usó API online, se cachean resultados localmente | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema recibe las coordenadas de la última ubicación del usuario | | 1.A.1. El sistema no recibe las coordenadas de la ultima ubicación  1.A.2. El sistema intenta obtener la ubicación actual llamando al UC-034 obtener ubicación  1.A.3.A.1. El sistema obtiene la ubicación y sigue en el paso siguiente  1.A.3.B.1. El sistema no encuentra la ubicación actual y registra error que retorna el UC-034, continua con el paso siguiente | |
| 2. El sistema consulta API online de autoridades | | 2.A.1. El sistema no consigue los datos de las autoridades ya sea por fallo de conexión o en el propio servicio  2.A.2. El sistema consulta los datos locales en busca de contactos de las autoridades  2.A.3.A.1. El sistema encuentra la lista de autoridades y procede al paso 2  2.A.3.B.1. El sistema encuentra la lista de autoridades pero esta desactualizada (3+ meses)  2.A.3.B.2. El sistema reintenta (hasta 3 reintentos) conectarse a la API de consulta de autoridades  2.A.3.C.1. El sistema no encuentra la lista de autoridades  2.A.3.C.2. El sistema usa datos mínimos con los números de emergencia genéricos | |
| 3. El sistema filtra resultados por: ciudad o región, distancia (configurable, default 5km), tipo de autoridad y horario | | 3.A.1. El sistema no encuentra autoridades en el radio configurado  3.A.2. El sistema amplía radio de búsqueda progresivamente hasta 200km  3.A.3.A.1. El sistema encuentra resultados y continua en el siguiente paso  3.A.3.B.1. El sistema no encuentra resultados y recurre a números de emergencia genéricos | |
| 4. El sistema ordena resultados por proximidad y relevancia para el tipo de emergencia | |  | |
| 5. El sistema devuelve un listado con (máximo 5 resultados): nombre, dirección, teléfono, distancia y tiempo estimado de arrivo (ETA) | | 5.A.1. El sistema no tiene datos para devolver  5.A.2. El sistema registra y notifica el caso de fallo y continua en el paso 6 | |
| 6. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

### Modulo Finalización

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-014** | **Finalizar Alarma** | | |
| Descripción | Proceso central que permite al usuario desbloquear manualmente el dispositivo y terminar el modo de emergencia, restaurando el funcionamiento normal del teléfono y asegurando el cierre ordenado de todos los servicios activos. | | |
| Objetivo | Restaurar el control total del dispositivo al usuario legítimo una vez que la situación de emergencia ha concluido, asegurando que la alarma no continúe de manera indefinida y que se ejecuten los procesos de cierre adecuados. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Media | Prioridad | Muy Alta |
| Usa | UC-015 | Extiende | UC-008 |
| Pre-condiciones | El dispositivo está en modo de alarma activo (UC-001 en ejecución)  El usuario tiene acceso físico al dispositivo y conoce el método de autenticación  El hardware necesario para autenticación (lector de huellas, pantalla táctil, etc.) está operativo  La ventana de cancelación inicial (5-30 segundos) ha expirado | | |
| Post-condiciones | El modo de alarma se desactiva completamente  Todas las funciones de recolección de evidencias se detienen  Las conexiones con el Centro de Monitoreo se cierran apropiadamente con notificación de “Alarma finalizada”  Se libera el bloqueo del dispositivo restaurando la interfaz normal  Se muestra la encuesta post-alarma (UC-014) inmediatamente  Se registra en el historial la finalización manual | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario presiona en cualquier parte de la pantalla o interactúa con los botones del dispositivo. | | 1.A.1. El servidor del CdM envía señal de finalización remota autorizada  1.A.2. El sistema valida la señal y si es auténtica, procede a finalizar la alarma sin requerir autenticación local  1.A.3. El sistema notifica al usuario que la alarma fue desactivada remotamente, detiene todos los servicios de recolección de evidencias y desbloquea el dispositivo  1.A.4. Se muestra pantalla de resumen en lugar de encuesta completa y continua en el paso 11 | |
| 2. El sistema presenta interfaz de finalización de alarma, que consiste un botón con la leyenda “Finalizar Alarma”, superpuesta a la interfaz de alarma bloqueada | |  | |
| 3. El usuario pulsa el botón de finalizar alarma | |  | |
| 4. El sistema presenta interfaz de autenticación de emergencia (huella, patrón, PIN o contraseña) | | 4.A.1. El dispositivo se apaga o reinicia durante el proceso de finalización  4.A.2. El dispositivo al reiniciarse llamara al UC-008: Reactivar Alarma tras Reinicio pero detecta que estaba en proceso de finalización y continua en el paso 4 | |
| 5. El usuario ingresa credenciales válidas mediante el método de autenticación preferido o que tenga configurado | |  | |
| 6. El sistema valida correctamente las credenciales ingresadas contra el almacén seguro del dispositivo | | 6.A.1. El sistema no logra validar las credenciales utilizadas por el usuario  6.A.2.A.1. El sistema detecta que es el fallo número igual o menor a 3, y vuelve al paso 4  6.A.2.B.1. El sistema detecta que es el fallo número mayor a 3, y bloquea el reingreso de credenciales por 2 minutos mostrando un temporizador  6.A.2.B.2. El sistema envía notificación al CdM para que se registre el intento de desbloqueo fallido como actividad sospechosa | |
| 7. El sistema notifica al CdM que el estado de alarma ha finalizado y guarda registro del evento con timestamp actualizado | |  | |
| 8. El sistema detiene todos los servicios de recolección de evidencias (audio, fotos y geolocalización) | |  | |
| 9. El sistema libera el bloqueo de interfaz y restaura la pantalla principal | |  | |
| 10. El sistema muestra la pantalla de encuesta post-alarma (UC-015) | |  | |
| 11. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-015** | **Mostrar Encuesta Post-alarma** | | |
| Descripción | Presenta un cuestionario estructurado al usuario inmediatamente después de finalizar una alarma, con el objetivo de recabar información contextual sobre el incidente, el estado del usuario, respuesta de autoridades y efectividad del sistema. | | |
| Objetivo | Recopilar datos cualitativos y cuantitativos sobre el incidente que complementen las evidencias automáticas, facilitando el análisis posterior. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Baja | Prioridad | Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | La alarma ha sido finalizada exitosamente  El dispositivo está desbloqueado y con interfaz normal operativa  La batería del dispositivo es suficiente para completar la encuesta  El usuario está en condiciones físicas y mentales para responder (opcional, puede posponerse) | | |
| Post-condiciones | Las respuestas de la encuesta se almacenan localmente y se sincronizan con el Centro de Monitoreo  El historial de la alarma se actualiza con la información aportada  Se generan métricas de efectividad del sistema basadas en las respuestas  Si el usuario no completa la encuesta, se guarda como borrador y se puede completar más tarde  El sistema retorna al estado normal de funcionamiento | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| El sistema muestra pantalla modal de encuesta post-alarma con las siguientes secciones:  Obligatorias:   * Motivo de la activación (robo, agresión, accidente, falsa alarma, otro) * Estado físico de la persona (escala 1-5, opción “herido/ necesita asistencia”) * Intervención de autoridades (sí/no, cuáles, tiempo de respuesta, etc) * Efectividad percibida del sistema (escala 1-5)   Opcionales:   * Descripción detallada del incidente (texto libre) * Daños o pérdidas sufridas (si/no, en caso de opción positiva mostrar para cargar texto libre) * Sugerencias de mejora (texto libre)   Y al final mostrar dos botones: enviar cuestionario y completar más tarde | |  | |
| 2. El usuario completa los datos y presiona enviar cuestionario | | 2.A.1. El usuario completa -o no los datos y presiona completar más tarde.  2.A.2. El sistema guarda localmente un borrador con las respuesta cargadas y va al paso 6 | |
| 3. El sistema valida que los datos marcados como obligatorios estén completos | | 3.A.1. El sistema detecta que los datos obligatorios están faltando  3.A.2. El sistema indicara al usuario cual es el dato faltante en pantalla y va a hacer foco en el/los campo/s faltante/s | |
| 4. El sistema guarda las respuestas en base de datos local | |  | |
| 5. El sistema envía respuestas con el CdM inmediatamente | |  | |
| 6. El sistema cierra la encuesta y retorna a la pantalla principal de la aplicación | |  | |
| 7. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-016** | **Consultar Historial del Usuario** | | |
| Descripción | Permite al usuario acceder a un registro local y/o remoto de todas las alarmas activadas en el pasado, incluyendo detalles como fecha, hora, método de activación, acciones tomadas por el sistema, evidencias capturadas y respuestas de encuestas. | | |
| Objetivo | Proveer al usuario de un medio para consultar incidentes pasados. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Baja | Prioridad | Media |
| Usa | No | Extiende | No |
| Pre-condiciones | El usuario ha iniciado sesión en la aplicación móvil  Existe al menos una alarma registrada en el historial | | |
| Post-condiciones | El usuario visualiza la lista de alarmas pasadas ordenadas cronológicamente con información de resumen  El usuario puede acceder a detalles específicos de cada alarma, incluyendo mapas, metadatos y respuestas de encuesta  Los datos remotos se sincronizan con el local para consistencia  El usuario puede exportar o compartir reportes específicos | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario navega a la sección “Consulta de Alarmas” desde el menú principal de la aplicación | |  | |
| 2. El sistema recupera el historial combinado: Primero carga desde base de datos local (rápido) y en segundo plano, sincroniza con servidor remoto para actualizar/recuperar historial completo | |  | |
| 3. El sistema muestra lista paginada con: fecha/hora, método de activación, estado (cancelada/completada/falsa), ubicación aproximada e icono de resumen, también permite aplicar filtros al usuario y también refrescar los datos | |  | |
| 4. El usuario selecciona una alarma específica de la lista | | 4.A.1. El usuario selecciona exportar la lista completa (o la sección filtrada)  4.A.2. El sistema genera archivo ZIP con:  - CSV estructurado con metadatos  - PDF de resumen estadístico  - Evidencias comprimidas (si usuario autoriza y hay espacio)  4.A.3. El sistema permite compartir el archivo vía métodos seguros (app propia, email cifrado, etc.) y continua en el paso 6 | |
| 5. El sistema muestra vista detallada con pestañas organizadas:   * Resumen (línea de tiempo del evento, duración, contactos notificados, etc) * Ubicación (mapa interactivo con puntos de ubicación o camino recorrido durante la alarma) * Evidencias (datos de fotos/audio -miniaturas, duraciones, timestamps-) * Encuesta (respuestas proporcionadas -si fue completada-) * Comentarios CdM (observaciones del CdM -si las hay-) | |  | |
| 6. El usuario cierra vista detallada y retorna a lista y sale de la vista de Consulta de Alarmas | |  | |
| 7. Fin del CU | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

### Modulo Configuracion

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-017** | **Gestionar Preferencias del Usuario** | | |
| Descripción | Permite al usuario configurar y personalizar todos los aspectos operativos de la aplicación, incluyendo métodos de activación, umbrales de sensibilidad, comportamientos durante emergencia y parámetros de privacidad. | | |
| Objetivo | Proveer una interfaz intuitiva y segura para que el usuario personalice el comportamiento del sistema de seguridad según sus necesidades específicas, hábitos de uso y nivel de riesgo percibido. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Alta |
| Usa | No | Extiende | no |
| Pre-condiciones | El usuario ha iniciado sesión en la aplicación  La aplicación tiene acceso a almacenamiento local para guardar preferencias  El usuario tiene permisos de administración sobre la aplicación | | |
| Post-condiciones | Todas las preferencias modificadas se guardan de forma persistente (local y sincronizadas con la nube)  Los cambios se aplican inmediatamente o al reiniciar servicios específicos  El sistema opera con los nuevos parámetros configurados  Se notifica al usuario que los cambios fueron aplicados exitosamente | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario accede a la sección "Configuración" desde el menú principal de la aplicación | |  | |
| 2. El sistema muestra pantalla de configuración con pestaña "General" seleccionada por defecto y presenta:   * Cabecera: con título de la pestaña y botones de desplazamiento y botón para ver categorías de configuración * Panel central: opciones de la categoría seleccionada * Barra inferior: botones Guardar, Cancelar y Restaurar. | |  | |
| 3. El usuario navega entre categorías mediante botones atrás(<) y siguiente(>) para secuencia circular o hace uso del menú contextual de selección directa | |  | |
| 4. El sistema responde a cada interacción del usuario yendo a la categoría seleccionada y presenta las opciones en el panel central | | 4.A.1. El sistema detecta que la pestaña es la de Contactos, y llama de forma embebida dentro del panel central al UC-018 y continua en el paso siguiente  4.B.1. El sistema detecta que la pestaña es la de Permisos, y llama de forma embebida dentro del panel central al UC-019 y continua en el paso siguiente | |
| 5. El usuario configura opciones disponibles y presiona en el botón guardar | | 5.A.1. El usuario presiona el botón cancelar  5.A.2. El sistema muestra dialogo de confirmación para cancelar los cambios  5.A.3.A.1. El usuario selecciona si  5.A.3.A.2. El sistema descarta los cambios y continua en el paso 9  5.A.3.B.1. El usuario selecciona no  5.A.3.B.2. El sistema cierra el dialogo y vuelve el foco al último cambio del usuario  5.B.1. El usuario presiona el botón restaurar  5.B.2. El sistema muestra dialogo de confirmación para restaurar la configuración por defecto  5.B.3.A.1. El usuario selecciona si  5.B.3.A.2. El sistema restaura la configuración por defecto y continua en el paso 7  5.B.3.B.1. El usuario selecciona no  5.B.3.B.2. El sistema cierra el dialogo y vuelve el foco al último cambio del usuario | |
| 6. El sistema valida consistencia de configuraciones | | 6.A.1. El sistema encuentra inconsistencias en la configuración  6.A.2. El sistema muestra en pantalla los errores de la configuración y continua al paso 5. | |
| 7. El sistema guarda configuración y aplica cambios | |  | |
| 8. El sistema vuelve a pantalla principal | |  | |
| 9. Fin del UC | |  | |
| Comentarios | Ver UI de Configuración | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-018** | **Gestionar Contactos de Emergencia** | | |
| Descripción | Permite al usuario definir, organizar y mantener una lista de contactos de confianza que serán notificados en caso de emergencia, especificando para cada uno los canales de comunicación preferidos y el orden de notificación. | | |
| Objetivo | Asegurar que en situación de emergencia, las personas correctas sean notificadas por los canales seleccionados efectivos, maximizando la probabilidad de respuesta rápida y adecuada. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Muy Alta |
| Usa | No | Extiende | UC-017 |
| Pre-condiciones | El usuario ha concedido permisos para acceder a la agenda de contactos  La aplicación tiene acceso a almacenamiento local para guardar la lista de contactos de emergencia  El usuario tiene al menos un método de contacto configurado en su perfil  La sesión del usuario es válida y activa | | |
| Post-condiciones | La lista de contactos de emergencia está actualizada con todos los cambios realizados  Para cada contacto, se almacenan los canales de notificación preferidos y el orden de prioridad  Los contactos están validados (formato correcto, canales disponibles verificados cuando es posible)  La configuración se sincroniza con el servidor para backup  El sistema está listo para notificar a estos contactos en caso de emergencia (UC-008) | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. Usuario accede a "Contactos de Emergencia" desde la sección de Configuración | |  | |
| 2. Sistema muestra lista actual de contactos de emergencia con:  Nombre  Relación (familiar, amigo, colega, etc.)  Canales de notificación (teléfono, WhatsApp, Telegram, SMS, etc)  Dirección (opcional)  botones de editar y eliminar por cada fila  y botones de añadir contacto, ordenar contactos, guardar y cancelar | |  | |
| 3. El usuario selecciona añadir contacto | | 3.A.1. El usuario selecciona un contacto y presiona eliminar  3.A.2. El sistema muestra dialogo de confirmación para la eliminación del contacto  3.A.3.A.1. El usuario selecciona confirmar  3.A.3.A.2. El sistema elimina la fiila seleccionada, refresca la lista y continua en el paso 2  3.A.3.B.1. El usuario selecciona cancelar  3.A.3.B.1. El sistema cierra el dialogo y vuelve el foco al ultimo elemento seleccionado  3.B.1. El usuario selecciona un contacto y presiona editar  3.B.2. El sistema muestra pantalla de edición de contacto  3.B.3.A.1. El usuario selecciona confirmar  3.B.3.A.2. El sistema sigue en el paso 8  3.B.3.B.1. El usuario selecciona cancelar  3.B.3.B.2. El sistema descarta los cambios, cierra pantalla de edición, refresca la lista y continua en el paso 2  3.C.1. El usuario selecciona ordenar contactos  3.C.2. El sistema muestra botones de posición –primero, arriba, abajo, ultimo- para posicionar la fila seleccionada y botones de confirmar y cancelar  3.C.3. El sistema también habilita que las filas de la lista se puedan ordenar arrastrándolas de lugar  3.C.4.A.1. El usuario selecciona confirmar  3.C.4.A.2. El sistema sigue en el paso 9  3.C.4.B.1. El usuario selecciona cancelar  3.C.4.B.2. El sistema descarta los cambios, cierra pantalla de ordenación, refresca la lista y continua en el paso 2 | |
| 4. El sistema muestra opción de importar contacto o ingreso manual | |  | |
| 5. El usuario selecciona importar contacto | | 3.B.1. El usuario selecciona ingresar manualmente  3.B.2. El sistema muestra pantalla de creación de nuevo contacto  3.B.3.A.1. El usuario selecciona confirmar  3.B.3.A.2. El sistema sigue en el paso 8  3.B.3.B.1. El usuario selecciona cancelar  3.B.3.B.2. El sistema descarta los cambios, cierra pantalla de edición, refresca la lista y continua en el paso 2 | |
| 6. El sistema muestra en una pantalla el listado de la agenda de contactos | |  | |
| 7. El usuario selecciona uno o varios contactos (hasta un máximo de 200) y confirma la accion | |  | |
| 8. El sistema valida que el formato del número de contacto y/o el mail sean correctos y el canal elegido este disponible | | 8.A.1. El sistema detecta que los valores introducidos no son correctos  8.A.2. muestra información y ubicación de los errores y vuelve al foco al elemento con datos no validos | |
| 9. El sistema guarda temporalmente los datos, cierra pantalla abierta y refresca la lista de contactos de emergencia | |  | |
| 10. El usuario presiona botón guardar | | 10.A.1. El usuario presiona botón cancelar o intenta salir de la pantalla  10.A.2. El sistema muestra dialogo de confirmación de cancelar los cambios  10.A.3.A.1. El usuario selecciona si  10.A.3.A.2. El sistema descarta los cambios y continua en el paso 2  10.A.3.B.1. El usuario selecciona no  10.A.3.B.1. El sistema cierra el dialogo y continua en el paso 2 | |
| 11. El sistema guarda los datos localmente y sincroniza con el servidor en segundo plano | |  | |
| 12. Fin del UC | |  | |
| Comentarios | Ver UI de creación/edición de contacto | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-019** | **Gestionar Permisos del Dispositivo** | | |
| Descripción | Gestiona la solicitud de todos los permisos del sistema operativo requeridos por la aplicación para su óptimo funcionamiento, explicando al usuario el propósito de cada permiso y las consecuencias de denegarlo. | | |
| Objetivo | Asegurar que la aplicación tenga los permisos necesarios para operar efectivamente, informando al usuario sobre por qué se requieren ciertos permisos y facilitando la gestión de estos a lo largo del ciclo de vida de la aplicación. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Medio | Prioridad | Alta |
| Usa | No | Extiende | UC-017 |
| Pre-condiciones | La aplicación está instalada y tiene una versión compatible con el sistema operativo  El usuario tiene permisos de administración sobre el dispositivo  El sistema operativo soporta el modelo de permisos requerido | | |
| Post-condiciones | Todos los permisos críticos están concedidos o denegados explícitamente por el usuario  La aplicación ajusta su funcionalidad según los permisos disponibles  El usuario comprende qué funcionalidades están limitadas por falta de permisos  El sistema registra el estado de permisos para diagnóstico y sugerencias proactivas | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario navega hacia la pestaña “Permisos” desde la sección de configuración | |  | |
| 2. El sistema muestra interfaz donde se muestran los permisos a las funcionalidades que la aplicación necesita para su correcto funcionamiento divididos en categorías:   * Críticos (ubicación, cámara, micrófono) * Importantes (contactos, SMS, almacenamiento) * Especiales (notificaciones, inicio automático, ejecución en segundo plano) | |  | |
| 3. El sistema muestra por cada funcionalidad una descripción, el estado actual (seleccionador con las opciones –permitir, solo con la app en uso, denegar-) y una notificación con la explicación de la necesidad del permiso y su función y las consecuencias de no otorgarlo | |  | |
| 4. El usuario otorga permiso a una funcionalidad | | 4.A.1. El usuario deniega permiso a una funcionalidad.  4.A.2. El sistema actualiza estado localmente  4.A.3. deshabilita o limita funcionalidades dependientes  4.A.4. Muestra advertencia sobre limitaciones que la app va a tener | |
| 5. El sistema solicita permiso al SO del dispositivo mediante diálogo nativo | |  | |
| 6. El SO del dispositivo concede el permiso, actualiza estado y habilita funcionalidades asociadas | | 6.A.1. El SO del dispositivo deniega el permiso  6.A.2. El sistema muestra explicación de por qué se denegó y ofrece una guía alternativa para obtener el permiso manualmente | |
| 7. El sistema actualiza el estado del permiso en la lista | |  | |
| 8. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

