PL1 Ingeniería del Software

Cristina Martínez Toledo: 09109126E
Roberto Seco Volkava: 09854422A

Indice

1. INTRODUCCIÓN

En un contexto global donde el cambio climático está incrementando la frecuencia e intensidad de los desastres naturales, es fundamental desarrollar herramientas tecnológicas que permitan mitigar sus impactos y mejorar la capacidad de respuesta ante emergencias. Entre estos fenómenos, las inundaciones severas representan una amenaza significativa para comunidades urbanas y rurales, causando pérdidas humanas, daños materiales y afectaciones a infraestructuras críticas.

Este trabajo tiene como objetivo abordar las fases de requisitos y análisis para el desarrollo de un sistema informático de alarma y prevención de riesgos ante catástrofes naturales, centrado en la detección temprana y prevención de eventos climáticos extremos. A través de la integración de datos ambientales en tiempo real, predicciones climáticas y mecanismos de notificación automática, el sistema permitirá una gestión eficiente de alertas y una respuesta rápida ante eventos climáticos extremos.

El sistema estará accesible mediante aplicación web y móvil, garantizando la vigilancia en tiempo real de variables críticas y la emisión de alertas hacia la población y las autoridades competentes. Se considerarán aspectos de seguridad, privacidad y cumplimiento normativo desde las primeras fases del diseño.

Este documento detalla los objetivos del sistema, actores implicados, funcionalidades esperadas y las condiciones bajo las cuales deberá operar, sirviendo como base formal para su posterior desarrollo técnico.

2. ESPECIFICACIÓN DE REQUISITOS

2.1 Propósito

El propósito de este documento es definir de forma clara, precisa y completa las fases de especificación de requisitos y análisis del desarrollo de un sistema informático que permitirá la monitorización en tiempo real de variables ambientales críticas, el procesamiento inteligente de datos y la emisión de alertas automáticas y geolocalizadas ante eventos climáticos extremos, con especial enfoque en la prevención de inundaciones severas y sus riesgos asociados. Este documento servirá como guía tanto para los desarrolladores como para los usuarios finales, responsables del mantenimiento y para todos los interesados involucrados en el desarrollo, implementación y utilización del sistema.

2.2. Ámbito del Sistema

El nombre del sistema será SIPREC (Sistema Inteligente de Prevención y Respuesta ante Eventos Climáticos). El SIPREC será un sistema informático diseñado para la monitorización en

tiempo real de variables ambientales críticas y la gestión de alertas tempranas ante eventos climáticos extremos, con especial énfasis en la prevención de inundaciones.

El sistema abarcará las siguientes funcionalidades principales:

- La recolección y análisis de datos en tiempo real desde sensores hidrológicos, estaciones meteorológicas y otras fuentes relevantes.
- Predecir riesgos climáticos de manera automática utilizando modelos predictivos basados en información meteorológica y umbrales de riesgo predefinidos.
- Generar alertas automáticas geolocalizadas en caso de detección de condiciones peligrosas, notificando a las autoridades y a la población afectada mediante SMS, notificaciones móviles y por correo electrónico, si así lo deciden.
- Interacción con la población, incluyendo recepción de informes post-evento, acceso a guías de actuación en emergencias, o envío de alertas y recomendaciones de seguridad, así como permitir a los usuarios enviar reportes a los sistemas de emergencia correspondientes sobre afectaciones en su zona.
- Coordinar acciones con organismos de emergencia, facilitando la toma de decisiones basada en información precisa y actualizada
- Accesibilidad multiplataforma, con versiones web y móvil, que permite operar ciertas funcionalidades del sistema incluso en modo offline.
- Seguridad de la información, mediante autenticación multifactor, cifrado extremo a extremo y registros de auditoría.
- Cumplimiento legal, garantizando la protección de datos personales conforme a las normativas europeas.

El sistema no hará lo siguiente:

- No reemplazará la toma de decisiones de los organismos de emergencia, sino que servirá como un apoyo tecnológico para mejorar la eficiencia de su respuesta.
- No hará predicciones meteorológicas propias: Aunque integrará servicios meteorológicos externos para análisis predictivo, el sistema no generará sus propios modelos climáticos ni sustituirá a agencias oficiales de meteorología.
- No actuará de forma autónoma en la ejecución de medidas físicas de mitigación (ej. cierre de compuertas, evacuación de áreas), sino que alertará a las autoridades responsables para que tomen las decisiones correspondientes.
- No tomará decisiones autónomas de evacuación o cierre de infraestructuras: La interpretación final de los datos y la ejecución de acciones y envío de notificaciones relacionadas con acciones a tomar ante un cierto evento climático extremo, como evacuaciones o cierres de carreteras, quedará en manos de las autoridades competentes.
- No almacenará imágenes ni videos en tiempo real: El sistema no contempla la captura, transmisión o almacenamiento de contenido audiovisual en vivo desde cámaras u otros dispositivos, limitándose al análisis y almacenamiento de datos estructurados y reportes de usuarios.

- No permitirá la interacción directa entre usuarios generales (no autorizados): la plataforma no funcionará como una red social ni tendrá funciones de mensajería entre ciudadanos.

Entre los beneficios esperados está la reducción del impacto de desastres naturales, minimizando pérdidas humanas y materiales, la mejora de la eficiencia en la toma de decisiones por parte de los organismos de respuesta ante emergencias y la mejora en la comunicación y coordinación entre entidades gubernamentales, servicios de emergencia y la población afectada, además de la automatización de la generación de alertas, permitiendo una respuesta más rápida y efectiva ante eventos climáticos extremos. Es fundamental además garantizar que el sistema sea escalable, seguro y accesible, cumpliendo con normativas de protección de datos.

2.3. Definiciones, Acrónimos y Abreviaturas

- SIPREC: Sistema Inteligente de Prevención y Respuesta ante Eventos Climáticos.
- IoT: Internet of Things (Internet de las Cosas). Hace referencia a la red de sensores y dispositivos conectados que recopilan y transmiten datos.
- API: Application Programming Interface. Conjunto de funciones y procedimientos que permiten la comunicación entre sistemas de software.
- SMS: Servicio de Mensajes Cortos.
- RGPD: Reglamento General de Protección de Datos.
- MQTT: Message Queuing Telemetry Transport. Protocolo ligero de mensajería usado para comunicación M2M e IoT.
- HTTP/HTTPS: Hypertext Transfer Protocol / Secure. Protocolos estándar para la transferencia de datos en la web.
- IEEE: Institute of Electrical and Electronics Engineers.
- RBAC: Role-Based Access Control. Control de acceso basado en roles.
- REST / RESTful Representational State Transfer. Estilo arquitectónico de APIs que utiliza HTTP para operaciones CRUD.
- 2FA / MFA: Two-Factor Authentication / Multi-Factor Authentication. Métodos de autenticación reforzada que requieren múltiples pruebas de identidad.
- GIS: Geographic Information System. Sistemas de información geográfica usados para mapear y analizar datos espaciales.
- WCAG 2.1: Web Content Accessibility Guidelines, versión 2.1. Normativa para garantizar la accesibilidad web.
- OWASP: Open Web Application Security Project. Proyecto que proporciona directrices sobre seguridad en aplicaciones web.
- CSRF: Cross-Site Request Forgery. Tipo de ataque que explota la confianza de un sitio web hacia el navegador del usuario.