### Modulo Autenticación

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-020** | **Registrar Usuario** | | |
| Descripción | Proceso inicial de creación de una nueva cuenta en la aplicación donde el usuario proporciona información personal básica, establece credenciales de acceso y acepta los términos y condiciones del servicio. | | |
| Objetivo | Crear una identidad digital segura y única para cada usuario, validando su identidad mínimamente y estableciendo las bases para la personalización y uso de todas las funcionalidades del sistema. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Medio | Prioridad | Alta |
| Usa | UC-017, UC-026 | Extiende | No |
| Pre-condiciones | La aplicación está instalada y es la primera ejecución o usuario selecciona "Crear cuenta"  El dispositivo tiene conectividad a internet  El usuario tiene acceso a un email o número de teléfono válido  El dispositivo cumple requisitos mínimos del sistema  El usuario acepta los términos y condiciones | | |
| Post-condiciones | Se crea una nueva cuenta con estado pendiente de verificación  Se envía código de verificación al email/teléfono proporcionado  Se almacenan temporalmente los datos de registro  Se habilita flujo de verificación de identidad  Se registra el intento de registro para auditoría | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario selecciona "Crear cuenta" desde el inicio de sesión en el dispositivo | |  | |
| 2. El sistema muestra formulario con lo siguiente:   * campos obligatorios (nombre completo, email, teléfono, contraseña, confirmar contraseña) * campos opcionales (dirección, fecha nacimiento, foto perfil) * check para aceptar términos y condiciones y link a documentación * botones de registrar (inicialmente deshabilitado) y cancelar | |  | |
| 3. El usuario llena los campos necesarios y chequea en aceptar términos y condiciones | |  | |
| 4. El sistema valida que los datos obligatorios están ingresados y cumplan con el formato necesario | | 4.A.1. El sistema detecta que los datos ingresados no cumplen con el formato necesario y muestra mensaje de error por campo y vuelve al paso 2 | |
| 5. El sistema habilita el botón registrar | |  | |
| 6. El usuario presiona sobre el botón registrar | |  | |
| 7. El sistema valida que el mail o el número de teléfono, no estén registrados con otra cuenta | | 7.A.1. El sistema detecta que el mail ya esta registrado bajo otra cuenta  7.A.2. El sistema notifica al usuario del error y ofrece corregir el mail o recuperar contraseña  7.A.3.A.1. El usuario cambia el mail  7.A.3.A.2. El sistema vuelve al paso 7  7.A.3.B.1. El usuario selecciona recuperar contraseña  7.A.3.B.1. El sistema llama al recuperar contraseña (UC-025)  7.B.1. El sistema detecta que el número de teléfono está registrado con otra cuenta  7.B.2. El sistema notifica al usuario y ofrece corregir el número de teléfono o desvincular el teléfono  7.B.3.A.1. El usuario cambia el numero  7.B.3.A.2. El sistema vuelve al paso 7  7.B.3.B.1. El usuario selecciona desvincular teléfono  7.B.3.B.2. El sistema procede a desvincular el teléfono y ejecuta el UC-026, luego si la desvinculación fue positiva continua en el paso 9 | |
| 8. El sistema guarda los datos de la persona transitoriamente con estado de pendiente de verificación | |  | |
| 9. El sistema envía un mail con un código de verificación, y muestra en pantalla un campo para introducir el código, un mensaje al usuario para que revise su correo y un botón para volver a reenviar el código. | |  | |
| 10. El usuario introduce el código enviado en el mail | |  | |
| 11. El sistema valida que el código coincida con el enviado por correo y guarda el estado de la cuenta en activa | | 11.A.1. El sistema detecta que el código ingresado es incorrecto y notifica al usuario y vuelve al paso 9 | |
| 12. El sistema procede a registrar el teléfono de la cuenta y ejecuta el UC-026 | |  | |
| 13. El sistema procede a presentar las configuraciones iniciales de la cuenta y ejecuta el UC-017 | |  | |
| 14. Fin de UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-021** | **Iniciar Sesion Usuario** | | |
| Descripción | Proceso específico de autenticación para usuarios de la aplicación, que verifica credenciales y establece una sesión segura en el dispositivo. | | |
| Objetivo | Permitir a usuarios móviles acceder a su cuenta de manera segura, proporcionando acceso personalizado a su perfil, configuración y funcionalidades. | | |
| Actor | Usuario | Actores Sec. | Servicio Auth |
| Complejidad | Media | Prioridad | Muy Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | El usuario tiene cuenta registrada y activa  No hay sesión activa o la sesión previa expiró  El dispositivo no está bloqueado por demasiados intentos | | |
| Post-condiciones | Se establece sesión autenticada  Se carga perfil del usuario, preferencias y datos personales  Se registra el evento de inicio de sesión para auditoría  Se habilitan todas las funcionalidades según nivel de acceso  Se sincronizan datos pendientes desde servidor | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario abre la aplicación no estando autenticado | |  | |
| 2. El sistema muestra formulario con: usuario, contraseña, opción "Recordarme",  botones de iniciar sesión, iniciar sesión con cuenta de Google/Facebook, iniciar sesión con huella, links a “Registrarse” y “¿Olvido su contraseña?” | |  | |
| 3. El usuario ingresa credenciales y selecciona "Iniciar Sesión" | | 3.A.1. El usuario selecciona Registrarse  3.A.2. El sistema ejecuta el UC-020 registrar usuario  3.B.1. El usuario selecciona recuperar contraseña  3.B.2. El sistema ejecuta el UC-023 recuperar contraseña | |
| 4. El sistema realiza validaciones básicas de formato y utiliza el servicio de autenticación | | 4.A.1. El sistema detecta que la cuenta no existe  4.A.2. El sistema muestra cartel de error y aumenta contador de fallos  4.A.3.A.1. El sistema detecta que el contador de fallos es menor a 3, y continua en el paso 2  4.A.3.B.1. El sistema detecta que el contador de fallos es mayor a 3, y bloquea la autenticación por 3 minutos y continua en el paso 2  4.B.1. El sistema detecta que la contraseña no tiene el formato necesario  4.B.2. El sistema muestra cartel de error y aumenta contador de fallos  4.B.3.A.1. El sistema detecta que el contador de fallos es menor a 3, y continua en el paso 2  4.B.3.B.1. El sistema detecta que el contador de fallos es mayor a 3, y bloquea la autenticación por 3 minutos y continua en el paso 2 | |
| 5. El servicio de autenticación verifica identidad con las credenciales y retorna token de seguridad, y datos del perfil | | 5.A.1. El servicio de autenticación no logro verificar las credenciales ingresadas por el usuario  5.A.2. El sistema muestra el mensaje de error que devuelve el servicio de autenticación y aumenta contador de fallos  5.A.3.A.1. El sistema detecta que el contador de fallos es menor a 3, y continua en el paso 2  5.A.3.B.1. El sistema detecta que el contador de fallos es mayor a 3, y bloquea la autenticación por 3 minutos y continua en el paso 2 | |
| 6. El sistema carga los datos de perfil, cifra y guarda token de forma segura y sincroniza configuracion del dispositivo | | 6.A.1. El sistema verifica que el dispositivo no está vinculado a la cuenta  6.A.2. El sistema llama al UC-024 para registrar el dispositivo a la cuenta | |
| 7. El sistema cierra interfaz de logueo y redirige a pantalla principal | |  | |
| 8. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-022** | **Cerrar Sesión Usuario** | | |
| Descripción | Proceso mediante el cual un usuario finaliza de manera segura su sesión, invalidando tokens y limpiando datos sensibles. | | |
| Objetivo | Proteger información personal cuando se comparte el dispositivo o cuando el usuario desea asegurar que nadie más pueda acceder a su cuenta desde ese dispositivo. | | |
| Actor | Usuario | Actores Sec. | Servicio Aut. |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | Existe una sesión activa de usuario en la aplicación móvil  La aplicación no está en modo de emergencia activa | | |
| Post-condiciones | Los tokens de autenticación se invalidan en servidor  Datos sensibles se eliminan de memoria de la aplicación  Credenciales almacenadas localmente se eliminan (excepto si selecciono "Recordarme")  Aplicación retorna al estado de no autenticado | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. Usuario accede al menú de perfil y selecciona "Cerrar Sesión" | |  | |
| 2. El sistema muestra diálogo de confirmación con opciones: cerrar sesion, cerrar sesión en todos los dispositivos y cancelar | |  | |
| 3. El usuario confirma seleccionando "Cerrar sesión" | | 3.A.1. El usuario cancela la operación  3.A.2. El sistema continua en el paso 8  3.B.1. El usuario selecciona cerrar sesión en todos los dispositivos  3.B.2. El sistema busca todos los dispositivos vinculados a la cuenta  3.B.3. El sistema envía solicitud de invalidación para cada dispositivo al servicio de autenticación y continua en el paso 5 | |
| 4. El sistema envía solicitud de invalidación al servicio de autenticación | |  | |
| 5. El sistema elimina token local del almacenamiento | |  | |
| 6. El sistema limpia datos sensibles de memoria | |  | |
| 7. El sistema redirige a pantalla de inicio de sesión y muestra mensaje de confirmación de sesión cerrada | |  | |
| 8. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-023** | **Recuperar Contraseña** | | |
| Descripción | Proceso automatizado que permite a un usuario recuperar su contraseña de acceso cuando la ha olvidado, mediante verificación de identidad a través de métodos alternativos registrados. | | |
| Objetivo | Restablecer acceso a la cuenta de manera segura sin comprometer la seguridad, asegurando que solo el propietario legítimo pueda cambiar la contraseña. | | |
| Actor | Usuario | Actores Sec. | n/a |
| Complejidad | Media | Prioridad | Media |
| Usa | No | Extiende | No |
| Pre-condiciones | El usuario tiene cuenta registrada y activa  El usuario tiene acceso al email/teléfono asociado a la cuenta  No se excedieron intentos de recuperación permitidos  La cuenta no está bloqueada por actividades sospechosas | | |
| Post-condiciones | Se envía enlace/código de recuperación al método de contacto verificado  Se habilita temporalmente la posibilidad de establecer una nueva contraseña  Después de que la contraseña haya sido cambiada, se invalidan todas las sesiones activas | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El usuario selecciona "¿Olvido su contraseña?" desde pantalla de login | |  | |
| 2. El sistema muestra formulario para identificar cuenta con mail o número de teléfono | |  | |
| 3. El usuario ingresa mail y presiona en recuperar contraseña | | 3.A.1. El usuario ingresa un numero de telefono y presiona en recuperar contraseña y continua en el paso siguiente | |
| 4. El sistema valida que la cuenta exista y que está activa | | 4.A.1. El sistema detecta que el mail o el telefono ingresados no pertenecen a ninguna cuenta  4.A.2. El sistema aumenta el contador de recuperos fallidos  4.A.3.A.1. El sistema detecta que el número de fallos es igual o menor a 3 y vuelve al paso 2  4.A.3.B.1. El sistema detecta que el número de fallos es mayor a 3  4.A.3.B.2. El sistema bloquea por 15 mins otro intento de recuperación.  4.B.1. El sistema detecta que la cuenta está bloqueada y muestra mensaje al usuario con el número de contacto al CdM  4.B.2. El sistema muestra mensaje de error al usuario con el número de contacto al CdM para desbloquear la cuenta | |
| 5. El sistema envía un correo con una clave que expira a los 10 mins a la cuenta indicada y muestra pantalla para ingresar código y/o volver a enviar si expiro | | 5.A.1. El sistema envía un SMS con una clave que expira a los 3 mins al número indicado  5.A.2. El sistema muestra una pantalla para ingresar el código recibido y/o volver a enviar si expiro | |
| 6. El usuario ingresa el código que le llego por mail | |  | |
| 7. El sistema valida que el código ingresado sea válido y no haya expirado | | 7.A.1. El sistema verifica que el codigo ingresado no es valido o ha expirado  7.A.2. El sistema aumenta el contador de recuperos fallidos  7.A.3.A.1. El sistema detecta que el número de recuperos es menor o igual a 3 y vuelve al paso 5.  7.A.3.B.1. El sistema detecta que el número de recuperos es mayor a 3  7.A.3.B.2. El sistema procede a bloquear la cuenta  7.A.3.B.3. El sistema muestra mensaje de error al usuario con el número de contacto al CdM para desbloquear la cuenta | |
| 8. El sistema muestra una pantalla para el ingreso de nueva contraseña y su confirmación | |  | |
| 9. El sistema valida que ambas contraseñas coincidan, tengan el formato correcto y no se hayan utilizado previamente | | 9.A.1. El sistema detecta que las contraseñas no coinciden y muestra mensaje de error  9.B.1. El sistema detecta que la contraseña ya fue utilizada con anterioridad por el usuario y muestra mensaje de error | |
| 10. El sistema guarda la contraseña e invalida las sesiones abiertas | |  | |
| 11. El sistema redirige a pantalla de login con mensaje "Contraseña actualizada" | |  | |
| 12. Fin de UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-024** | **Registrar Dispositivo** | | |
| Descripción | Proceso de vinculación formal de un dispositivo físico (smartphone) con la cuenta de usuario, creando perfil único del dispositivo para personalización. | | |
| Objetivo | Identificar de manera única cada dispositivo asociado a una cuenta, permitiendo características personalizadas por dispositivo | | |
| Actor | n/a | Actores Sec. | Usuario |
| Complejidad | Media | Prioridad | Media |
| Usa | No | Extiende | No |
| Pre-condiciones | Usuario completó registro o inició sesión exitosamente  La aplicación tiene permisos para acceder a identificadores únicos del dispositivo  El dispositivo no está actualmente registrado con esta cuenta  Existe conectividad a internet para sincronizar con servidor | | |
| Post-condiciones | Se crea perfil único del dispositivo en base de datos del sistema  Se generan y almacenan configuraciones específicas para este dispositivo  Se configuran preferencias por defecto específicas para este tipo de dispositivo  Se establece relación cuenta-dispositivo con permisos y restricciones apropiadas  El dispositivo aparece en lista de "Dispositivos conectados" en perfil del usuario | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema recopila información sobre el dispositivo: IMEI, numero de teléfono, modelo, marca, SO, características del hardware, resolución, idioma, zona horaria, etc. | |  | |
| 2. El sistema envía información al servidor con: ID de usuario autenticado, token sesión y los datos del dispositivo | |  | |
| 3. El sistema valida que el usuario puede registrar nuevo dispositivo, genera ID para el dispositivo, nombre descriptivo, tipo dispositivo y fecha de registro | | 3.A.1. El sistema detecta que el dispositivo esta vinculado a otra cuenta activa  3.A.2. El sistema notifica al email de la cuenta que el dispositivo está tratando de ser vinculado a otra cuenta y ofrece desvincular dispositivo o informar actividad sospechosa  3.A.3. El sistema informa al usuario que el dispositivo está siendo usado por otra cuenta activa y va al paso 6  3.B.1. La sistema detecta que la cuenta ya tiene la cantidad máxima de dispositivos vinculados  3.B.2. El sistema informa al usuario que deberá desvincular algún dispositivo para vincular el nuevo móvil y ofrece desvincular dispositivo | |
| 4. El sistema asocia el dispositivo a la cuenta del usuario | |  | |
| 5. El Sistema muestra mensaje de “dispositivo vinculado exitosamente” | |  | |
| 6. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-025** | **Gestionar Operadores** | | |
| Descripción | Proceso administrativo que permite al Administrador del Centro de Monitoreo crear, modificar, desactivar y gestionar cuentas de operadores que utilizarán la plataforma web del CdM | | |
| Objetivo | Mantener control centralizado y seguro sobre personal autorizado para acceder al sistema de monitoreo, asegurando que solo personas validadas con permisos adecuados puedan responder a alarmas. | | |
| Actor | Administrador CdM | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | El Administrador inició sesión en plataforma web con credenciales de administrador  El sistema de gestión de usuarios está operativo y accesible  El Administrador tiene permisos de administración completos sobre módulo de operadores | | |
| Post-condiciones | Se registran nuevos operadores, se modifican sus datos o bien se da de baja operadores del CdM  Los operadores afectados reciben notificaciones de los cambios aplicados  Todos los cambios hechos quedan registrados en el sistema de auditoría con timestamp y administrador responsable | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El administrador de CdM accede a "Gestión de Operadores" desde panel de administración del panel de control del CdM | |  | |
| 2. El sistema muestra lista de operadores existentes con: nombre, legajo, estado, rol, último acceso y acciones: editar, eliminar, habilitar/deshabilitar, restablecer contraseña, ver historial y un botón en la cabecera para añadir nuevo | |  | |
| 3. El administrador de CdM selecciona añadir un operador | | 3.A.1. El administrador selecciona editar operador  3.A.2. El sistema muestra el formulario de añadir, pero con el legajo deshabilitado y sin contraseña temporal y continua en el paso 5  3.B.1. El administrador selecciona eliminar operador  3.B.2. El sistema muestra dialogo de confirmación y que seleccione un motivo y/o ponga un texto a su elección  3.B.3.A.1. El administrador selecciona un motivo y presiona confirmar  3.B.3.A.2. El sistema borra el usuario, crea un registro de auditoria con el motivo, el responsable y la fecha  3.B.3.A.3. El sistema refresca la lista y continua en el paso 2  3.B.3.B.1. El administrador no selecciona un motivo y presiona confirmar  3.B.3.B.2. El sistema muestra mensaje de error para que se seleccione el motivo  3.B.3.C.1. El administrador presiona cancelar  3.B.3.C.2. El sistema sigue en el paso 2  3.C.1. El administrador selecciona habilitar o deshabilitar un operador  3.C.2. El sistema muestra un dialogo de confirmación para habilitar o deshabilitar el operador y pide seleccionar un motivo y/o ponga un texto a su elección.  3.C.3.A.1. El administrador selecciona un motivo y presiona confirmar  3.C.3.A.2. El sistema habilita o deshabilita el usuario según sea seleccionado  3.C.3.A.3. El sistema crea un registro de auditoria con el motivo, el responsable y la fecha  3.C.3.A.4. El sistema envía un correo al mail del operador indicándole el estado de su cuenta, el motivo del cambio y por quien fue hecho  3.C.3.A.5. El sistema refresca la lista y continua en el paso 2  3.C.3.B.1. El administrador no selecciona un motivo y presiona confirmar  3.C.3.B.2. El sistema muestra mensaje de error para que se seleccione el motivo  3.C.3.C.1. El administrador presiona cancelar  3.C.3.C.2. El sistema sigue en el paso 2  3.D.1. El administrador selecciona restablecer contraseña  3.D.2. El sistema ejecuta el UC-028 restablecer contraseña  3.E.1. El administrador selecciona ver historial  3.E.2. El sistema ejecuta el UC-033 consultar historial CdM filtrado por operador seleccionado y continua en el paso 2 | |
| 4. El sistema muestra un formulario para cargar datos personales (nombre, dirección, correo institucional, teléfono), legajo, rol –operador, administrador-, turno del operador y botones de aceptar y cancelar | |  | |
| 5. El administrador de CdM llena los datos personales y presiona aceptar | |  | |
| 6. El sistema valida que los datos cumplan el formato necesario y se respete la unicidad de la dirección de correo y el legajo. | | 6.A.1. El sistema detecta que los datos no tienen formato correcto y muestra mensaje de error en los campos no validos  6.B.1. El sistema verifica que el correo ya está designado a otro operador en activo  6.B.2. El sistema muestra mensaje de error de unicidad de correo | |
| 7. El sistema guarda los datos del operador con estado pendiente de activación | |  | |
| 8. El sistema ejecuta el UC-026 restablecer contraseña | |  | |
| 9. El sistema muestra mensaje de operación exitosa y refresca la lista | |  | |
| 10. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-026** | **Iniciar Sesion CdM** | | |
| Descripción | Proceso de autenticación específico para operadores del Centro de Monitoreo que acceden a la plataforma web administrativa del CdM | | |
| Objetivo | Controlar el acceso a la plataforma de monitoreo asegurando que solo personal autorizado pueda visualizar y gestionar las alarmas. | | |
| Actor | Operador, Administrador CdM | Actores Sec. | Servicio Auth |
| Complejidad | Media | Prioridad | Media |
| Usa | No | Extiende | UC-028 |
| Pre-condiciones | El operador tiene cuenta creada y activa  El operador tiene acceso a dispositivo autorizado  El operador conoce sus credenciales de acceso  El sistema de autenticación está operativo  No hay sesión activa previa para este operador | | |
| Post-condiciones | Se establece sesión autenticada  Se carga interfaz de monitoreo con alarmas activas y datos relevantes  Se registra el evento de inicio de sesión para auditoría  Se activan notificaciones en tiempo real para nuevas alarmas según turno y zona asignada  Se muestra estado del operador como "disponible" para asignación de nuevas alarmas | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El operador accede a la plataforma web del CdM desde una terminal autorizada | |  | |
| 2. El sistema muestra formulario con: usuario, contraseña y botones de iniciar sesión y restablecer contraseña | |  | |
| 3. El operador ingresa credenciales y selecciona "Iniciar Sesión" | | 3.A.1. El operador selecciona Restablecer contraseña  3.A.2. El sistema envía un mail al administrador de CdM con un texto por defecto informando que el operador necesita restablecer la contraseña | |
| 4. El sistema realiza validaciones básicas de formato y utiliza el servicio de autenticación | | 4.A.1. El sistema detecta que la cuenta no existe o la contraseña es incorrecta  4.A.2. El sistema muestra cartel de error y aumenta contador de fallos  4.A.3.A.1. El sistema detecta que el contador de fallos es menor a 3, y continua en el paso 2  4.A.3.B.1. El sistema detecta que el contador de fallos es mayor a 3, deshabilita la cuenta del operador y continua en paso 8  4.B.1. El sistema detecta que la cuenta no existe o la contraseña es incorrecta  4.B.2. El sistema muestra cartel de error, aumenta contador de fallos y muestra opción de restablecer contraseña  4.A.3.A.1. El sistema detecta que el contador de fallos es menor a 3, y continua en el paso 2  4.A.3.B.1. El sistema detecta que el contador de fallos es mayor a 3, deshabilita la cuenta del operador y continua en paso 8  4.C.1. El sistema detecta que es una cuenta bloqueada o dada de baja  4.C.2. El sistema muestra error en pantalla y le indica al operador que debe comunicarse con el administrador del CdM y continua en el paso 8  4.D.1. El sistema detecta que la contraseña es transitoria  4.D.2. El sistema muestra en pantalla dos campos para ingresar nueva contraseña, confirmación de contraseña y botón de aceptar  4.D.3. El sistema valida que la nueva contraseña cumpla con el formato requerido y no se haya utilizado antes  4.D.4. El sistema guarda la nueva contraseña, muestra mensaje de actualización de contraseña exitosa y vuelve al paso 2 | |
| 5. El servicio de autenticación verifica identidad con las credenciales y retorna token de seguridad, y datos del operador | | 5.A.1. El servicio de autenticación no logro verificar las credenciales ingresadas por el operador  5.A.2. El sistema muestra el mensaje de error que devuelve el servicio de autenticación y aumenta contador de fallos  5.A.3.A.1. El sistema detecta que el contador de fallos es menor a 3, y continua en el paso 2  5.A.3.B.1. El sistema detecta que el contador de fallos es mayor a 3, deshabilita la cuenta del operador y continua en paso 8 | |
| 6. El sistema carga los datos del operador, cifra y guarda token de forma segura | |  | |
| 7. El sistema cierra interfaz de logueo y redirige a pantalla principal | |  | |
| 8. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-027** | **Cerrar Sesión CdM** | | |
| Descripción | Proceso mediante el cual un operador del Centro de Monitoreo finaliza de manera segura su sesión en la plataforma web administrativa del CdM | | |
| Objetivo | Garantizar que al finalizar el turno o al ausentarse, el operador no deje sesión activa que pueda ser utilizada por personas no autorizadas. | | |
| Actor | Operador CdM | Actores Sec. | Servicio Aut |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | Existe una sesión activa de un operador en la plataforma web  El operador ha terminado su turno o necesita cerrar sesión  La plataforma web está operativa y tiene conectividad con servidor de autenticación | | |
| Post-condiciones | El token de sesión se invalida en el servidor  Se eliminan datos de sesión del lado del cliente  Se registra evento de cierre de sesión en logs de auditoría  El operador es marcado como "no disponible" en sistema de asignación | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. Usuario accede al menú de perfil y selecciona "Cerrar Sesión" | |  | |
| 2. El sistema muestra diálogo de confirmación "¿Está seguro que desea cerrar sesion?" | |  | |
| 3. El operador confirma seleccionando "Confirmar" | | 3.A.1. El operador cancela la operación  3.A.2. El sistema continua en el paso 8 | |
| 4. El sistema envía solicitud de invalidación al servicio de autenticación | |  | |
| 5. El sistema elimina token local del almacenamiento | |  | |
| 6. El sistema limpia datos sensibles de memoria | |  | |
| 7. El sistema redirige a pantalla de inicio de sesión del CdM y muestra mensaje de confirmación de sesión cerrada | |  | |
| 8. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-028** | **Restablecer contraseña** | | |
| Descripción | Proceso administrativo mediante el cual el Administrador del Centro de Monitoreo restablece la contraseña de un operador, generando nueva contraseña temporal. | | |
| Objetivo | Permitir recuperación de acceso a operadores que han olvidado contraseña o por motivos de seguridad, manteniendo control sobre el proceso. | | |
| Actor | Administrador CdM | Actores Sec. | n/a |
| Complejidad | Media | Prioridad | Media |
| Usa | No | Extiende | No |
| Pre-condiciones | El administrador inició sesión en plataforma web con credenciales de administrador y tiene permisos para restablecer contraseñas  El operador existe en sistema y tiene cuenta activa | | |
| Post-condiciones | Se genera nueva contraseña temporal para el operador  Se invalida contraseña anterior y la sesión del operador  Se notifica al operador sobre el restablecimiento  Se fuerza al operador a cambiar contraseña temporal en próximo inicio de sesión | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El administrador de CdM selecciona Restablecer Contraseña desde gestionar operadores o entra desde el link enviado a su correo pidiendo restablecer una contraseña | |  | |
| 2. El sistema muestra diálogo con nombre y legajo del operador, advertencia, opción notificar –si/no-, campo motivo y botón restablecer o cancelar | |  | |
| 3. El administrador ingresa motivo y confirma acción | | 3.A.1. El administrador no ingresa el motivo  3.A.2. El sistema muestra mensaje de error indicando que falta el motivo | |
| 4. El sistema genera una contraseña temporal segura | |  | |
| 5. El sistema guarda la contraseña como temporal, se la asigna al operador e invalida las sesiones que tenga abiertas | |  | |
| 6. El sistema manda un mail al operador con la contraseña temporal y un link para iniciar sesión en la plataforma | |  | |
| 7. El sistema muestra mensaje de confirmación de restablecimiento de contraseña exitoso | |  | |
| 8. Fin de UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