- CSV / JSON / XLSX Formatos estándar para el intercambio y análisis de datos: Comma-Separated Values, JavaScript Object Notation, Excel Spreadsheet.
- XSS: Cross-Site Scripting. Ataque basado en la inyección de scripts maliciosos en páginas web.
- IoT: Internet of Things (Internet de las Cosas). Red de dispositivos físicos interconectados que recopilan y transmiten datos.
- TPS: Transactions Per Second. Transacciones por segundo que el sistema debe soportar.
- JSON / CSV / XLSX Formatos de intercambio de datos: JavaScript Object Notation, valores separados por coma, y Excel Spreadsheet.
- TLS 1.3: Transport Layer Security, versión 1.3. Protocolo criptográfico para la seguridad en las comunicaciones.
- AES-256: Advanced Encryption Standard con clave de 256 bits. Estándar de cifrado simétrico.
- IDS / IPS: Intrusion Detection / Prevention Systems. Sistemas de detección y prevención de intrusos.
- EN 301 549: Estándar europeo de accesibilidad para productos y servicios TIC.
- AEMET / ECMWF / SMN: Agencias meteorológicas oficiales: Agencia Estatal de Meteorología (España), European Centre for Medium-Range Weather Forecasts, y Servicio Meteorológico Nacional (de distintos países).
- DDoS: Distributed Denial of Service. Ataque que busca colapsar un sistema mediante múltiples solicitudes simultáneas.
- Sensor IoT: Dispositivo conectado a internet que recolecta información del entorno físico (como temperatura, humedad o nivel del río).
- Offline: Capacidad de funcionar sin conexión a internet.
- Microservicios: Una arquitectura basada en microservicios divide el sistema en componentes independientes que pueden ser desarrollados, desplegados, escalados y actualizados de forma separada.
-

2.4. Referencias

- IEEE Std 830-1998 – IEEE Recommended Practice for Software Requirements Specifications. Estándar internacional para la redacción estructurada, verificable y trazable de especificaciones de requisitos de software.
- ISO/IEC 27001 – Seguridad de la información y gestión de riesgos. Norma internacional que establece un sistema de gestión para proteger activos de información frente a amenazas, garantizando su confidencialidad, integridad y disponibilidad.
- ISO/IEC 27017 – Seguridad para servicios cloud: directrices para proveedores y clientes. Extensión de la norma ISO/IEC 27001 centrada en entornos de computación en la nube, tanto públicos como privados.

- GDPR (UE 2016/679) – Reglamento General de Protección de Datos de la Unión Europea. Normativa europea obligatoria sobre la protección de datos personales y privacidad de los ciudadanos, con implicaciones directas en el tratamiento de la información dentro del sistema.
- ISO 22320 – Gestión de emergencias: requisitos para la gestión eficaz de incidentes. Establece los principios de interoperabilidad, coordinación y toma de decisiones durante situaciones de emergencia.
- ISO 19115 – Normativa internacional para metadatos geoespaciales. Estándar para la descripción y estructuración de datos espaciales, clave en sistemas que integran mapas interactivos y capas GIS.
- ISO/IEC 25010 – Modelo de calidad del software: características y subcaracterísticas. Define los atributos que debe tener un software de calidad, incluyendo fiabilidad, mantenibilidad, usabilidad, seguridad, eficiencia y portabilidad.
- WCAG 2.1 Nivel AA – Directrices de accesibilidad para contenidos web. Conjunto de recomendaciones para hacer accesible el contenido digital a personas con discapacidad, conforme a la legislación europea y española.
- EN 301 549 – Accesibilidad de productos y servicios TIC en el contexto europeo. Norma obligatoria para la accesibilidad en tecnologías digitales utilizadas por administraciones públicas y servicios esenciales.
- OWASP Top 10 – Buenas prácticas para la seguridad de aplicaciones web y móviles.
- TLS 1.3 o superior – Estándar para comunicaciones cifradas y transmisión segura de datos. Protocolo de cifrado que garantiza la confidencialidad e integridad de la información transmitida en redes.
- Reglamento de desarrollo del RD 1112/2018 (España) – Accesibilidad digital del sector público. Normativa española que adapta WCAG 2.1 al contexto nacional y define requisitos obligatorios para aplicaciones y sitios web públicos.

Además de las normativas y estándares anteriores, el desarrollo del sistema se ha apoyado en tecnologías ampliamente reconocidas como MQTT (protocolo de mensajería ligero para IoT), HTTP/HTTPS (protocolo web seguro), FastAPI y Node.js (frameworks para desarrollo backend), React y Angular (librerías para desarrollo frontend), PostgreSQL y MongoDB (gestores de bases de datos relacional y NoSQL), Docker y Kubernetes (contenedores y orquestación), Firebase Cloud Messaging y AWS SNS (notificaciones push), SendGrid y SMTP (correo electrónico), y plataformas GIS como OpenStreetMap, Mapbox y Google Maps para la visualización geográfica.

El uso de estas tecnologías se documenta y respalda mediante herramientas como Swagger/OpenAPI para la documentación de APIs, y se aplican estándares de buenas prácticas para la integración, despliegue y mantenimiento continuo del sistema.

2.5. Visión General del Documento

Este documento constituye la Especificación de Requisitos del Software (ERS) del Sistema Inteligente de Prevención y Respuesta ante Eventos Climáticos (SIPREC). Ha sido elaborado siguiendo las directrices establecidas en el estándar IEEE Std 830-1998 y contiene una descripción exhaustiva y estructurada de todos los elementos necesarios para el desarrollo, validación y mantenimiento del sistema.
El documento está organizado en varias secciones, cada una centrada en un aspecto específico del sistema:

- Sección 1 – Introducción: Presenta el contexto del sistema, su objetivo general, alcance y motivación para su desarrollo.
- Sección 2 – Descripción General del Sistema: Resume las características clave del SIPREC, incluyendo el ámbito del sistema, sus funciones principales, actores involucrados, restricciones generales, suposiciones, dependencias y requisitos futuros.
- Sección 3 – Requisitos Específicos: Especifica los requisitos funcionales y no funcionales del sistema (relacionados con rendimiento, diseño, interfaces, seguridad, fiabilidad, mantenibilidad, requerimientos legales y otros atributos de calidad)