### Modulo Monitoreo

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-029** | **Gestionar Alarmas Entrantes** | | |
| Descripción | Interfaz principal del operador del CdM que presenta un tablero con las alarmas de emergencia asignadas a él, mostrando datos en tiempo real y permitiendo la gestión inicial de cada caso. | | |
| Objetivo | Permitir al operador del CdM supervisar de manera inmediata y todas las emergencias activas bajo su responsabilidad, facilitando una respuesta rápida y organizada. | | |
| Actor | Operador CdM,  Administrador CdM | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Alta |
| Usa | UC-030 | Extiende | No |
| Pre-condiciones | El operador ha iniciado sesión en la plataforma web del CdM  El sistema tiene alarmas activas asignadas al operador o en cola general.  El servicio de notificaciones está operativo. | | |
| Post-condiciones | Las alarmas asignadas al operador se muestran en el tablero  El operador puede seleccionar una alarma para iniciar su verificación  El mapa interactivo muestra la ubicación en tiempo real de las alarmas activas | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El operador o el administrador de CdM accede al tablero principal de la plataforma web del CdM tras iniciar sesión. | |  | |
| 2. El sistema recupera la lista de alarmas activas asignadas al operador, así como las alarmas no asignadas (si el operador es administrador o tiene permisos). | | 2.A.1. El sistema verifica que el operador tiene permisos de administrador  2.A.2. El sistema muestra todas las alarmas activas, las que no tiene operador asignado y las finalizadas en el último turno | |
| 3. El sistema muestra el tablero de monitoreo compuesto de   * Panel Central mapa interactivo con marcadores en las ubicaciones de cada alarma * Panel Inferior listado de las alarmas, con nombre de usuario, hora de activación, tipo de ubicación obtenido, estado e indicadores de nuevas evidencias recibidas. | |  | |
| 4. El sistema actualiza automáticamente el tablero de alarmas cada 15 seg o puede hacerse manualmente mediante un botón de refrescar | |  | |
| 5. El sistema detecta nueva entrada de alarma y muestra la nueva alarma asignada al operador | | 5.A.1. El sistema detecta que el operador tiene permisos de administrador y entra una nueva alarma  5.A.2. El sistema procede a asignar la alarma a un operador disponible y llama al UC-032 asignar operador  5.A.3. El sistema muestra mensaje de información de nueva entrada para el administrador | |
| 6. El operador selecciona ver detalle de la nueva alarma | | 6.A.1. El operador tarda más de 20 seg en revisar el detalle de la alarma entrante  6.A.2. El sistema refuerza la notificación al usuario y vuelve a esperar otros 20 seg  6.A.3. El operador sigue sin tomar la alarma  6.A.4. El sistema actualiza la alarma como no tomada  6.A.5. El sistema llama al UC-032 para asignar a otro operador, envía notificación al administrador de turno por mail y continua en el paso 9. | |
| 7. El sistema actualiza la nueva alarma al estado “en verificación” por el operador, con timestamp | |  | |
| 8. El sistema procede a mostrar el detalle de la alarma y ejecuta el UC-030 ver detalle de alarma | |  | |
| 9. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-030** | **Verificar Alarma** | | |
| Descripción | Proceso mediante el cual el operador del CdM evalúa una alarma entrante específica, analizando las evidencias para confirmar la situación de emergencia, descartar falsas alarmas y asignar un nivel de prioridad que guíe la respuesta. | | |
| Objetivo | Filtrar activaciones accidentales y determinar la gravedad de la emergencia para priorizar recursos y decidir el curso de acción apropiado, especialmente la notificación a autoridades (UC-031). | | |
| Actor | Operador CdM | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Alta |
| Usa | UC-013, UC-031 | Extiende | No |
| Pre-condiciones | El operador tiene acceso al tablero de alarmas  El operador ha seleccionado una alarma en estado "Nueva" o "En Verificación".  El sistema tiene disponibles algunas evidencias iniciales | | |
| Post-condiciones | La alarma cambia su estado a Verificada o Descartada.  Se registra en el historial de la alarma la acción del operador, la prioridad asignada y el timestamp.  Se habilita el flujo para notificar autoridades | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El operador selecciona una alarma desde el tablero del CdM. | |  | |
| 2. El sistema procede a obtener las autoridades más cercanas al hecho y ejecuta el UC-013 | |  | |
| 3. El sistema abre una vista detallada de la alarma, mostrando:   * Datos del Usuario: Nombre, dirección registrada, contacto. * Ubicación: Mapa con trazado histórico, última posición. Tipo de fuente (GPS/Red). * Evidencias: Reproductor de audio grabado. Galería de fotos capturadas (frontal/trasera). Nivel de batería del dispositivo * Autoridades: Listado de autoridades cercanas al hecho * Controles: Selector para asignar Prioridad –Alta, Media, Baja- y botones Notificar Autoridades, Descartar Alarma | | 3.A.1. El sistema detecta que se abre en modo consulta y muestra todos los campos y botones deshabilitados  3.A.2. El sistema muestra un nuevo botón cerrar habilitado  3.A.3. El operador presiona cerrar  3.A.4. El sistema continua en el paso 8 | |
| 4. El operador revisa la información y las evidencias, selecciona la prioridad, la autoridades competentes para el hecho y presiona en Notificar Autoridades. | | 4.A.1. El operador selecciona Descartar Alarma  4.A.2. El sistema muestra un dialogo de confirmación con un campo para definir el motivo  4.A.3.A.1. El operador selecciona confirmar  4.A.3.A.2. El sistema registra el motivo de la baja con el timestamp, y retira la alarma de la lista de alarmas prioritarias  4.A.3.A.3. El sistema envía señal para finalizar alarma en el dispositivo del usuario  4.A.3.A.1. El operador selecciona cancelar  4.A.3.A.2. El sistema cancela el proceso y retorna al paso 3 | |
| 5. El sistema actualiza el estado de la alarma, la prioridad y registra la acción con timestamp | |  | |
| 6. El sistema procede a notificar a las autoridades y ejecuta el UC-031 | |  | |
| 7. El sistema muestra un mensaje de confirmación Alarma verificada y priorizada | |  | |
| 8. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-031** | **Notificar Autoridades** | | |
| Descripción | Proceso manual ejecutado por el operador del CdM para informar y coordinar con las autoridades policiales o de emergencia locales más cercanas a la ubicación del incidente, una vez verificada la alarma como de alta prioridad. | | |
| Objetivo | Establecer el vínculo formal con los organismos de seguridad competentes para movilizar una respuesta física y profesional en el lugar de los hechos, completando el ciclo de protección. | | |
| Actor | Operador CdM | Actores Sec. | Autoridades |
| Complejidad | Media | Prioridad | Media |
| Usa | No | Extiende | No |
| Pre-condiciones | El operador ha verificado una alarma y le ha asignado prioridad Alta.  El sistema ha obtenido una ubicación válida del dispositivo  Existe un protocolo y datos de las autoridades correspondientes a la zona. | | |
| Post-condiciones | Se establece comunicación con la autoridad designada.  Se transmite a la autoridad la información crítica del incidente (ubicación, datos usuario, naturaleza).  Se registra en el sistema la acción, la hora, la autoridad contactada y el nombre/identificación del receptor.  El estado de la alarma cambia a "Autoridades Notificadas". | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El operador selecciona Notificar Autoridades desde la verificación de la alarma | |  | |
| 2. El sistema muestra un diálogo con   * Información generada para transmitir dirección aproximada, coordenadas, nombre y teléfono del usuario, hora de activación, tipo de activación. * El numero de contacto de las autoridades seleccionadas * Botones Llamar y Enviar SMS | |  | |
| 3. El operador revisa la información, añade observaciones si es necesario y selecciona el botón de llamar como medio de contacto | | 3.A.1. El operador selecciona enviar SMS  3.A.2. El sistema genera un mensaje adecuado para SMS con datos resumidos  3.A.3. El sistema procede a enviar el mensaje y llama al UC-012 | |
| 4. El operador realiza la comunicación verbal o confirma el envío del mensaje. | |  | |
| 5. El sistema muestra un campo para que se ingrese un breve resumen de la respuesta de las autoridades | |  | |
| 6. El sistema registra toda la acción, cambia el estado de la alarma a notificada y muestra confirmación. | |  | |
| 7. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-032** | **Asignar Operador** | | |
| Descripción | Proceso administrativo, típicamente realizado por un Supervisor o Administrador del CdM, mediante el cual se distribuyen manual o semiautomáticamente las alarmas entrantes que no tienen un operador asignado entre los operadores disponibles y activos en el sistema. | | |
| Objetivo | Garantizar una distribución balanceada de la carga de trabajo entre los operadores del centro, asegurando que cada alarma sea atendida de manera oportuna por un recurso humano disponible. | | |
| Actor | Administrador CdM | Actores Sec. | n/a |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | UC-029 |
| Pre-condiciones | El administrador ha iniciado sesión en la plataforma web con permisos de administración.  Existe al menos una alarma en estado nuevo sin operador asignado.  Existe al menos un operador del CdM con sesión activa y estado disponible. | | |
| Post-condiciones | La alarma seleccionada queda asignada a un operador específico.  El estado de la alarma cambia a asignada.  El operador asignado recibe una notificación en su tablero sobre la nueva alarma. | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El administrador selecciona una alarma con estado sin asignar desde la lista de Gestionar Alarmas, que está en estado nueva o no tomada | | 1.A.1. El sistema llama automáticamente cuando una nueva alarma se detecta para asignar un operador que esté disponible | |
| 2. El sistema verifica que la alarma este en estado nuevo y genera un ID único de alarma | |  | |
| 3. El sistema muestra un dialogo con los datos básicos de la alarma y la lista de operadores disponibles | | 3.A.1. El sistema detecta que no hay operadores disponibles  3.A.2. El sistema muestra en pantalla todos los operadores que están activos y la cantidad de alarmas en cola que tiene cada uno, ordenados de manera ascendente y continua en el paso 4 | |
| 4. El administrador selecciona un operador para asignar la alarma | |  | |
| 5. El sistema asocia la alarma con el operador, actualiza el estado de la alarma a asignada y el ID. | |  | |
| 6. El sistema muestra un mensaje de confirmación con el id asignado y el nombre del operador | |  | |
| 7. Fin de UC. | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-033** | **Consultar Historial de Alarmas** | | |
| Descripción | Funcionalidad que permite al operador del CdM buscar, filtrar y revisar el registro histórico completo de todas las alarmas gestionadas por el centro, incluyendo las finalizadas, falsas alarmas y aquellas en curso. | | |
| Objetivo | Facilitar el análisis post-incidente, la generación de reportes estadísticos y la auditoría del funcionamiento del sistema y de las acciones tomadas por los operadores. | | |
| Actor | Operador CdM,  Administrador CdM | Actores Sec. | n/a |
| Complejidad | Baja | Prioridad | Baja |
| Usa | UC-030 | Extiende | No |
| Pre-condiciones | El operador ha iniciado sesión en la plataforma web del CdM.  Existen alarmas registradas en el sistema | | |
| Post-condiciones | El sistema presenta una lista paginada/filtrada de alarmas según los criterios de búsqueda.  El operador puede visualizar el detalle completo de cualquier alarma del historial. | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El operador navega a la sección de Historial desde el menú principal | |  | |
| 2. El sistema muestra en pantalla un listado de alarmas son las siguientes características:  ordenado por fecha descedente y filtrado por operador y que permite aplicar múltiples criterios de filtrado (por fechas, por estado, por nombre, etc) y de ordenación (mismo que lso criterios) | | 2.A.1. El sistema detecta que el usuario tiene permisos de administrador  2.A.1. El sistema agrega la posibilidad de filtrar por operador | |
| 3. El operador define los filtros que desea y hace clic en Buscar. | |  | |
| 4. El sistema consulta sus datos aplicando los filtros y ordenación definidos y refresca el listado de alarmas. | |  | |
| 5. El operador puede seleccionar cualquier alarma de la lista para mostrar una vista con más detalle | | 5.A.1. El operador puede seleccionar descargar listado  5.A.2. El sistema ofrecerá las opciones de descarga posibles, pdf o xls  5.A.3. El operador selecciona alguna de las opciones  5.A.4. El sistema genera un archivo del tipo seleccionado para ser descargado automáticamente | |
| 6. El sistema procede a mostrar en pantalla el detalle de la alarma y llama al UC-030 en modo consulta | |  | |
| 7. Fin de UC. | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

### Modulo Evidencias

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-034** | **Obtener Ubicación** | | |
| Descripción | Permite localizar el dispositivo del usuario a través de GPS, o de red celular | | |
| Objetivo | Obtener la ubicación en tiempo real del dispositivo del usuario que inicio el estado de alarma | | |
| Actor | n/a | Actores Sec. | Servicio de GPS, Servicio de Red Celular |
| Complejidad | Alta | Prioridad | Alta |
| Usa | UC-037,UC-038 | Extiende | No |
| Pre-condiciones | El dispositivo tiene los permisos de ubicación (GPS y red) concedidos por el usuario (UC-019).  La alarma está activa (UC-001 en ejecución).  El dispositivo tiene capacidad de hardware para obtener una ubicación (GPS o radio celular). | | |
| Post-condiciones | Se obtienen coordenadas geográficas (latitud, longitud).  Se registra el método de obtención (GPS/Red) y la precisión estimada.  Las coordenadas se envían al flujo de notificaciones y/o se almacenan localmente. | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema esta en estado de alarma y procede a buscar la ubicación actual | |  | |
| 2. El sistema procede a obtener la ubicación mediante el GPS del dispositivo, con un timeout de 10 seg | |  | |
| 3. El sistema procede a obtener el nivel de batería para definir el umbral y llama al UC-038 | |  | |
| 4. El sistema llama al servicio GPS devuelve una ubicación con precisión aceptable, toma esas coordenadas, y se marca como obtenido por GPS | | 4.A.1. El sistema detecta que el servicio de GPS falla  4.A.2. El sistema procede a obtener la ubicación mediante triangulación con red celular, con un timeout de 10 seg  4.A.3.A.1. El servicio de Red Celular devuelve una ubicación y continua en el paso 4  4.A.3.B.1. El servicio de Red Celular falla  4.A.3.B.2. El sistema busca la última ubicación almacenada y continua en el paso 6  4.B.1. El sistema consulta el estado de la batería al UC-038 y está en el nivel crítico  4.B.2. El sistema procede a obtener la ubicación mediante triangulación con red celular, con un timeout de 10 seg  4.B.3.A.1. El servicio de Red Celular devuelve una ubicación con método Red y continua en el paso 4  4.B.3.B.1. El servicio de Red Celular falla  4.B.3.B.2. El sistema busca la última ubicación almacenada con método almacenada y continua en el paso 6 | |
| 5. El sistema procede a guardar la ubicación obtenida, junto con timestamp y método de obtención y llama al UC-037 | |  | |
| 6. El sistema retorna la ubicación obtenida con metadatos | |  | |
| 7. Fin del UC | |  | |
| Comentarios | Los fallos contemplado en los servicios son baja calidad de ubicación, que no responda con la ubicación y salga por timeout, o que no esté el permiso concedido por el usuario | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-035** | **Grabar Audio** | | |
| Descripción | Proceso automatizado que inicia una grabación de audio ambiental en segundo plano con una calidad optimizada, dividida en segmentos manejables, durante el estado de alarma activa. | | |
| Objetivo | Capturar evidencia auditiva crítica del incidente (voces, sonidos ambientales) que pueda ser utilizada por el CdM para verificar la emergencia y su nivel de gravedad. | | |
| Actor | n/a | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Media |
| Usa | UC-037, UC-038 | Extiende | No |
| Pre-condiciones | La alarma está activa (UC-001 en ejecución).  El dispositivo tiene permiso para usar el micrófono  El nivel de batería está por encima del umbral configurado para operaciones no críticas | | |
| Post-condiciones | Se inicia un servicio de grabación de audio en segundo plano.  Se generan archivos de audio segmentados  Cada segmento se almacena localmente y se pone en cola para transmisión al CdM | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema después de confirmar la activación de la alarma, inicia el servicio de grabación de audio | |  | |
| 2. El sistema procede a obtener el nivel de batería para definir el umbral y llama al UC-038 | |  | |
| 3. El sistema adopta el formato de audio configurado para la mejor calidad y tamaño. | | 3.A.1. El sistema detecta que el nivel de batería está en el nivel bajo  3.A.2. El sistema baja la calidad del audio a la mitad y comprime el formato  3.B.1. El sistema detecta que el nivel de batería está en el nivel critico  3.B.2. El sistema deja de capturar el sonido ambiente, hasta que vuelva a cargarse el dispositivo, registra en base la limitación por batería y continua en el paso 8 | |
| 4. El sistema divide el flujo de audio en archivos separados de una cierta duración (preconfigurable, 15 segundos por defecto) | |  | |
| 5. El sistema asocia a cada segmento de audio, el ID de la alarma y el timestamp de inicio y fin del segmento de la grabación | |  | |
| 6. El sistema procede a guardar el segmento de audio y llama al UC-037 | |  | |
| 7. El sistema repite el ciclo cada hasta finalizar el estado de alarma o nivel de batería critico | |  | |
| 8. Fin de UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-036** | **Capturar Fotos** | | |
| Descripción | Proceso automatizado que toma fotografías periódicas utilizando las cámaras frontal y trasera del dispositivo de manera alternada, solo cuando se detecta un nivel mínimo de luz ambiental. | | |
| Objetivo | Obtener evidencia visual del entorno y de posibles agresores durante la emergencia, proporcionando al CdM información contextual valiosa para evaluar la situación. | | |
| Actor | n/a | Actores Sec. | n/a |
| Complejidad | Alta | Prioridad | Media |
| Usa | UC-038 | Extiende | No |
| Pre-condiciones | La alarma está activa (UC-001 en ejecución).  El dispositivo tiene permiso para usar algunas de las cámaras del dispositivo  Existe un nivel de luz ambiental por encima de un umbral configurable  El nivel de batería está por encima del umbral configurado para operaciones intensivas | | |
| Post-condiciones | Se capturan imágenes desde las cámaras frontal y/o trasera.  Las imágenes se comprimen y se almacenan localmente  Las imágenes se ponen en cola para transmisión al CdM | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema después de confirmar la activación de la alarma, inicia el servicio de captura de fotos | |  | |
| 2. El sistema procede a obtener el nivel de batería para definir el umbral y llama al UC-038 | |  | |
| 3. El sistema determina el nivel de luminosidad ambiente con el sensor de luz ambiental | |  | |
| 4. El sistema verifica que la luz ambiental de las cámaras trasera y frontal están por encima del umbral mínimo, y el nivel de batería es óptimo y captura una foto de cada cámara con el mayor enfoque posible y la mejor calidad configurada | | 4.A.1. El sistema detecta que la luz ambiental de alguna cámara está por debajo del umbral mínimo  4.A.2. El sistema no captura la foto y continua en el paso 7  4.B.1. El sistema detecta que no han sido otorgados permisos la cámara frontal y/o trasera  4.B.2.A.1. El sistema detecta que una cámara no está habilitada, se desiste de capturar la foto y continua en el paso 7  4.B.2.B.2. El sistema detecta que ambas cámaras no están habilitadas, se desiste de capturar la foto y continua en el paso 8  4.C.1. El sistema detecta que la batería está en el umbral bajo  4.C.2. El sistema disminuye la calidad de la captura y continua en el paso 5  4.D.1. El sistema detecta que la batería está en el umbral crítico, se desiste de capturar fotos y continua en el paso 8 | |
| 5. El sistema asigna un timestamp para las fotos, cifra los datos y los comprime | |  | |
| 6. El sistema procede a guardar las capturas de las fotos y llama al UC-037 | |  | |
| 7. El sistema repite el ciclo desde el paso 2 cada cierto tiempo (preconfigurado, 5 segundos por defecto) hasta finalizar el estado de alarma o nivel de batería en estado bajo | |  | |
| 8. Fin de UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

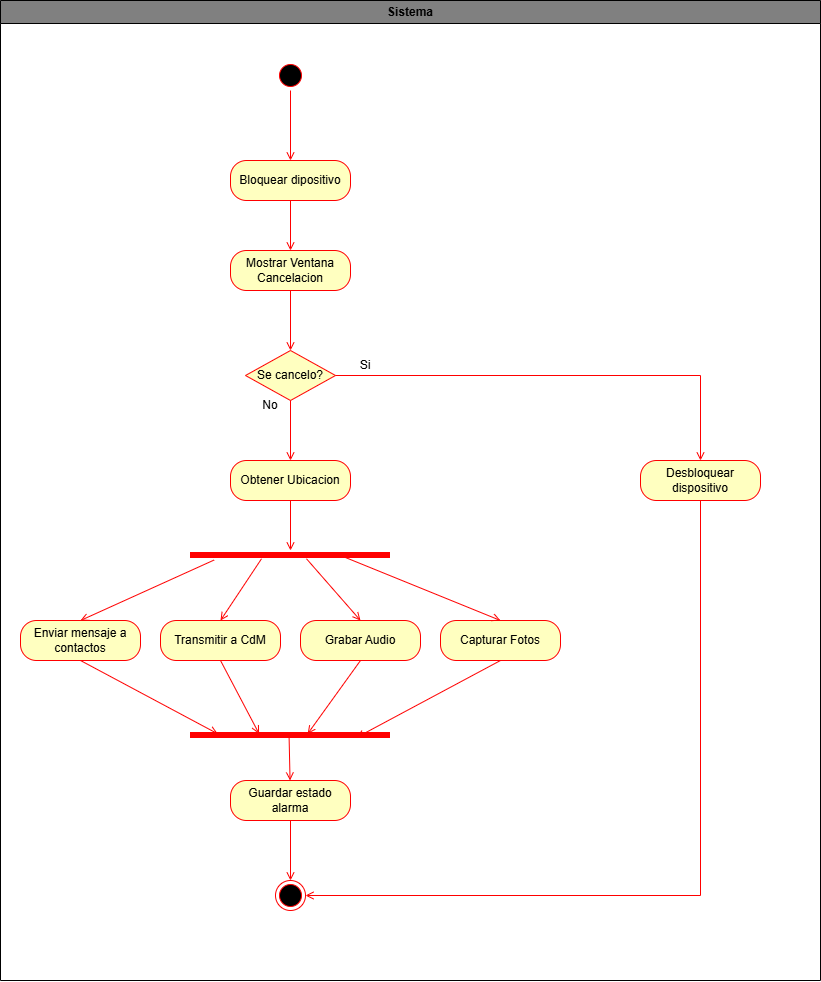
|  |  |  |  |
| --- | --- | --- | --- |
| **UC-037** | **Almacenar Datos Localmente** | | |
| Descripción | Proceso de contingencia que guarda en una base de datos local segura o en el almacenamiento interno del dispositivo todos los datos generados durante una alarma (estado, ubicaciones, archivos de audio, fotos) cuando no hay conectividad a Internet o cuando se necesita persistencia inmediata. | | |
| Objetivo | Garantizar que ninguna evidencia o información crítica se pierda debido a fallos en la red, permitiendo su envío posterior y asegurando la persistencia del estado de alarma tras reinicios | | |
| Actor | Operador CdM,  Administrador CdM | Actores Sec. | n/a |
| Complejidad | Media | Prioridad | Alta |
| Usa | No | Extiende | No |
| Pre-condiciones | La alarma está activa o acaba de activarse.  El dispositivo tiene espacio de almacenamiento interno disponible. | | |
| Post-condiciones | Los datos estructurados (ubicaciones, timestamps, eventos) se guardan en una base de datos local.  Los archivos binarios (audio, fotos) se guardan en un directorio privado de la aplicación.  Se mantiene un registro del estado persistente de la alarma.  Se crea una cola de trabajos pendientes para los datos que deben transmitirse cuando se recupere la conectividad. | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema llama al UC cuando un dato debe ser persistido | |  | |
| 2. El sistema determina el tipo de dato que se trata:   * Datos estructurados: Se inserta un registro en la tabla correspondiente de la base local * Archivos multimedia: Se guarda el archivo en un directorio con un nombre único basado en id de alarma, timestamp y tipo. * Estado de alarma: Se actualiza una bandera de activación de alarma y se guarda el timestamp de inicio en | | 2.A.1. El sistema detecta que el dispositivo no tiene capacidad de almacenamiento suficiente  2.A.2. El sistema elimina los archivos más antiguos que hayan sido enviados al CdM  2.A.3.A.1. El sistema tiene espacio suficiente y continua con el guardado de los datos  2.A.3.B.1. El sistema no tiene espacio suficiente verifica políticas de configuración, si está habilitado la sobreescritura de datos antiguos  2.A.3.B.2.A.1. El sistema tiene activada la política de sobreescritura sobre datos más antiguos y permite sobreescribirlos  2.A.3.B.2.B.1. El sistema no tiene activada la política de sobreescritura sobre datos más antiguos  2.A.3.B.2.B.2. El sistema muestra mensaje de error de almacenaje lleno y continua al paso 5 | |
| 3. El sistema crea un registro para cada dato que debe ser transmitido al CdM, el sistema crea o actualiza una entrada en una tabla de datos pendientes, que contiene la ruta al archivo, el tipo, y los intentos fallidos. | |  | |
| 4. El sistema confirma la escritura local | |  | |
| 5. Fin del UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| **UC-038** | **Consultar Nivel de Bateria** | | |
| Descripción | Servicio de consulta que evalúa el nivel actual de batería del dispositivo y lo clasifica en un estado según umbrales configurados. Este estado es devuelto a los procesos que lo invocan para que tomen decisiones autónomas sobre sus operaciones. | | |
| Objetivo | Centralizar y normalizar la lógica de evaluación del estado de energía del dispositivo, proporcionando una interfaz simple y consistente para que otros casos de uso puedan adaptar su comportamiento de manera eficiente y predecible. | | |
| Actor | n/a | Actores Sec. | n/a |
| Complejidad | Baja | Prioridad | Media |
| Usa | No | Extiende | No |
| Pre-condiciones | La aplicación posee permisos para consultar el nivel de batería.  Los umbrales de clasificación están configurados. | | |
| Post-condiciones | Se obtiene el porcentaje actual de batería.  Se devuelve el estado y nivel de carga correspondiente. | | |
| **Flujo Principal** | | **Flujo Alternativo** | |
| 1. El sistema necesita obtener el nivel de batería y el umbral en el que se encuentra | |  | |
| 2. El sistema consulta al SO del dispositivo el nivel de batería actual (en porcentaje) y si está conectado a un cargador. | |  | |
| 3. El sistema recupera los umbrales configurados desde las preferencias de la aplicación. | |  | |
| 4. El sistema clasifica el estado según los siguientes criterios:   * Normal: el dispositivo está conectado a un cargador, o el nivel de carga es mayor o igual al umbral normal * Regular: el porcentaje de batería es menor que el umbral normal * Bajo: el porcentaje de batería es menor que el umbral regular. * Critico: el porcentaje de batería es menor que el umbral bajo | |  | |
| 5. El sistema devuelve el porcentaje de batería restante y el umbral donde se encuentra | |  | |
| 6. Fin de UC | |  | |
| Comentarios | - | | |
| Autor | Fernando Martin | Versión | 1.0 |

# Análisis

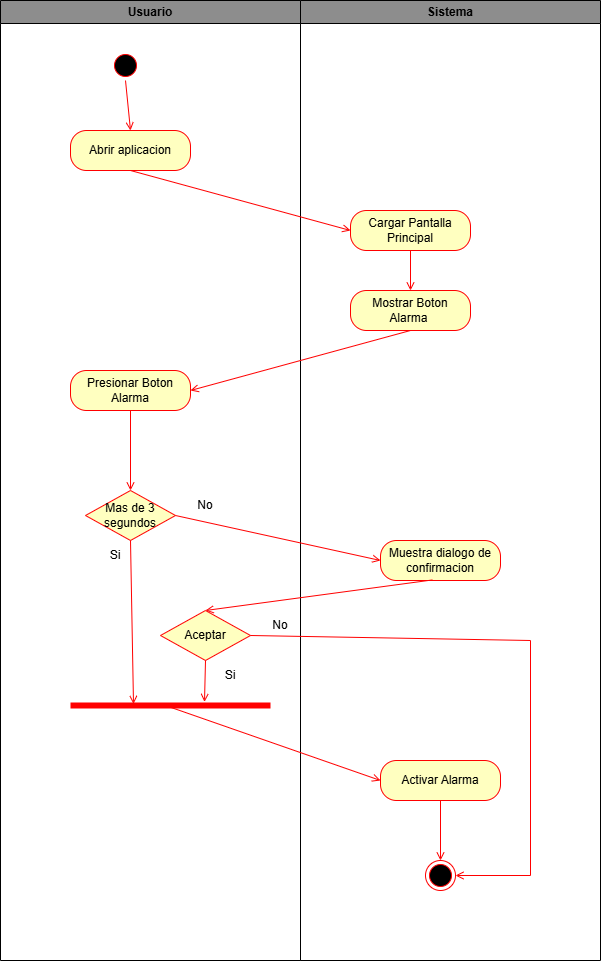
## Diagramas de Actividades

### UC-001: Activar Alarma



*Imagen 7-1 Diagrama de Actividad UC-001:Activar Alarma*

### UC-002: Activar Manualmente



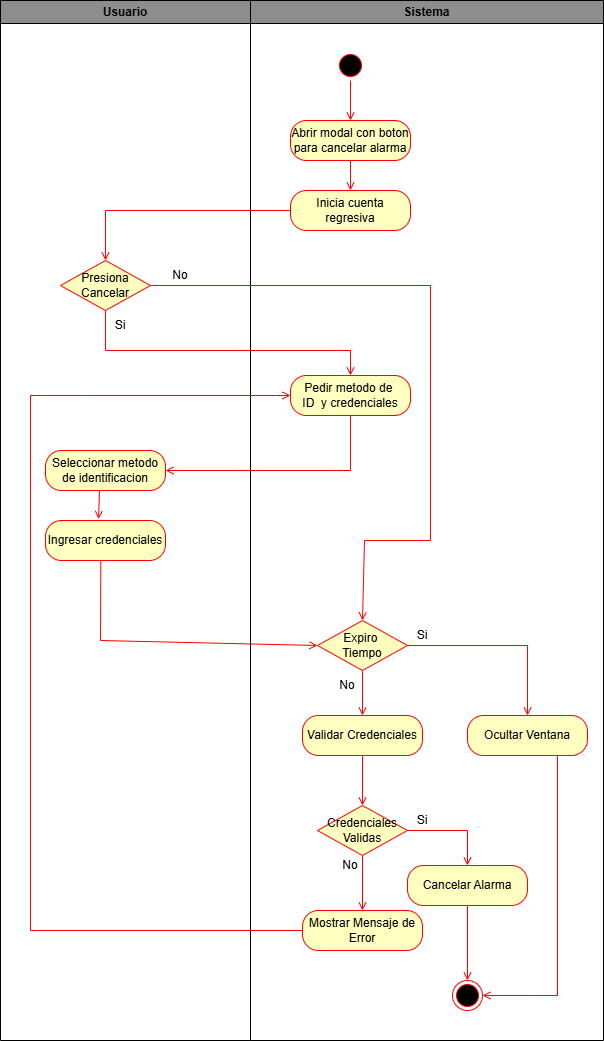
*Imagen 7-2 Diagrama de Actividad UC-002:Activar Manualmente*

### UC-006: Bloquear Dispositivo



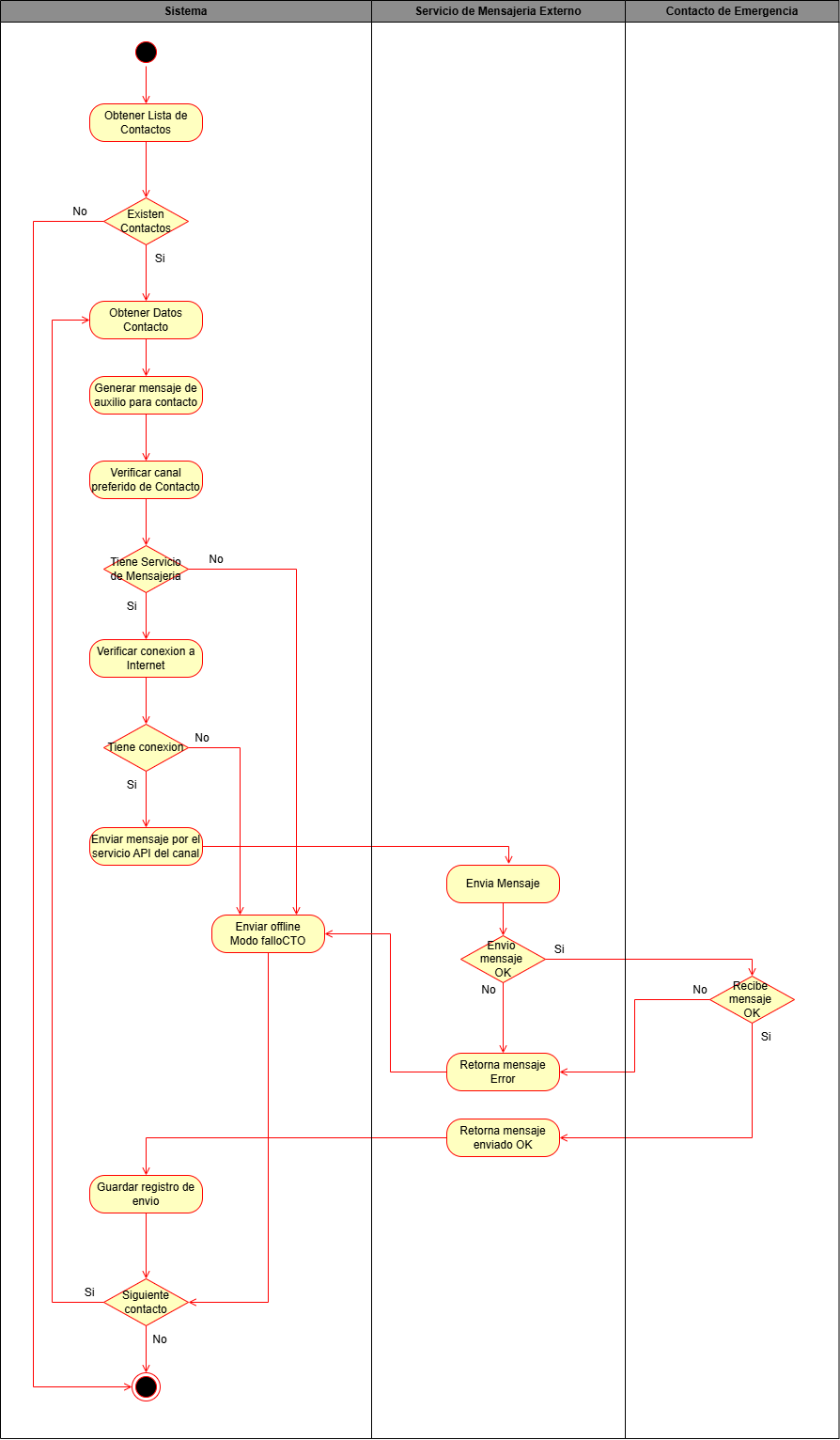
*Imagen 7-3 Diagrama de Actividad UC-006:Bloquear Dispositivo*