2.6 Descripción General

2.6.1. Perspectiva del Producto

El Sistema Inteligente de Prevención y Respuesta ante Eventos Climáticos (SIPREC) se concibe como una solución modular, escalable y distribuida, orientada a complementar las capacidades existentes de vigilancia meteorológica, gestión de emergencias y comunicación con la población. El sistema actuará como una herramienta interoperable de apoyo a organismos de emergencia, autoridades locales y usuarios en zonas de riesgo, accesible mediante aplicación web y móvil. El sistema deberá interoperar con otras plataformas existentes, tales como:

1. Sistemas de entrada y adquisición de datos
   - Sistemas Meteorológicos Oficiales
     SIPREC deberá integrarse con APIs y bases de datos ofrecidas por organismos como el Servicio Meteorológico Nacional (SMN), AEMET, ECMWF u otras entidades internacionales, utilizando formatos estandarizados (JSON/XML, RESTful APIs) y **servicios programados o en tiempo real.**

   - Redes de Sensores Ambientales (IoT)
     El sistema deberá conectarse con plataformas que integran sensores desplegados por organismos públicos o privados (pluviómetros, sensores de caudal, temperatura, humedad, etc.). La interoperabilidad se realizará mediante protocolos IoT como MQTT, HTTP, o CoAP, con capacidad para adaptar los datos de las múltiples fuentes heterogéneas de datos a un esquema unificado de procesamiento interno.

2. Sistemas de georreferenciación y visualización
   - Infraestructuras de mapas y geolocalización
     SIPREC integrará servicios de mapas interactivos mediante proveedores como Google Maps, OpenStreetMap, Mapbox, u otros equivalentes, para representar zonas en riesgo, rutas de evacuación y capas GIS relevantes.

3. Sistemas de notificación y alerta
   - SIPREC deberá emitir alertas mediante:
     -SMS masivos a través de pasarelas SMPP o HTTP API de operadores móviles.
     -Correo electrónico vía SMTP seguro o servicios como SendGrid.
     -Notificaciones móviles push, utilizando Firebase Cloud Messaging (FCM), AWS SNS, o Apple Push Notification Service (APNs).

4. Infraestructura tecnológica y de procesamiento
   - Uso de Amazon Web Services (AWS), Microsoft Azure o Google Cloud Platform (GCP) para el despliegue de servicios de backend, bases de datos, almacenamiento de logs y procesamiento masivo de datos. Servicios de análisis en tiempo real como AWS Lambda, Google BigQuery o Azure Stream Analytics podrán ser utilizados para escalar la capacidad predictiva y de correlación de datos del sistema.

2.6.2. Funciones del Producto

El SIPREC proporcionará un conjunto de funciones clave organizadas en cuatro áreas principales:

1. Adquisición y análisis de datos
   - Recolección en tiempo real de variables ambientales críticas a través de sensores meteorológicos, hidrológicos, de viento, humedad y temperatura.
   - Análisis y validación de datos por expertos científicos, quienes podrán revisar datos históricos, generar modelos predictivos y colaborar en la calibración del sistema.
   - Análisis de datos automático según un cierto modelo predictivo. Estimación de posibles escenarios de riesgo e impacto basado en datos históricos y actuales.

2. Generación y distribución de alertas
   - Generación automática de alertas geolocalizadas ante la detección de condiciones peligrosas, en base a umbrales definidos por expertos o algoritmos predictivos.
   - Determinados perfiles de usuario, definidos en secciones posteriores, podrán gestionar manualmente alertas existentes.
   - Envío de las notificaciones de alerta vía SMS, email y en la aplicación móvil.
   - Historial de eventos y alertas para auditoría y análisis posterior.

3. Gestión de usuarios e interfaz de visualización
   - Acceso diferenciado según perfiles de usuario, permitiendo funcionalidades específicas para científicos, autoridades gubernamentales, servicios de emergencia y ciudadanía

- Configuración personalizada de alertas y notificaciones.
- Garantía de accesibilidad y usabilidad, adaptando la plataforma para personas con discapacidades sensoriales, motoras o cognitivas, conforme a las normas vigentes.
- Panel de administración para la gestión de usuarios y control de permisos.
- Visualización de datos en tiempo real, con distinto nivel de detalle y formato dependiendo del tipo de usuario.

4. Coordinación interinstitucional
    - Comunicación estructurada en tiempo real entre organismos meteorológicos, autoridades gubernamentales y servicios de emergencia.
    - Generación de reportes y análisis de eventos previos para mejorar estrategias de mitigación

El sistema también contará con soporte limitado en modo offline desde la aplicación móvil, garantizando el acceso a funciones críticas en condiciones de conectividad restringida. Asimismo, todas las funcionalidades estarán protegidas mediante controles de acceso, cifrado de datos y cumplimiento de las normativas europeas de protección de datos personales.

2.6.3. Características de los Usuarios

SIPREC estará diseñado para ser utilizado por diferentes tipos de usuarios, cada uno con distintos niveles de conocimiento técnico y responsabilidades dentro del sistema:
1. Personal de gestión de emergencias
Entre estos usuarios se encuentran organismos de protección Civil, bomberos, unidades de rescate y otros organismos encargados de la respuesta ante desastres. Tienen una formación técnica o universitaria en áreas como gestión de riesgos, seguridad civil o emergencias y alta experiencia en la gestión de emergencias, pero variable en el uso de sistemas informáticos avanzados, por lo que necesitan una interfaz intuitiva y accesible para la toma rápida de decisiones, que facilite el acceso rápido a mapas, alertas activas y rutas de evacuación. Además necesitan capacidad para registrar incidentes de campo y consultar información actualizada en tiempo real y acceso operativo a funciones específicas de su rol sin sobrecarga de información técnica.

2. Autoridades gubernamentales y municipales
Incluyen funcionarios de planificación territorial, urbanismo y medio ambiente, con formación universitaria en administración pública, ingeniería ambiental, geografía o disciplinas relacionadas. Su experiencia variará según el cargo, pero en general cuentan con experiencia en gestión de políticas de prevención de desastres. Estos usuarios tendrán un acceso privilegiado a la mayoría de funcionalidades, paneles estratégicos de visualización y toma de decisiones, y necesitan capacidad para activar o validar alertas, supervisar informes y coordinar instituciones, generar reportes institucionales y análisis post-evento, y tendrán control sobre permisos de otros usuarios institucionales.