### UC-007: Mostrar Ventana de Cancelación



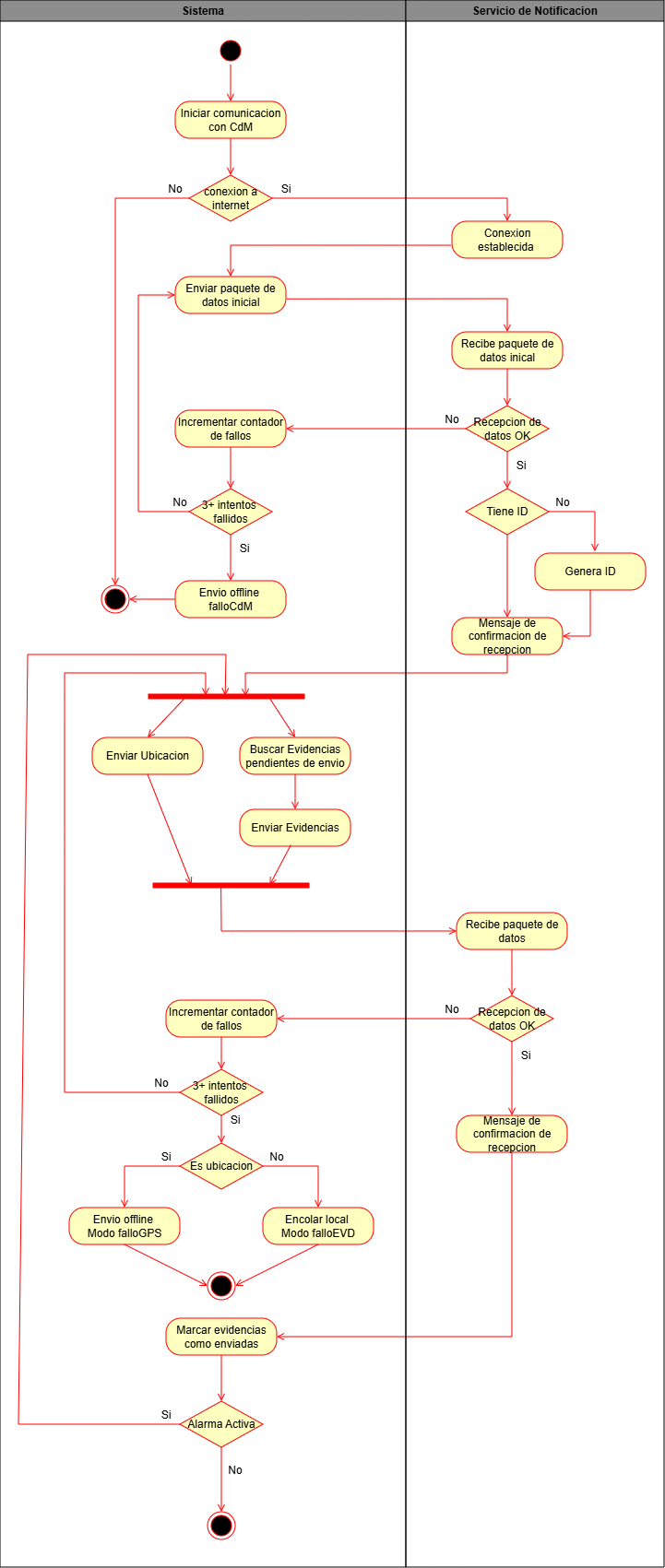
*Imagen 7-4 Diagrama de Actividad UC-007:Mostrar Ventana de Cancelación*

### UC-009: Enviar Alarma a Contactos



*Imagen 7-5 Diagrama de Actividad UC-009:Enviar Alarma a Contactos*

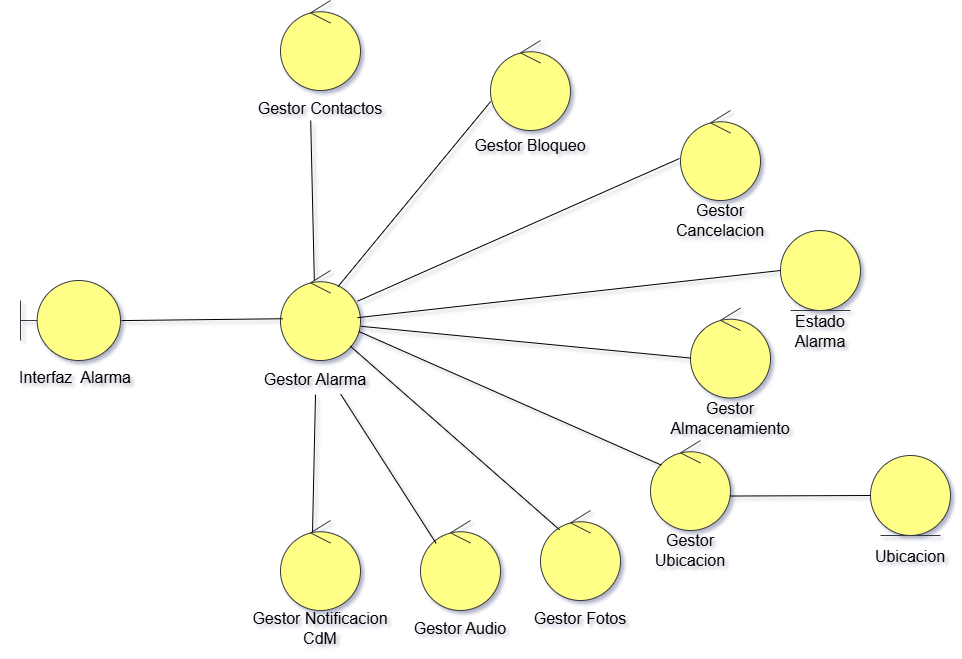
### UC-010: Transmitir a Centro de Monitoreo



*Imagen 7-6 Diagrama de Actividad UC-010: Transmitir a Centro de Monitoreo*

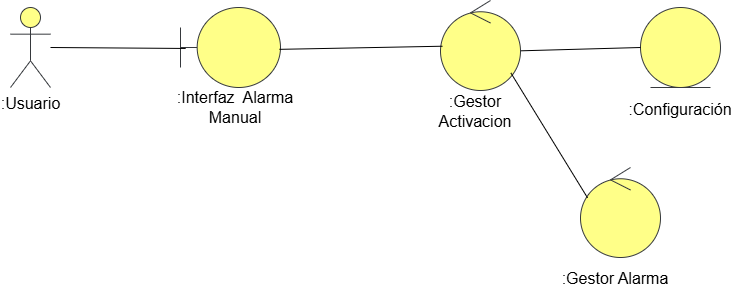
## Diagramas de Clases de Análisis

### UC-001: Activar Alarma



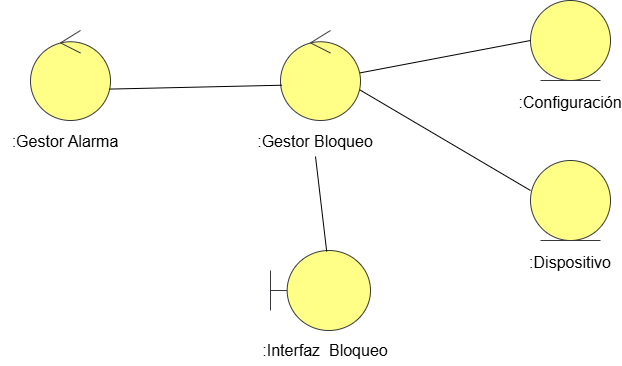
*Imagen 7-7 Diagrama de Clases de Analisis UC-001*

### UC-002: Activar Manualmente



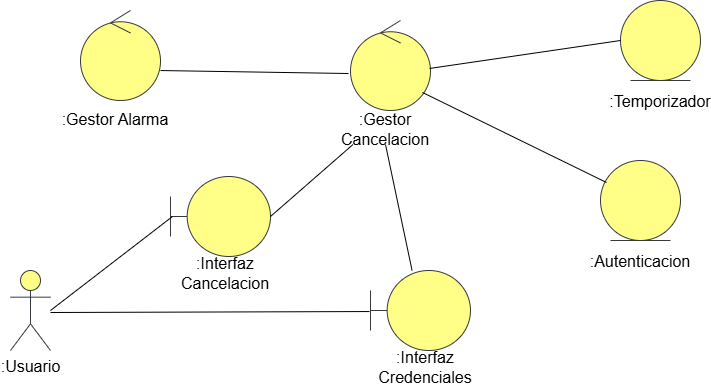
*Imagen 7-8 Diagrama de Clases de Analisis UC-002*

### UC-006: Bloquear Dispositivo



*Imagen 7-9 Diagrama de Clases de Analisis UC-003*

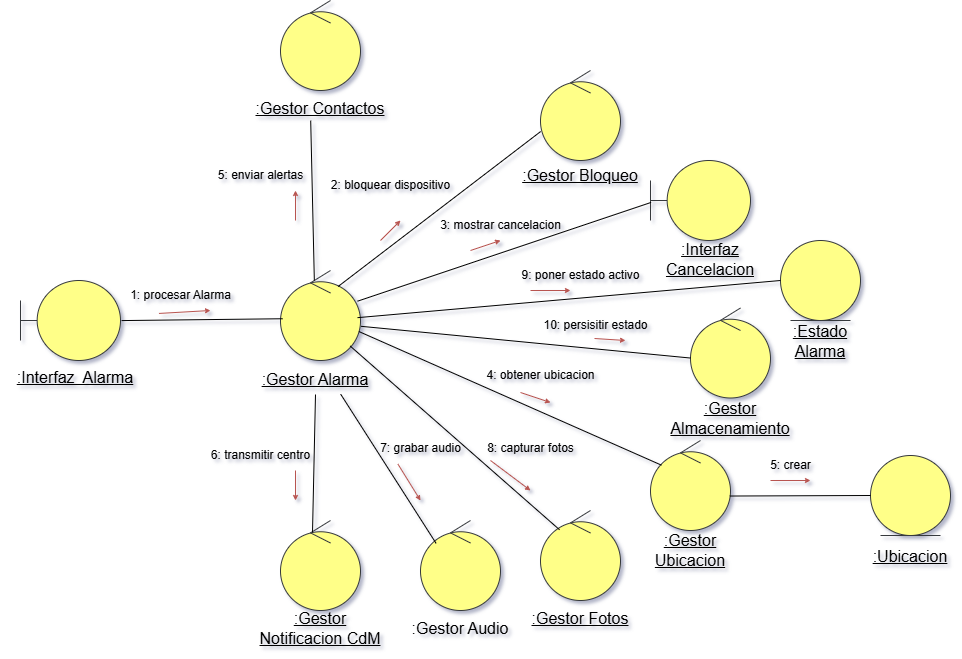
### UC-007: Mostrar Ventana de Cancelación



*Imagen 7-10 Diagrama de Clases de Analisis UC-007*

## Diagramas de Colaboración

### UC-001: Activar Alarma



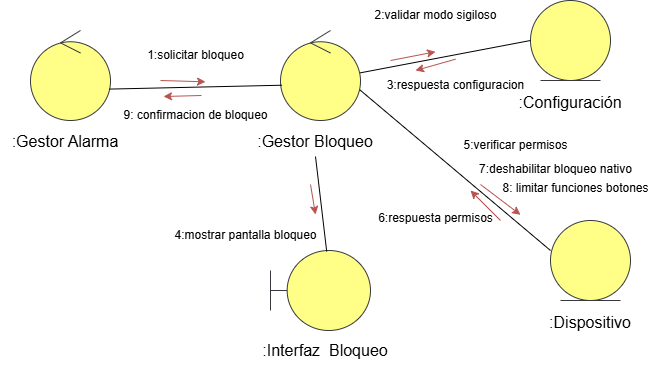
*Imagen 7-11 Diagrama de Colaboración UC-001*

### UC-002: Activar Manualmente



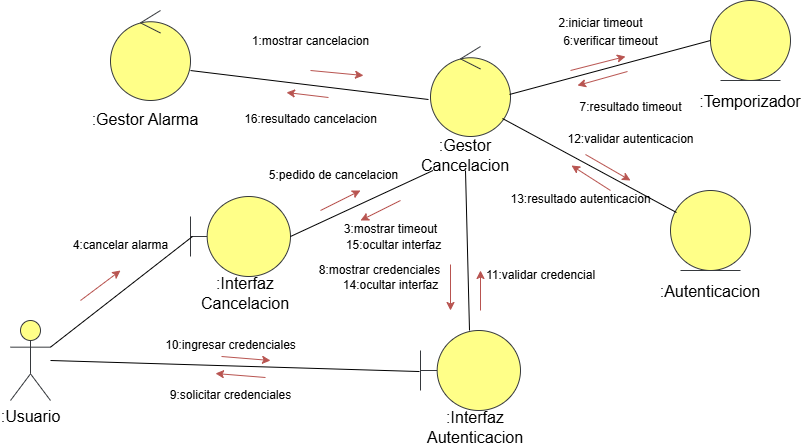
*Imagen 7-12 Diagrama de Colaboración UC-002*

### UC-006: Bloquear Dispositivo



*Imagen 7-13 Diagrama de Colaboración UC-006*

### UC-007: Mostrar Ventana de Cancelación



*Imagen 7-14 Diagrama de Colaboración UC-007*

# Diseño

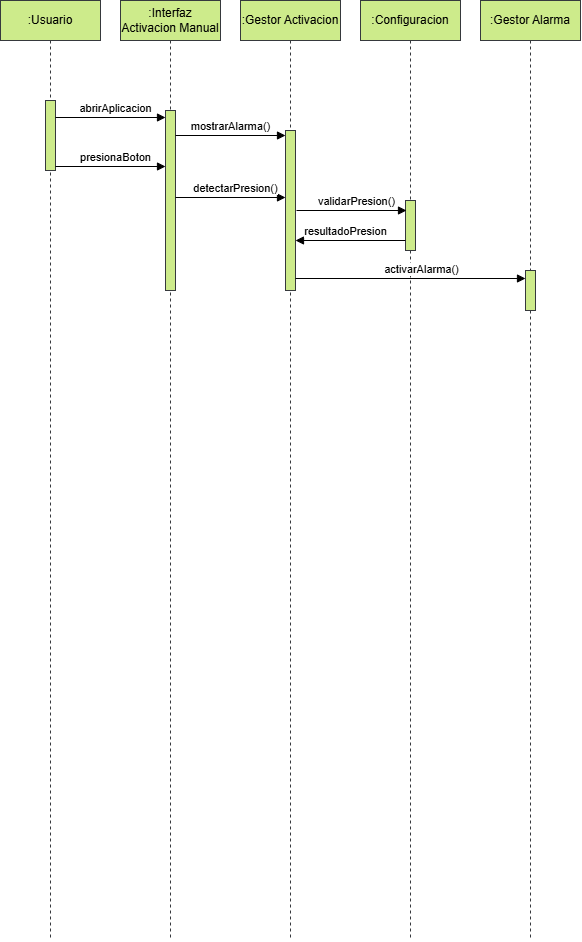
## Diagramas de Secuencia

### UC-001: Activar Alarma



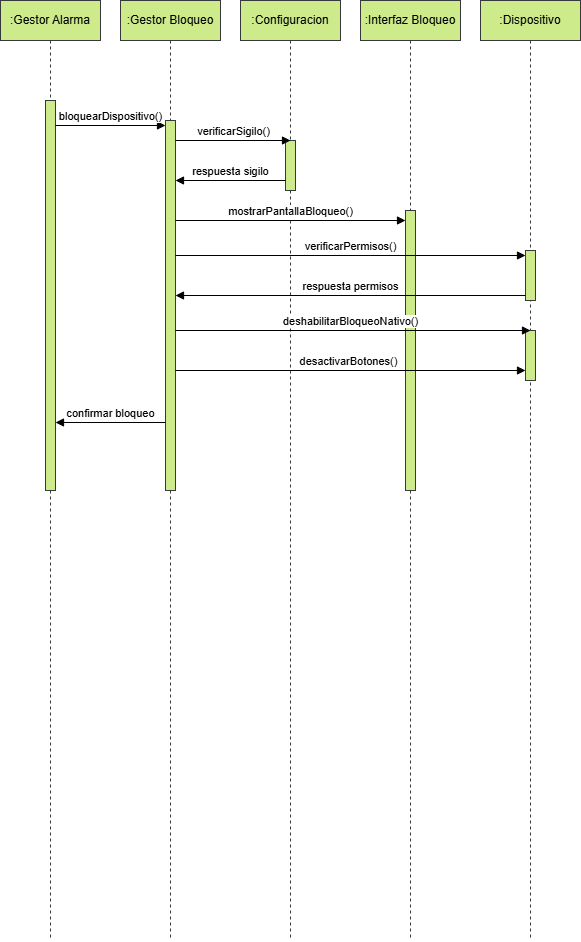
*Imagen 8-1 Diagrama de secuencia UC-001*

### UC-002: Activar Manualmente



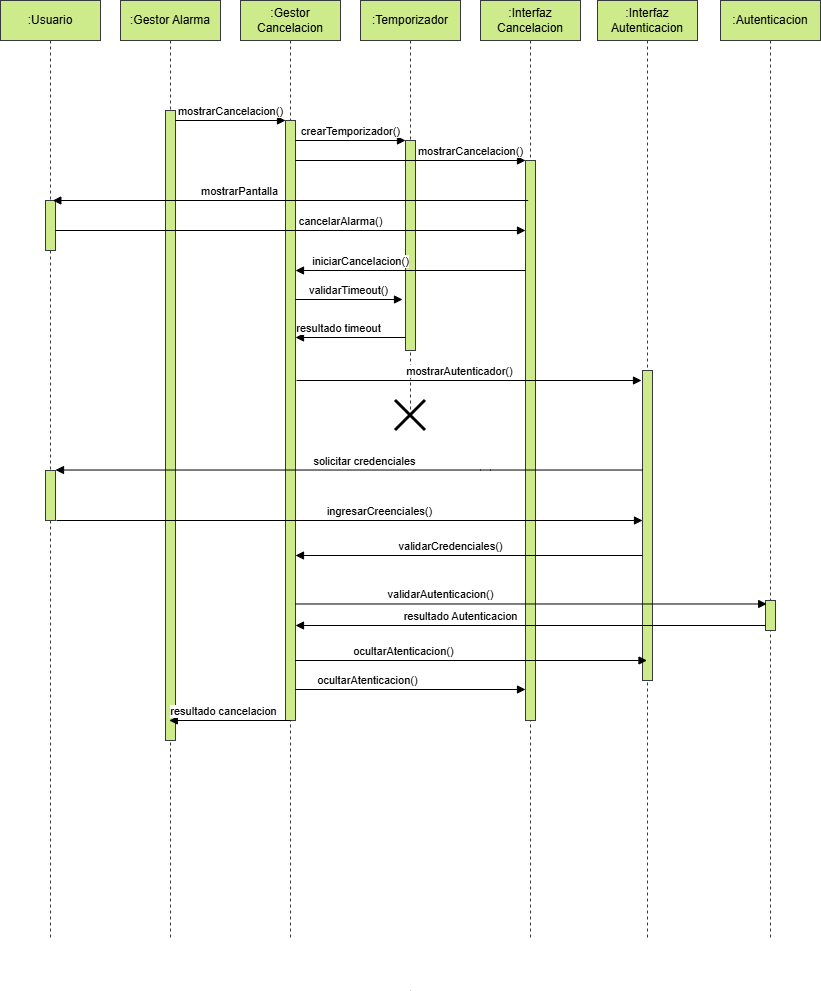
*Imagen 8-2 Diagrama de secuencia UC-002*

### UC-006: Bloquear Dispositivo



*Imagen 8-3 Diagrama de secuencia UC-006*

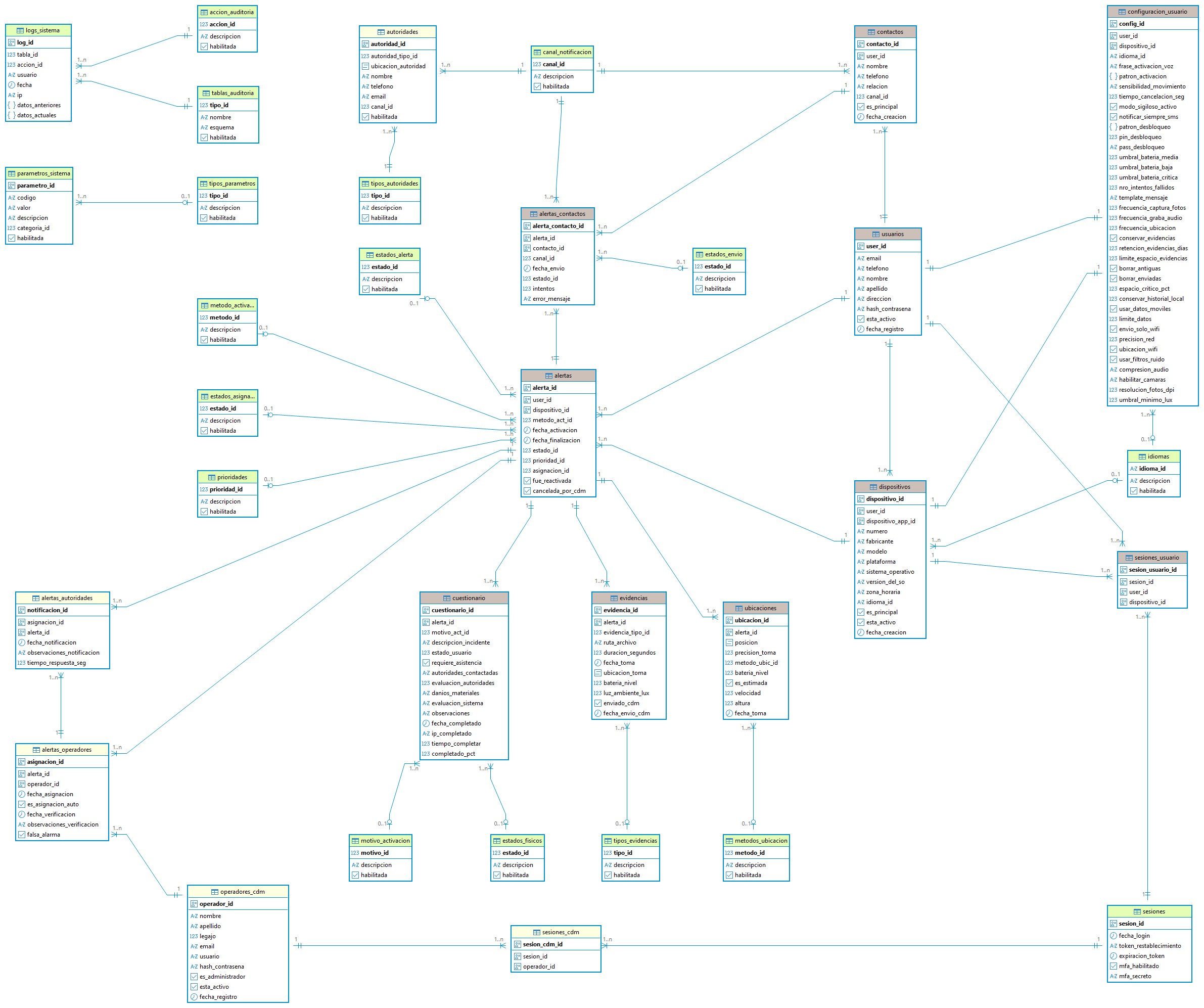
### UC-007: Mostrar Ventana de Cancelación



*Imagen 8-4 Diagrama de secuencia UC-007*

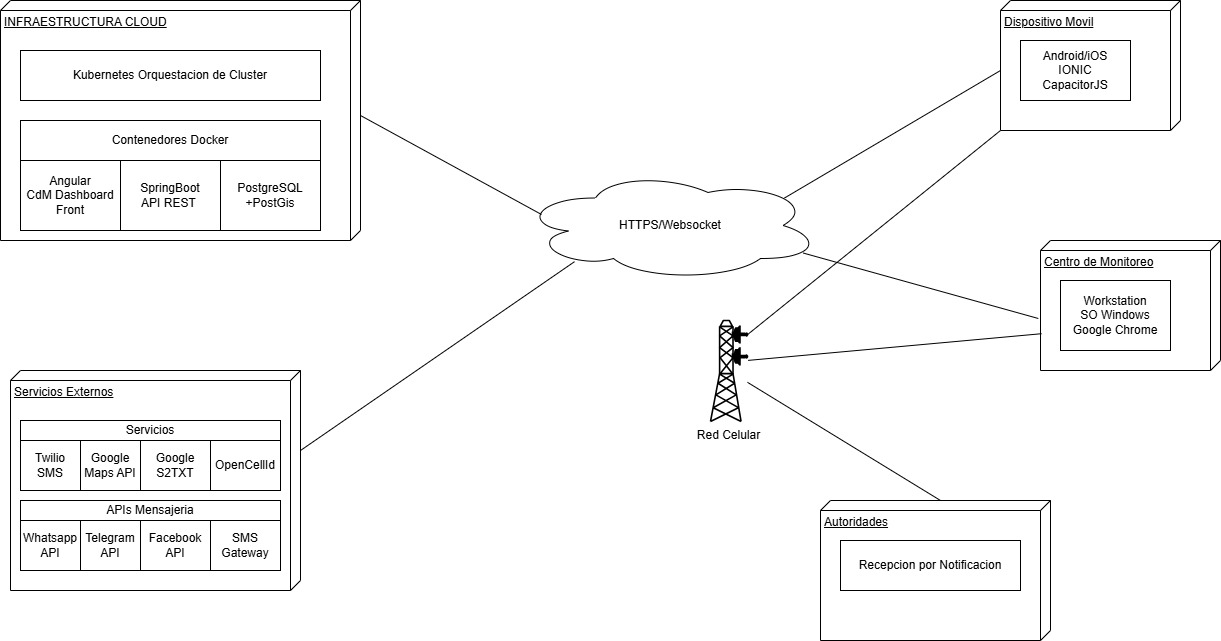
# Implementación

## Modelo de Base de Datos



*Imagen 9-1 Modelo de Base de Datos*

## Diagrama de Despliegue



*Imagen 9-2 Diagrama de Despliegue*

## Versionado del Proyecto

El versionado del proyecto constituye un proceso esencial para la gestión, control y seguimiento de la evolución del sistema de software. Mediante el uso de un sistema de control de versiones distribuido, se registran de manera sistemática los cambios realizados sobre el código fuente, permitiendo mantener un historial completo de modificaciones, facilitar el trabajo colaborativo y asegurar la trazabilidad de las decisiones técnicas adoptadas. Asimismo, el versionado contribuye a mejorar la calidad del desarrollo, al posibilitar la detección temprana de errores, la recuperación ante fallos y la correcta gestión de versiones estables y en desarrollo, favoreciendo la mantenibilidad y escalabilidad del sistema.

El sistema de control de versiones Git permite definir múltiples archivos .gitignore distribuidos jerárquicamente en la estructura del proyecto. Las reglas definidas en estos archivos se aplican de forma acumulativa, otorgando mayor prioridad a aquellos ubicados en niveles más profundos del árbol de directorios. Esta característica posibilita establecer políticas generales de exclusión en la raíz del repositorio y, simultáneamente, definir excepciones o reglas específicas en módulos particulares, facilitando la gestión flexible y precisa del versionado.

### Lineamientos de Versionado

Se adopta el esquema de versionado semántico, estructurado de la siguiente manera:

* **MAJOR** representa cambios incompatibles con versiones anteriores.
* **MINOR** indica la incorporación de nuevas funcionalidades compatibles.
* **PATCH** corresponde a correcciones de errores y mejoras menores.

Se establece una estrategia de ramas simplificada, basada en una rama principal (main) destinada a versiones estables, y ramas auxiliares para el desarrollo de nuevas funcionalidades, correcciones y mejoras.

Se emplean convenciones estandarizadas para los mensajes de commit, con el objetivo de garantizar claridad, trazabilidad y coherencia en el historial de cambios.

Cada versión estable del sistema se identifica mediante etiquetas (tags), facilitando la auditoría, el control de calidad y la posibilidad de revertir cambios ante eventuales fallos.

Se implementa un control sistemático de versiones de base de datos, mediante scripts de migración versionados, garantizando la consistencia estructural entre entornos de desarrollo, prueba y producción.

Se mantiene la compatibilidad retroactiva de las interfaces de programación (API), versionando los servicios expuestos para permitir una transición progresiva entre versiones.

### Repositorios del Proyecto

* GitHub Link: <https://github.com/femartin-dev/secure-on>
* Clonar: git clone <https://github.com/femartin-dev/secure-on.git>

## Lineamientos de Código y Buenas Practicas

### Lineamientos de Código Java

El presente documento establece las convenciones, patrones y buenas prácticas para el desarrollo de software en Java. Su objetivo es mantener un código fuente legible, mantenible, escalable y coherente en todos los proyectos, facilitando la colaboración entre equipos y reduciendo la deuda técnica.

1. **Convenciones de Nomenclatura**

|  |  |  |
| --- | --- | --- |
| Elemento | Convención | Ejemplo |
| Clases | Sustantivos en PascalCase. | Cliente, CuentaBancaria |
| Interfaces | Adjetivos o sustantivos en PascalCase. Opcional prefijo "I". | Serializable, Runnable, RepositorioCliente |
| Métodos | Verbos en camelCase. | obtenerCliente(), calcularTotal() |
| Variables | camelCase, nombres significativos. Evitar abreviaturas. | nombreCliente, totalPagar |
| Constantes | MAYÚSCULAS con guiones bajos. | MAX\_INTENTOS, URL\_BASE |
| Paquetes | Minúsculas, separadas por puntos. Prefijo con dominio invertido. | com.empresa.proyecto.modulo |
| Enumeraciones | PascalCase para el tipo, MAYÚSCULAS para las constantes. | enum Estado { ACTIVO, INACTIVO } |
| Genéricos | Una sola letra mayúscula (T, U, E, K, V). | List<T>, Map<K, V> |

1. **Estructura del Código**
   * *Organización de Archivos*

Una clase pública por archivo, con el mismo nombre del archivo.

Ubicar las clases en paquetes que reflejen su funcionalidad (ej: model, service, controller, repository).

* + *Imports*

Importar clases específicas, no usar import paquete.\*.

Orden: estáticos, luego Java/Jakarta, luego librerías externas, luego proyectos propios. Separar grupos con una línea en blanco.

* + *Indentación y Espacios*

Usar 4 espacios para la indentación (no tabuladores).

Una línea en blanco entre métodos.

Espacios alrededor de operadores binarios (=, +, ==, &&).

Llaves de apertura en la misma línea ( if (condicion) { ).

* + *Longitud de Líneas*

Máximo 120 caracteres. Si excede, dividir la línea de forma legible.

* + *Comentarios*

Evitar comentarios obvios. Preferir código autoexplicativo.

Usar // para comentarios de una línea y /\* \*/ para bloques.

Comentarios TODO o FIXME seguidos de una descripción y responsable.

* + *JavaDoc*

Documentar todas las clases, métodos públicos y constantes.

Incluir descripción, parámetros (@param), retorno (@return) y excepciones (@throws).

Utilizar etiquetas HTML simples cuando sea necesario.

Ej: Código Java

/\*\*

\* Calcula el total de la compra aplicando impuestos.

\*

\* @param subtotal Monto sin impuestos

\* @param tasaImpuesto Porcentaje de impuesto (ej: 0.21 para 21%)

\* @return Total con impuestos incluidos

\* @throws IllegalArgumentException si subtotal es negativo

\*/

public double calcularTotal(double subtotal, double tasaImpuesto) {

// ...

}

1. **Principios de Diseño**

**SOLID:** Aplicar en el diseño de clases.

* **S** (*Responsabilidad Única*): Cada clase debe tener una sola razón para cambiar.
* **O**(*Abierto/Cerrado*): Abiertas para extensión, cerradas para modificación.
* **L** (*Sustitución de Liskov*): Las subclases deben poder reemplazar a sus clases base.
* **I** (*Segregación de Interfaces*): Preferir interfaces específicas a una general.
* **D** (*Inversión de Dependencias*): Depender de abstracciones, no de implementaciones concretas.

**DRY** (*Don't Repeat Yourself*): Evitar duplicación de código mediante abstracciones.

**KISS** (*Keep It Simple, Stupid*): Preferir soluciones simples sobre complejas.

**YAGNI** (*You Aren't Gonna Need It*): No agregar funcionalidad hasta que sea necesaria.

1. **Patrones de Diseño Comunes**

* **Singleton:** su objetivo es garantizar una única instancia de una clase (ej: configuración global). Usar inicialización segura (enum o clase con constructor privado).
* **Factory Method:** sirve para crear objetos sin especificar la clase exacta. Útil para frameworks.
* **Abstract Factory:** es útil para crear familias de objetos relacionados.
* **Builder:** patron que permite construir objetos complejos con muchos parámetros opcionales.
* **Strategy:** permite encapsular algoritmos intercambiables (ej: distintos métodos de pago).
* **Observer:** permite notificar cambios a múltiples objetos (ej: eventos).
* **Decorator:** se encarga de añadir responsabilidades dinámicamente a un objeto.
* **Template Method:** patron que se encarga de definir el esqueleto de un algoritmo, permitiendo que subclases redefinan pasos.
* **DAO / Repository:** permite separar la lógica de acceso a datos del resto de la aplicación.
* **DTO:** su objetivo es transferir datos entre capas sin exponer entidades de dominio.