3. Centros meteorológicos y científicos
Usuarios como meteorólogos, hidrólogos y analistas de datos ambientales, con formación universitaria o de posgrado en ciencias meteorológicas, hidrología, ingeniería ambiental o geofísica. Tienen una alta experiencia en el análisis de datos climáticos y la predicción de eventos meteorológicos, y están muy familiarizados con software de modelado climático y bases de datos meteorológicas.
Estos usuarios requieren acceso privilegiado a datos en bruto, históricos y en tiempo real, y herramientas avanzadas para poder llevar a cabo análisis estadísticos y modelizaciones, además de tener la capacidad de hacer propuestas relacionadas con la gestión de las alarmas, actualizar los modelos de predicción y llevar a cabo otras funciones críticas

4. Población general y comunidades en zonas de riesgo
Son los ciudadanos que habitan en áreas que puedan llegar a ser vulnerables a inundaciones y otros desastres naturales. Tienen un nivel educacional muy diverso, desde personas con educación básica hasta niveles universitarios, y en general poca o nula experiencia en sistemas tecnológicos avanzados o prevención de riesgos. Sin embargo, debido a la expansión de las nuevas tecnologías hoy en día, están muy familiarizados con dispositivos móviles y aplicaciones de notificación. Por esto, necesitan una interfaz simple y accesible para recibir las alertas y recomendaciones de seguridad, además de que la información que se les proporcione debe ser clara y directa, sin tecnicismos complejos, para que sea un software “para todo el mundo” y las alarmas e información lleguen al mayor número de personas posible.

Para aumentar el alcance del sistema, este estará diseñado con interfaces accesibles, multilingües, compatibles con dispositivos móviles y con principios de diseño inclusivo para personas con discapacidad, y todas las interfaces y funcionalidades del sistema estarán diseñadas considerando las características específicas de cada perfil de usuario, con el objetivo de maximizar la usabilidad, seguridad y efectividad operativa de SIPREC.

2.4. Restricciones

2.4.1 Políticas de la Empresa

El desarrollo del SIPREC deberá alinearse con las siguientes directrices:

- Cumplimiento de normativas y estándares nacionales e internacionales en gestión de emergencias y protección de datos (punto 3.5.3).
- Las acciones relacionadas con la emisión de alertas a la población deberán ser autorizadas o supervisadas por personal autorizado competente, siguiendo protocolos establecidos
- Durante el desarrollo, se deberá seguir una política organizacional de control de versiones, revisión de código y documentación exhaustiva del software, basada en buenas prácticas de ingeniería (por ejemplo, uso de Git con gestión de ramas).

- Enfoque en la escalabilidad, reutilización y mantenimiento del sistema, asegurando su evolución en el tiempo, con una arquitectura modular.

2.4.2 Limitaciones del Hardware

El sistema deberá ser compatible con la infraestructura tecnológica existente, considerando:

- Servidores del sistema potentes con procesadores multi-núcleo y capacidad de procesamiento en tiempo real.
- Compatibilidad con los protocolos de los sensores hidrológicos (LoRa, ZigBee, MQTT…).
- Dispositivos móviles compatibles con Android e iOS, con capacidad para recibir notificaciones push.
- Los dispositivos de usuarios móviles pueden ser de gama media o baja, por lo que la aplicación debe ser liviana y eficiente, funcional incluso con recursos limitados de CPU, memoria o batería.
- En escenarios críticos, el sistema debe operar con infraestructura mínima o degradada, incluyendo modos offline.

2.4.3 Interfaces con Otras Aplicaciones

El SIPREC deberá integrarse con otros sistemas mediante APIs y protocolos estándar, incluyendo:

- Servicios meteorológicos como ECMWF, NOAA, AEMET o SMN.
- Sensores IoT conectados a la red mediante MQTT o HTTP.
- Sistema de Posicionamiento Global (GPS) u otros sistemas de localización para obtener la ubicación de los usuarios
- Sistemas de comunicación masiva para la difusión de alertas vía SMS, notificaciones push y email
- Conexiones de red mediante Wi-Fi, 4G, 5G u otras tecnologías, necesarias para el envío y recepción de datos en tiempo real desde sensores y dispositivos móviles

2.4.4 Operaciones Paralelas

El sistema deberá soportar la ejecución de múltiples procesos simultáneos, incluyendo:

- Monitoreo en tiempo real de múltiples fuentes de datos sin afectar el rendimiento.
- Procesamiento paralelo y asincrónico en tareas críticas como el análisis de datos en tiempo real, envío de alertas masivas y gestión de sensores.
- Múltiples usuarios accediendo simultáneamente a recursos compartidos (visualización de mapas, activación de alertas, consulta de reportes).
- Acceso simultáneo de múltiples usuarios con distintos niveles de permisos.

Se deberá asegurar consistencia y sincronización en operaciones concurrentes, especialmente en la actualización de datos críticos como estado de alertas o rutas de evacuación.

2.4.5 Funciones de Auditoría

El SIPREC también deberá contar con un módulo de auditoría que registre:

- Acciones realizadas por cada usuario (alta, modificación o eliminación de datos).
- Eventos, alertas generadas y modificaciones en el sistema realizadas por cada usuario.
- Historial de accesos fallidos o intentos de autenticación no válidos.

Estos registros deberán cumplir con las normativas de seguridad de la información, que se verán en puntos posteriores, y permitir trazabilidad completa en caso de auditorías o incidentes.

2.4.6 Funciones de Control

El sistema implementará funciones de control, realizadas por distintos usuarios autorizados, para garantizar su operatividad y seguridad:

- Control de acceso basado en roles (RBAC) para limitar permisos de usuarios.
- Activación, modificación o anulación manual de alertas.
- Gestión de configuraciones centralizada, permitiendo modificar umbrales de riesgo y modelos meteorológicos sin afectar la estabilidad del sistema.

2.4.7 Lenguajes de Programación

Para el desarrollo del SIPREC se utilizarán los siguientes lenguajes de programación:

- Backend: Python y Node.js para procesamiento de datos y servicios API.
- Frontend Web: React o Angular para la interfaz de usuario.
- Aplicación Móvil: Kotlin (Android) y Swift (iOS) para las aplicaciones móviles nativas o Flutter o React Native como opción multiplataforma.
- Base de Datos: PostgreSQL para datos estructurados y MongoDB para almacenamiento de registros de eventos.

2.4.8 Protocolos de Comunicación

El SIPREC utilizará protocolos estándar para garantizar la interoperabilidad y eficiencia en la transmisión de datos:

- HTTP/HTTPS para la comunicación entre clientes y servidores.
- MQTT para la transmisión de datos en tiempo real desde sensores hidrológicos.
- RESTful APIs y WebSockets para integración con otros sistemas y actualización en tiempo real.
- SMTP y SMS Gateway para la difusión de alertas a usuarios.

2.4.9 Requisitos de Habilidad

- El sistema debe estar diseñado considerando que los usuarios tendrán diferentes niveles de competencia técnica, desde personal altamente técnico (científicos, analistas) hasta usuarios no especializados (comunidades locales).

- Las interfaces deben ser intuitivas, accesibles y adaptadas a distintos perfiles, mediante personalización del panel o ayudas contextuales.

2.4.10 Criticalidad de la Aplicación

El SIPREC es un sistema crítico para la prevención de desastres naturales y la seguridad pública, lo que implica:

- Alta disponibilidad, evitando tiempos de inactividad en momentos clave.
- Tolerancia a fallos, con respaldo en servidores redundantes y balanceo de carga.
- Recuperación ante desastres, con copias de seguridad automáticas y almacenamiento en la nube.
- Las actualizaciones del sistema deben ser controladas y auditables, evitando interrupciones imprevistas.

2.4.11 Consideraciones Acerca de la Seguridad

La seguridad del sistema es prioritaria para evitar accesos no autorizados y manipulación de datos. Se implementarán:

- Cifrado de datos en tránsito y en reposo (TLS 1.3, AES-256).
- Autenticación multifactor (MFA) para accesos administrativos.
- Firewall y detección de intrusos para prevenir ataques cibernéticos.
- Cumplimiento con regulaciones de protección de datos (3.4.3)
- Control de acceso por roles
- Prevención contra ataques comunes (inyección, CSRF, XSS)
- Auditoría y monitoreo continuo
- Evaluaciones periódicas de seguridad y pruebas de penetración.
- Se utilizarán librerías y dependencias actualizadas, evitando vulnerabilidades conocidas
- Toda la infraestructura deberá cumplir con normas ISO 27001 (seguridad de la información) o equivalentes en materia de seguridad.

Las restricciones de seguridad y estándares que se tienen que seguir se tratarán de forma detallada en apartados posteriores.

2.5. Suposiciones y Dependencias

El desarrollo e implementación de SIPREC dependen de una serie de factores técnicos, organizacionales y operativos. Si alguno de estos factores cambiase, podría ser necesario ajustar los requisitos del sistema.

2.5.1 Suposiciones

El desarrollo del sistema se basa en las siguientes suposiciones:

- Disponibilidad de Sensores y Fuentes de Datos.

    - Existen redes de sensores meteorológicos e hidrológicos en las zonas objetivo, o se proveerán mediante colaboración con entidades públicas o privadas.
    - Los sensores utilizan protocolos de transmisión compatibles (MQTT, HTTP, CoAP, etc.) y disponen de conectividad suficiente para el envío periódico de datos.
    - SIPREC tendrá acceso autorizado a APIs de meteorología oficial como AEMET, ECMWF, NOAA o equivalentes.

- Infraestructura y Recursos Tecnológicos
    - SIPREC se desplegará sobre servidores en la nube o infraestructura local con alta disponibilidad.
    - El entorno de ejecución soportará los lenguajes, protocolos y arquitecturas definidos en los apartados técnicos del documento.
    - Se espera que los servidores, servicios en la nube, conectividad y soporte técnico estén garantizados durante toda la vida útil del sistema.
    - Se espera que los usuarios dispongan de dispositivos compatibles con navegadores web modernos y sistemas móviles con Android o iOS.
    - Los usuarios (especialmente autoridades y servicios de emergencia) y los sensores tendrán acceso a una red funcional para transmitir y recibir información en tiempo real. En zonas con conectividad limitada, algunas funcionalidades (como sincronización de reportes) podrían no estar garantizadas.

- Adopción institucional
    - Se presupone que las entidades gubernamentales, meteorológicas y de emergencia adoptarán el sistema y lo integrarán en sus protocolos de gestión de riesgos, por lo que los científicos, analistas y administradores del sistema dispondrán del tiempo, conocimiento y herramientas para mantener actualizados los umbrales de riesgo, modelos predictivos…
    - Las entidades colaboradoras participarán en la instalación, mantenimiento y operación de sensores.

2.5.2 Dependencias

El funcionamiento del SIPREC está sujeto a una serie de dependencias clave externas que, en caso de cambiar o fallar, podrían afectar su operatividad:

- Infraestructura Tecnológica
    - Dependencia de proveedores de servicios en la nube para el almacenamiento y procesamiento de datos.
    - Necesidad de servidores de alta disponibilidad para garantizar tiempos de respuesta mínimos.
- Integración con Sistemas Externos.
    - El sistema depende del correcto funcionamiento de servicios externos como proveedores de meteorología, mapas, geolocalización, y telecomunicaciones,

según lo visto en el punto 2.4.3. Fallos o interrupciones en estos servicios pueden afectar directamente a la operatividad del sistema.

- Regulaciones y Políticas Gubernamentales (punto 3.5.3)
    - SIPREC depende del cumplimiento de normativas como el RGPD y otras disposiciones sobre protección de datos, gestión de emergencias, interoperabilidad y accesibilidad digital. Cambios normativos futuros podrían requerir ajustes funcionales o estructurales del sistema.
- Disponibilidad y Confiabilidad de Sensores y “superusuarios”
    - El sistema depende de la transmisión constante y precisa de los sensores para el monitoreo en tiempo real. Errores en la trasmisión de datos por fallo o desconexión de sensores pueden afectar la generación automática de alertas.
    - Los distintos usuarios autorizados deberán realizar sus respectivas funciones fundamentales como consultar la información, analizarla y gestionar las alarmas para que el sistema funcione correctamente de cara al usuario general.
- Accesibilidad y Usabilidad
    - Disponibilidad de redes móviles y acceso a internet en zonas de riesgo para la correcta recepción de alertas, aunque se incluirá una cierta funcionalidad offline básica.
    - Compatibilidad con versiones actualizadas de navegadores y sistemas operativos móviles.
    - Para la correcta recepción de alertas, los dispositivos deben tener activadas las notificaciones, GPS y servicios de ubicación.

2.6. Requisitos Futuros

A medida que el Sistema Inteligente de Prevención y Respuesta ante Eventos Climáticos (SIPREC) evolucione, se podrán analizar e implementar mejoras que optimicen su funcionamiento, amplíen su alcance y aumenten su capacidad predictiva y de respuesta ante desastres naturales. A continuación, se presentan algunas de las mejoras y funcionalidades previstas para futuras versiones del sistema.

- Implementación de Inteligencia Artificial y Aprendizaje Automático
    - Desarrollo de modelos predictivos avanzados mediante técnicas de machine learning para mejorar la detección temprana de eventos climáticos extremos.
    - Uso de redes neuronales y modelos de series temporales para optimizar las predicciones del sistema.
    - Implementación de algoritmos de análisis de tendencias para identificar patrones climáticos anómalos.
- Integración con Dispositivos IoT y Sensores Avanzados
    - Compatibilidad con sensores inteligentes de nueva generación, incluyendo drones equipados con cámaras térmicas y radares meteorológicos.
    - Mejora en la conectividad de sensores en áreas remotas mediante redes LPWAN u otras tecnologías avanzadas.