1. **Manejo de Excepciones**

* Usar excepciones checked para condiciones recuperables (ej: IOException).
* Usar excepciones unchecked (RuntimeException) para errores de programación (ej: NullPointerException).
* No dejar excepciones con catch vacío. Como mínimo, registrar el error (log.error).
* Preferir try-with-resources para recursos que implementan AutoCloseable.
* Lanzar excepciones específicas (ej: ClienteNoEncontradoException) en lugar de genéricas.
* Documentar las excepciones lanzadas con @throws en JavaDoc.

ejemplo

public Cliente buscarCliente(Long id) throws ClienteNoEncontradoException {

Cliente cliente = repositorio.findById(id);

if (cliente == null) {

throw new ClienteNoEncontradoException("Cliente con ID " + id + " no existe");

}

return cliente;

}

1. **Comunicación entre Módulos**

*APIs e Interfaces*

* Definir contratos claros mediante interfaces.
* Usar DTOs (Data Transfer Objects) para intercambiar datos entre capas o servicios remotos.
* Versionar APIs (ej: /api/v1/clientes).

*Eventos y Mensajería*

* Para comunicación asíncrona, utilizar eventos (Spring Events, CDI Events)
* Los eventos deben ser inmutables y contener solo datos necesarios.

*Dependencias*

* Evitar dependencias cíclicas entre módulos.
* Inyectar dependencias mediante constructor (favorece inmutabilidad y testabilidad).

1. **Pruebas**

*Pruebas Unitarias*

* Nombrar métodos de prueba en formato metodo\_condicion\_resultadoEsperado

(ej: calcularTotal\_conImpuesto\_retornaTotalCorrecto).

* Usar @BeforeEach para inicialización común.
* Aislar la unidad bajo prueba mediante mocking (Mockito)
* Cobertura mínima del 80% en líneas de código crítico.

*Pruebas de Integración*

* Verificar interacción con bases de datos, servicios externos, etc.
* Usar bases de datos en memoria (H2) o contenedores (Testcontainers).

*Principios FIRST*

* Fast: Rápidas de ejecutar.
* Independent: Independientes entre sí.
* Repeatable: Repetibles en cualquier entorno.
* Self-validating: Resultado claro (éxito/fallo).
* Timely: Escritas justo antes del código de producción (TDD).

1. **Rendimiento y Buenas Prácticas**

* Evitar optimizaciones prematuras. Primero código claro, luego perfilar si es necesario.
* Usar colecciones adecuadas: ArrayList para acceso por índice, LinkedList para inserciones frecuentes, HashMap para búsquedas.
* Preferir inmutabilidad: usar final para variables y campos, clases record (Java 14+).
* Manejar hilos con ExecutorService en lugar de Thread directamente.
* Sincronizar solo bloques críticos, no métodos completos.
* Utilizar StringBuilder para concatenaciones en bucles.
* Cerrar recursos (archivos, conexiones) correctamente (try-with-resources).

1. **Estilo y Formateo**

Se establece seguir el Google Java Style Guide o el estilo de Oracle.

* Indentación: 4 espacios.
* Líneas en blanco: Separar métodos, bloques lógicos.
* Orden de miembros:
* Constantes estáticas
* Variables estáticas
* Variables de instancia
* Constructores
* Métodos
* Clases internas
* Anotaciones: En líneas separadas (excepto las de parámetros).

1. **Gestión de Dependencias**

* Usar Maven o Gradle para declarar dependencias.
* Mantener versiones en propiedades (Maven) o en bloque ext (Gradle).
* Evitar dependencias con "SNAPSHOT" en ramas estables.

# Pruebas

## Casos de Prueba Unitarios

### UC-001: ACTIVAR ALARMA

1. **Caso de Prueba 1: Activación exitosa sin cancelación**

**ID: CP-001-001**

**Descripción:** Usuario activa la alarma y no cancela durante la ventana de cancelación

**Precondiciones:**

* Dispositivo desbloqueado
* Aplicación en primer plano
* Permisos de ubicación y micrófono concedidos
* Conexión a internet disponible

**Pasos:**

* Usuario presiona botón de alarma
* Sistema muestra ventana de cancelación (15 segundos)
* Usuario NO interactúa con ventana de cancelación
* Tiempo de cancelación expira

Resultado esperado:

* Se bloquea el dispositivo
* Se obtiene ubicación actual
* Se envían alarmas a contactos de emergencia
* Se transmite alarma al centro de monitoreo
* Se inicia grabación de audio
* Se capturan fotos periódicamente
* Se almacenan datos localmente
* Se registra el evento en log del sistema

1. **Caso de Prueba 2: Activación con cancelación exitosa**

**ID: CP-001-002**

**Descripción:** Usuario activa la alarma y la cancela durante la ventana de cancelación

**Precondiciones:**

* Dispositivo desbloqueado
* Usuario con credenciales de autenticación configuradas

**Pasos:**

* Usuario presiona botón de alarma
* Sistema muestra ventana de cancelación
* Usuario selecciona "Cancelar Alarma"
* Usuario ingresa credenciales correctas (PIN/huella)
* Autenticación exitosa

**Resultado esperado:**

* Procesos de alarma se interrumpen
* Evento se registra en log como "cancelado"
* Dispositivo se desbloquea
* Sistema restaura estado normal
* No se envían alarmas externas

1. **Caso de Prueba 3: Activación con falla de autenticación**

**ID: CP-001-003**

**Descripción:** Usuario intenta cancelar pero falla la autenticación

**Precondiciones:**

* Usuario tiene PIN configurado como 1234
* Ventana de cancelación activa

**Pasos:**

* Usuario activa la alarma
* Usuario selecciona "Cancelar Alarma"
* Usuario ingresa PIN incorrecto (0000)
* Sistema muestra error
* Usuario no reintenta antes de que expire el tiempo

**Resultado esperado:**

* Se muestra mensaje de error de autenticación
* Al expirar el tiempo, se procede con la activación completa
* Se ejecutan todos los subprocesos de alarma

1. **Caso de Prueba 4: Activación sin permisos de ubicación**

**ID: CP-001-004**

**Descripción:** Sistema activa alarma sin permisos de ubicación concedidos

**Precondiciones:**

* Permisos de ubicación denegados
* Modo sigiloso desactivado

**Pasos:**

* Usuario activa la alarma
* No se cancela durante ventana de cancelación
* Sistema intenta obtener ubicación

**Resultado esperado:**

* Sistema procede con activación sin datos de ubicación
* Se envía alerta indicando "ubicación no disponible"
* Se ejecutan otros subprocesos (audio, fotos, contactos)
* Se registra error de ubicación en logs

1. **Caso de Prueba 5: Activación sin conexión a internet**

**ID: CP-001-005**

**Descripción:** Alarma se activa sin conectividad de red

**Precondiciones:**

* Dispositivo en modo avión
* Sin conexión Wi-Fi o datos móviles

**Pasos:**

* Usuario activa la alarma
* No se cancela
* Sistema intenta enviar alarmas

**Resultado esperado:**

* Alarmas a contactos se almacenan en cola local
* Transmisión a centro de monitoreo falla
* Datos se almacenan localmente para envío posterior
* Sistema notifica "sin conexión, datos guardados localmente"

### UC-002: ACTIVAR MANUALMENTE

1. **Caso de Prueba 1: Activación manual con presión larga exitosa**

**ID: CP-002-001**

**Descripción:** Usuario presiona botón por más de 3 segundos

**Precondiciones:**

* Tiempo de presión configurado en 3 segundos
* Botón de alarma visible en pantalla principal

**Pasos:**

* *Usuario abre aplicación*
* *Sistema muestra botón de alarma*
* *Usuario mantiene presionado botón por 4 segundos*
* *Resultado esperado:*
* *Se invoca UC-001 directamente*
* *No se muestra diálogo de confirmación*
* *Alarma se activa con modo "manual"*

1. **Caso de Prueba 2:** Activación manual con presión corta y confirmación

**ID: CP-002-002**

**Descripción:** Usuario presiona brevemente y confirma en diálogo

**Precondiciones:**

* Tiempo de presión configurado en 3 segundos

**Pasos:**

* Usuario presiona botón por 2 segundos
* Sistema muestra diálogo de confirmación
* Usuario selecciona "Activar"

**Resultado esperado:**

* Se muestra diálogo de confirmación
* Al confirmar, se invoca UC-001
* Alarma se activa con modo "manual"

1. **Caso de Prueba 3: Activación manual cancelada**

**ID: CP-002-003**

**Descripción:** Usuario presiona brevemente y cancela en diálogo

**Precondiciones:**

* Botón de alarma visible

**Pasos:**

* Usuario presiona botón por 1 segundo
* Sistema muestra diálogo de confirmación
* Usuario selecciona "Cancelar"

**Resultado esperado:**

* Diálogo se cierra
* No se activa alarma
* Sistema permanece en estado normal

1. **Caso de Prueba 4: Botón no visible por configuración**

**ID: CP-002-004**

**Descripción:** Botón de alarma no se renderiza según configuración

**Precondiciones:**

* Configuración "mostrar botón" desactivada

**Pasos:**

* Usuario abre aplicación
* Sistema renderiza pantalla principal
* Resultado esperado:
* Botón de alarma no es visible
* Usuario no puede activar manualmente desde pantalla principal
* Mensaje de log: "Botón deshabilitado por configuración"

### UC-006: BLOQUEAR DISPOSITIVO

1. **Caso de Prueba 1: Bloqueo con modo sigiloso activado**

**ID: CP-006-001**

**Descripción:** Sistema bloquea dispositivo en modo sigiloso

**Precondiciones:**

Modo sigiloso activado en configuración

Permisos de administración de dispositivo concedidos

**Pasos:**

* Desde UC-001 se solicita bloqueo
* GestorBloqueo verifica modo sigiloso
* Sistema ejecuta bloqueo

**Resultado esperado:**

* Pantalla se oscurece completamente
* Botones físicos se deshabilitan
* Métodos de desbloqueo nativos se inhabilitan
* No se muestra interfaz de emergencia visible

1. **Caso de Prueba 2: Bloqueo con modo sigiloso desactivado**

**ID: CP-006-002**

**Descripción:** Bloqueo con interfaz de emergencia visible

**Precondiciones:**

Modo sigiloso desactivado

Permisos de bloqueo concedidos

**Pasos:**

* Se solicita bloqueo desde alarma
* Modo sigiloso está desactivado
* Sistema verifica permisos

**Resultado esperado**

* Muestra interfaz de emergencia a pantalla completa
* Deshabilita métodos de desbloqueo estándar
* Limita botones físicos (volumen, power)
* Mantiene pantalla encendida

1. **Caso de Prueba 3: Bloqueo sin permisos de administración**

**ID: CP-006-003**

**Descripción:** Sistema intenta bloquear sin permisos necesarios

**Precondiciones:**

* Aplicación sin permisos de administrador de dispositivo
* SO Android sin permisos especiales concedidos

**Pasos:**

* Se solicita bloqueo
* Sistema verifica permisos
* Permisos insuficientes

**Resultado esperado:**

* Implementa bloqueo alternativo
* Limita funcionalidad de botones físicos

1. **Caso de Prueba 4: Intento de desbloqueo durante alarma**

**ID: CP-006-004**

**Descripción:** Usuario intenta desbloquear dispositivo durante alarma activa

**Precondiciones:**

* Dispositivo bloqueado por UC-006
* Alarma activa en progreso

**Pasos:**

* Usuario presiona botón de power
* Usuario intenta deslizar para desbloquear
* Usuario intenta usar huella dactilar

**Resultado esperado:**

* Botón de power no responde
* Gestos de desbloqueo están deshabilitados
* Biometría rechaza el desbloqueo
* Pantalla permanece en estado de bloqueo

### UC-007: MOSTRAR VENTANA DE CANCELACIÓN

1. **Caso de Prueba 1: Cancelación exitosa con PIN**

**ID: CP-007-001**

**Descripción:** Usuario cancela alarma ingresando PIN correcto

**Precondiciones:**

* PIN de cancelación configurado como 4567
* Ventana de cancelación visible (15 segundos)

**Pasos**

* Ventana de cancelación se muestra
* Usuario selecciona "Cancelar Alarma"
* Sistema solicita autenticación
* Usuario ingresa PIN: 4567
* Autenticación exitosa

**Resultado esperado:**

* Alarma se cancela inmediatamente
* Ventana de cancelación se oculta
* Estado normal se restaura
* Evento se registra como "cancelado por usuario"

1. **Caso de Prueba 2: Cancelación con huella dactilar**

**ID: CP-007-002**

**Descripción:** Usuario cancela usando autenticación biométrica

**Precondiciones:**

* Huella dactilar registrada en dispositivo
* Biometría configurada para cancelación

**Pasos:**

* Usuario selecciona cancelar
* Sistema muestra opción de huella
* Usuario escanea huella válida
* Autenticación biométrica exitosa

**Resultado esperado:**

* Autenticación biométrica aceptada
* Alarma se cancela
* No se solicita PIN adicional
* Ventana se cierra

1. **Caso de Prueba 3: Múltiples intentos fallidos de autenticación**

**ID: CP-007-003**

**Descripción:** Usuario falla autenticación múltiples veces

**Precondiciones:**

* Límite de 3 intentos configurado
* Tiempo de cancelación: 15 segundos

**Pasos:**

* Usuario selecciona cancelar
* Ingresa PIN incorrecto (intento 1)
* Ingresa PIN incorrecto (intento 2)
* Ingresa PIN incorrecto (intento 3)
* Tiempo aún no ha expirado

**Resultado esperado:**

* Primer y segundo intento muestran error
* Tercer intento bloquea autenticación por 30 segundos
* Mensaje: "Demasiados intentos, espere 30 segundos"
* Alarma continúa si tiempo de ventana expira

1. **Caso de Prueba 4: Tiempo de cancelación expirado**

**ID: CP-007-004**

**Descripción:** Ventana de cancelación expira sin interacción

**Precondiciones:**

* Tiempo de cancelación configurado a 15 segundos
* Usuario no interactúa con dispositivo

**Pasos:**

* Ventana de cancelación se muestra
* Cuenta regresiva inicia desde 15
* Usuario no toca la pantalla
* Temporizador llega a 0

**Resultado esperado:**

* Ventana se oculta automáticamente
* Alarma procede con activación completa
* No se requiere interacción adicional
* Log registra: "Cancelación expirada, alarma activada"

1. **Caso de Prueba 5: Cancelación durante modo sigiloso**

**ID: CP-007-005**

**Descripción:** Usuario intenta cancelar cuando modo sigiloso está activo

**Precondiciones:**

* Modo sigiloso activado
* Pantalla oscura durante activación

**Pasos:**

* Alarma se activa en modo sigiloso
* Pantalla está oscura
* Usuario presiona área de pantalla para cancelación
* Sistema muestra interfaz de cancelación sobreexpuesta

**Resultado esperado:**

* Interfaz de cancelación es visible sobre fondo oscuro
* Autenticación funciona normalmente
* Si se cancela, pantalla vuelve a estado normal
* Si no, pantalla vuelve a oscuro completo

# Bibliografía

* *The unified software development process. Addison-Wesley Professional. Jacobson, I., Booch, G., & Rumbaugh, J. (1999).*
* *Docker: Up & Running: Shipping Reliable Containers in Production (3ra ed.). O'Reilly Media. Kane, S., & Matthias, K. (2023).*
* *Angular. (s.f.). Angular documentation. Recuperado el 10 de diciembre de 2025, de* <https://angular.dev/>
* *Android Developers. (s.f.). Documentación para desarrolladores de Android. Recuperado el 10 de diciembre de 2025, de* <https://developer.android.com/>
* *Capacitor. (s.f.). Capacitor documentation. Recuperado el 10 de diciembre de 2025, de* <https://capacitorjs.com/docs/>
* *Ionic. (s.f.). Ionic documentation. Recuperado el 10 de diciembre de 2025, de* <https://ionicframework.com/docs/>
* *Oracle. (s.f.). Java Platform, Standard Edition Documentation. Recuperado el 10 de diciembre de 2025, de* <https://docs.oracle.com/javase/>
* *MDN Web Docs. (s.f.). Referencia de JavaScript. Recuperado el 10 de diciembre de 2025, de* <https://developer.mozilla.org/es/docs/Web/JavaScript>
* *PostGIS Project. (s.f.). PostGIS documentation. Recuperado el 10 de diciembre de 2025, de* <https://postgis.net/documentation/>
* *PostgreSQL Global Development Group. (s.f.). PostgreSQL documentation. Recuperado el 10 de diciembre de 2025, de* <https://www.postgresql.org/docs/>
* *Spring. (s.f.). Spring Boot Reference Documentation. Recuperado el 10 de diciembre de 2025, de* <https://docs.spring.io/spring-boot/documentation.html>
* *Google. (s.f.). Documentación de Google Maps Platform. Recuperado el 10 de diciembre de 2025, de* <https://developers.google.com/maps/documentation?hl=es-419>