- Expansión a otros tipos de desastres naturales y expansión del alcance
    - Extensión del sistema para la detección y monitoreo de otros desastres naturales de forma más precisa, como incendios forestales, actividad volcánica, terremotos o deslizamientos de tierra.
    - Integración con sistemas de monitoreo volcánico y sísmico para ofrecer alertas tempranas de actividad geológica.
    - Extender el alcance de uso de la aplicación para que se pueda utilizar en otros países o regiones, además de en zonas más remotas.
    - Añadir nuevos idiomas para maximizar la accesibilidad en diferentes contextos culturales.
- Mayor Personalización de Alertas y Notificaciones
    - Desarrollo de un sistema de alertas basado en IA, que personalice los avisos según el nivel de riesgo de cada usuario.
    - Implementación de canales de notificación adicionales, como integración con redes sociales, asistentes virtuales y aplicaciones de mensajería (WhatsApp, Telegram).
    - Posibilidad de configuración avanzada de umbrales de riesgo por parte de los usuarios según sus necesidades específicas.
- Visualización de Datos en Formato Avanzado, e implementación de Simulaciones y Análisis de Impacto
    - Implementación de dashboards interactivos con mapas de calor y visualización en 3D de áreas de riesgo.
    - Integración con realidad aumentada para simular escenarios de desastre y ayudar en la planificación de evacuaciones.
    - Desarrollo de herramientas de análisis geoespacial avanzado para evaluar la vulnerabilidad de infraestructuras críticas.
    - Creación de módulos de entrenamiento y capacitación en línea para mejorar la preparación de organismos de emergencia.
    - Incorporación de sistemas de apoyo a la decisión (DSS) que sugieran acciones preventivas en base a datos actuales y patrones históricos.
- Mejora en la Seguridad y Privacidad del Sistema
    - Actualización de los mecanismos de protección de datos conforme evolucionen las normativas nacionales e internacionales
    - Refuerzo de la ciberseguridad mediante mecanismos proactivos y sistemas de detección inteligente de intrusos.

3. Requisitos Específicos

3.1. Interfaces Externas

Esta sección describe los requisitos que afectan a la interacción de SIPREC con los usuarios, otros sistemas de software y hardware, así como los protocolos de comunicación.

3.1.1 Interfaz de usuario

El sistema dispondrá de dos tipos de interfaz gráfica:

- Aplicación web, accesible desde navegadores actualizados y adaptada a distintos tamaños de pantalla.
- Aplicación móvil, disponible para sistemas Android e iOS, con funcionamiento parcial en modo offline.

Las interfaces cumplirán con criterios de accesibilidad digital (según el estándar WCAG 2.1), incluyendo contraste adecuado, navegación por teclado, y compatibilidad con lectores de pantalla. Además, la IU deberá ser multilingüe (al menos en castellano e inglés) y presentar información en lenguaje claro, especialmente en situaciones críticas.

Las interfaces se adaptarán a diferentes perfiles de usuario:

- Usuarios institucionales (autoridades, gestores de emergencia, científicos) tendrán acceso a paneles de control avanzados con gestión de alertas, recursos y visualización de datos complejos. Los usuarios autorizados tendrán pantallas, mapas, elementos y opciones adicionales necesarios para cumplir sus funciones específicas
- Usuarios generales visualizarán alertas, mapas de riesgo, guías de actuación e información personalizada por ubicación; sólo se visualizará la información genérica.

La información del panel principal de la interfaz de usuario, visible para todos los usuarios, se dividirá de la siguiente forma:

- Mapa interactivo en tiempo real (componente central visual).
    - Visualización geoespacial de zonas de riesgo actuales y pronosticadas y mensajes de actuación: rutas de evacuación, puntos seguros, centros de atención o refugio….
    - Se podrán superponer capas GIS: pluviometría, temperatura, velocidad del viento, humedad del suelo, etc.
    - El usuario podrá hacer zoom y explorarlo, además de seleccionar una zona para desplegar un resumen de las alertas en esa zona
    - Se hará uso de colores intuitivos (codificación por nivel de alerta; verde, amarillo, rojo), símbolos y leyendas explicativas.
- Resumen de alertas activas
    - Se mostrará una lista con un resumen de todas las alertas activas en la zona del usuario, pudiendo éste seleccionar una para ver la información completa asociada a ese evento.
    - Habrá una opción para acceder a las recomendaciones generales de seguridad para ese evento (búsqueda automática por ese evento)
- Sección de recomendaciones generales de seguridad:
    - Muestra guías o recomendaciones breves de actuación según el tipo de evento activo o consultado: Inundaciones, incendios, tormentas, olas de calor, etc.

    - Las guías deberán utilizar un lenguaje comprensible no técnico, y estructurarse en formato instructivo con texto e iconografía de apoyo que permita una comprensión rápida por parte de la población general.
    - La sección de recomendaciones se presentará en formato de entradas temáticas consultables, organizadas por tipo de evento.
- Widget de clima
    - Visualizar temperatura, sensación térmica, humedad, precipitaciones y otros datos en tiempo real, de manera resumida y simple (no los datos obtenidos de los sensores sino valores estadísticos). Esto, además de servir simplemente para informar del clima, permite a los usuarios prepararse mejor si por ejemplo vieran que al día siguiente hay riesgo alto de lluvias continuadas, entender y visualizar de forma sencilla si las condiciones tienen previsto mejorar o empeorar…
    - Tal y como en una aplicación meteorológica común, mostrará información del tiempo en tiempo real (temperatura, humedad, precipitaciones, etc., una previsión a 7 días y un resumen histórico de la última semana
    - Los datos provendrán tanto de los propios sensores de precipitaciones, temperatura, etc, como de los servicios oficiales como AEMET con los que interoperará el sistema.

Para cada evento de alarma se mostrará el nivel de riesgo, el tipo de evento, la hora estimada de impacto y recomendaciones, además de los mensajes urgentes activos mandados por las autoridades.

3.1.2 Interfaces con otros sistemas (hardware y software)

Hardware:

- SIPREC se conectará indirectamente con redes de sensores ambientales distribuidos geográficamente. La comunicación se realizará a través de plataformas intermediarias (gateways IoT o servidores concentradores), no con los sensores individuales. Estos sensores serán de distintos tipos y recogerán distintos datos:
    - Sensores hidrológicos: niveles de agua en ríos, presas, embalses.
    - Sensores meteorológicos: precipitación, temperatura, presión atmosférica, viento.
    - Sensores de humedad del suelo y del aire.
- Los sensores estarán integrados mediante gateways IoT o servidores intermedios y se comunicarán con el sistema mediante protocolos como:
    - MQTT: para comunicaciones ligeras en tiempo real.
    - CoAP: para redes con baja capacidad.
    - HTTP REST: para sensores gestionados mediante servicios web.

La frecuencia de transmisión variará por tipo de sensor. El sistema deberá detectar interrupciones en los flujos de datos y registrar alertas por pérdida de conectividad o transmisión errónea.

Software

- SIPREC interoperará con varios sistemas mediante APIs bien definidas, seguras y documentadas. Estas interfaces permitirán la consulta, integración y actualización de datos en tiempo real o diferido. Los servicios integrados serán:
    - Servicios meteorológicos oficiales (como AEMET, ECMWF) para predicción del clima y alertas tempranas, con comunicación vía APIs REST o SOAP con autenticación segura
    - Sistemas GIS y plataformas de mapas como OpenStreetMap, Mapbox o Google Maps, con conexión a través de APIs REST y servicios de mapas web compatibles.
    - Pasarelas de mensajería para el envío de notificaciones masivas a la población, como gateways de SMS, correo electrónico y notificaciones push (SendGrid, Firebase, etc.), con integración mediante APIs HTTP, SMTP seguro o servicios especializados como SMPP.

Todos los módulos del sistema deberán utilizar interfaces bien definidas y documentadas para permitir su integración modular y futura ampliación o sustitución de componentes, de forma que los módulos del sistema sean modificables o reemplazables sin afectar la operación general del sistema.

3.1.3 Interfaces de comunicación

- Las comunicaciones entre el servidor central y los dispositivos cliente (web y móvil) se realizarán mediante protocolo HTTPS (TLS 1.3 o superior), garantizando la confidencialidad e integridad de los datos.
- La transmisión de datos desde sensores o plataformas IoT utilizará protocolos seguros y livianos como MQTT con TLS para sensores conectados mediante redes móviles o inestables, y HTTP(S) o WebSockets para entornos con conectividad más robusta o sensores gestionados por servicios web.
- El sistema deberá estar preparado para trabajar con conectividad intermitente en dispositivos móviles, sincronizando datos cuando se restablezca la conexión. La arquitectura deberá contemplar reintentos automáticos, gestión de errores y almacenamiento temporal local en caso de conectividad limitada.
- La emisión de alertas a la población se realizará a través de notificaciones push móviles, mediante servicios como Firebase Cloud Messaging, AWS SNS o equivalente, mensajes SMS, usando pasarelas SMPP o APIs de operadores, y correo electrónico, mediante servicios SMTP o plataformas como SendGrid.

Todos los canales deberán estar auditados y registrar confirmaciones de entrega o fallos.

3.2. Funciones

En esta sección se especifican todas las acciones o funciones que el SIPREC deberá considerar. Estas funciones han sido organizadas por tipos de usuario, dado que distintos actores interactúan con el sistema de manera diferente y poseen requisitos específicos. Esta organización permite una mayor claridad en la especificación de requisitos, evitando redundancias al asignar funciones específicas a cada tipo de usuario, una mejor planificación de pruebas, ya que cada función está directamente ligada a un usuario y su interacción con el sistema, y facilidad de trazabilidad, garantizando que cada usuario tenga acceso a las funciones que le corresponden según su rol.
Según lo visto en la 3.1.1, habrá ciertas funciones que son generales para todos los usuarios; las que permiten visualizar la interfaz general del sistema.

3.2.1 Funciones de la Población General

Usuarios finales que reciben alertas y recomendaciones de seguridad

ID	Función	Descripción
FU-01	Modificar idioma	Cambiar el idioma seleccionado automáticamente por otro. Como mínimo estará en español e inglés.
FU-02	Configuración de preferencias de notificación	Añadir, modificar o eliminar un email (permitir o denegar que se manden notificaciones y recomendaciones al correo)
FU-03	Recepción de alertas	Recibir notificaciones de emergencia en función de la geolocalización del dispositivo. Las notificaciones podrán ser emitidas mediante SMS, notificación push, correo electrónico (si está activado), y visualización en la aplicación. Estas alertas podrán corresponder a fenómenos climáticos o mensajes urgentes emitidos por autoridades autorizadas
FU-04	Consultar alertas activas y mensajes urgentes	Ver información sobre eventos climáticos en curso en la zona del usuario, en el mapa interactivo, permitiendo interactuar con él y seleccionar una zona concreta, y en la lista completa de alertas en la zona
FU-05	Consultar datos climáticos	Consultar el resumen meteorológico en tiempo real, presentado de forma clara y accesible para usuarios no técnicos.
FU-06	Ver recomendaciones no urgentes de seguridad	Visualizar recomendaciones o mensajes no urgentes de seguridad y medidas preventivas, permitiendo filtrar según el tipo de evento.

FU-07	Descarga de recomendaciones	Se podrá descargar en modo pdf una entrada de las recomendaciones de seguridad para uso offline.
FU-08	Reporte de incidentes	Enviar reportes sobre afectaciones en su comunidad. Se incluirá una descripción del problema, la ubicación, y opcionalmente imágenes y videos para facilitar la evaluación de los incidentes.

3.2.2 Funciones del Personal de Gestión de Emergencias

Estos usuarios incluyen Protección Civil, bomberos y agencias de respuesta ante desastres. Necesitan acceso a herramientas de monitoreo, alerta y coordinación de emergencias.

ID	Función	Descripción
FE-01	Autenticación segura	Iniciar sesión como usuario autorizado mediante credenciales seguras
FE-02	Visualización del estado actual de emergencias	Visualizar en tiempo real los eventos climáticos/alertas activas que afectan a su jurisdicción. Esto será una adición a la visualización de alertas de la interfaz general (en lugar de mostrar la zona del gps del usuario, se mostrará su área de cobertura)
FE-03	Recepción de alertas geolocalizadas	Recibir notificaciones cuando se active una alerta en una zona bajo su jurisdicción o cobertura. De nuevo, esto es una modificación a la función de “recepción de alertas” en la zona gps, siendo ahora la zona bajo su jurisdicción.
FE-04	Visualización y gestión de reportes ciudadanos	Los usuarios de emergencias podrán visualizar los reportes de usuarios generales que afecten a su área de cobertura para decidir cómo actuar en respuesta. Los reportes se mostrarán junto al estado actual del reporte, que podrá ser modificado por los equipos de emergencias, para mejorar la sincronización entre equipos. Los estados podrán ser: -Esperando atención: estado inicial por defecto -Atención en curso: un equipo ha confirmado que está actuando sobre el reporte -Atendido: la intervención ha finalizado -Rechazado: Se ha considerado que no es relevante (reporte duplicado, enviado por error…)
FE-05	Recepción de instrucciones operativas	Recibir órdenes o recomendaciones de actuación emitidas por las autoridades para un determinado evento.

FE-06	Administrar jurisdicciones	Añadir una nueva zona bajo la jurisdicción del equipo de emergencias concreto a la que prestará sus servicios, o dejar de prestar servicio a una zona concreta.
FE-07	Acceso a detalles técnicos de una alerta	Consultar información detallada de cada alerta, incluyendo datos adicionales no visibles para el usuario general como variables desencadenantes (ej. nivel del río, precipitación), probabilidad de evolución o agravamiento del evento o infraestructuras críticas en la zona (carreteras, presas, hospitales).
FE-08	Proponer modificaciones en las recomendaciones de actuación	Proponer nuevas recomendaciones de actuación ante un cierto evento, os eliminar o modificar entradas ya existentes (en la ventana de recomendaciones generales). Estas propuestas serán gestionadas por las autoridades gubernamentales o municipales correspondientes.
FE-09	Registro de actuaciones en campo	Registrar acciones llevadas a cabo (ej. rescates, evacuaciones, cierres de carreteras) para un cierto evento. Se podrá enviar un reporte breve de la actuación a las autoridades
FE-10	Envío de avisos a los usuarios generales	Avisar a los usuarios generales de las actuaciones en campo de una cierta zona (ej. si hay alguna carretera cortada o alguna evacuación). Estos avisos se enviarán en tiempo real, mostrándose de la misma manera que una alarma por evento climático, y sin necesidad de ser verificados por las autoridades, ya que son especialmente críticos.
FE-11	Actualización del estado de una zona	Marcar zonas como “Atendidas”, “Evacuadas”, “Sin acceso” o “En evaluación” para su seguimiento por otros equipos o autoridades.
FE-12	Consulta de históricos de actuación	Consultar eventos de alerta pasados, con detalles de acciones realizadas por el servicio, tiempos de respuesta y zonas afectadas.

3.2.3 Funciones de Centros Meteorológicos y Científicos

Organismos especializados en la predicción del clima y el monitoreo de variables hidrológicas. Además de las funciones generales relacionadas con la visualización de la interfaz general del sistema, se añadirán las siguientes:

ID	Función	Descripción

FC-01	Autenticación segura	Iniciar sesión como usuario autorizado del tipo científico o analista meteorológico con credenciales seguras .
FC-02	Acceso a datos completos en tiempo real	Visualizar en tiempo real la información completa de los datos recopilados por el sistema. Se podrá realizar un filtrado por zona concreta, tipo de sensor…
FC-03	Descarga de datasets	El sistema deberá permitir exportar datos en formatos estándar (CSV, JSON, XLSX) para su análisis offline mediante herramientas externas (R, Python, MATLAB...).
FC-04	Subida de resultados	Si se realizan análisis con herramientas externas, como estadísticas o informes para las autoridades, estos resultados se podrán subir al sistema.
FC-05	Integración con modelos climáticos	El sistema deberá permitir integrar o cargar modelos de predicción desarrollados por los científicos con los que se harán las predicciones. Estos modelos son algoritmos o simulaciones matemáticas que predicen cómo evolucionará una condición climática o ambiental a partir de los datos actuales e históricos.
FC-06	Ajustar parámetros de modelos	Se deberían poder actualizar y modificar ciertos parámetros de los modelos subidos para optimizar de manera rápida y sencilla las detecciones y predicciones del sistema, sin tener que subir un modelo completamente nuevo.
FC-07	Configuración de umbrales de riesgo	El sistema deberá permitir modificar los umbrales críticos de variables que generan alertas automáticas.
FC-08	Gestión manual de alertas	Proponer revisiones de alertas activas para añadir observaciones técnicas, modificarlas o eliminarlas si fuera necesario (por ejemplo si es un falso positivo). También, si los expertos detectan alguna situación crítica que no haya sido detectada de forma automática, podrán proponer alarmas manualmente.
FC-09	Añadir observaciones y recomendaciones	Proponer observaciones o recomendaciones técnicas (ej. “posible crecida anticipada en zona sur”). Estas recomendaciones se enviarán directamente a las autoridades gubernamentales de la zona asociada, que las gestionarán como crean necesario.
FC-10	Análisis de datos	Comparar ciertos datos climáticos históricos (un cierto rango de fechas) con algún modelo subido a la plataforma para evaluar el comportamiento del modelo, comparar modelos o extraer patrones y correlaciones

FC-11	Acceso a históricos de datos completos	Consultar los registros históricos con los datos detallados de un rango de fechas, con opción de filtrado por zona concreta geográfica, tipo de sensor…

3.2.4 Funciones de Autoridades Gubernamentales y Municipales

Incluye alcaldías, gobiernos locales y departamentos de planificación territorial. Su interés es la prevención y mitigación de desastres. Además de las funciones generales relacionadas con la visualización de la interfaz general del sistema, se añadirán las siguientes:

ID	Función	Descripción
FG-01	Iniciar sesión	Acceder con credenciales oficiales como autoridad gubernamental o municipal.
FG-02	Visualización de estado en tiempo real	En el mapa interactivo, se mostrarán todas las zonas bajo la jurisdicción de la institución en lugar de en la zona gps, mostrando como información adicional el estado y reportes de los servicios de emergencia asociados a cada evento.
FG-03	Coordinación con servicios de emergencia	Consultar la situación operativa de los cuerpos de emergencia, enviar instrucciones directas a un equipo concreto que trabaje bajo la jurisdicción de la autoridad, y definir o activar protocolos para todos los equipos de la jurisdicción (por ejemplo: “priorizar evacuación en barrio X”).
FG-04	Revisión y validación de alertas	Revisar alertas manualmente (tanto climáticas como mensajes urgentes generados por las propias autoridades) y modificarlas o cancelarlas si procede. Además, se podrán aceptar o descartar propuestas hechas por los centros climáticos sobre las alertas (aceptar que estos creen nuevas alertas o modifiquen o eliminen alguna existente).
FG-05	Gestionar mensajes urgentes	Gestionar las recomendaciones o mensajes asociados a un cierto evento. Estas observaciones pueden provenir de propuestas de los centros meteorológicos o los servicios de emergencia. Podrán ser aceptadas y añadidas al evento asociado si se considerase necesario, o directamente descartadas. Además, la propia autoridad podrá añadir o eliminar una observación de un evento concreto.

FG-06	Comunicación con ciudadanos	Enviar mensajes o avisos urgentes (alertas de actuación) a la población en riesgo (como zonas de refugio, infraestructuras dañadas, protocolos de actuación…). Estos mensajes se mostrarán de la misma manera que una alarma por evento climático.
FG-07	Gestión de zonas y jurisdicciones	Gestionar el territorio bajo su responsabilidad, incluyendo: -División de los servicios de emergencia por distritos, barrios o zonas (incluyendo añadir o eliminar zonas bajo la jurisdicción de cada uno) -Asociación de sensores por región
FG-08	Administración de permisos	Gestionar cuentas de todos los demás usuarios del sistema. Incluye crear credenciales institucionales para usuarios autorizados nuevos del sistema.
FG-09	Consultar datos históricos	Obtener estadísticas de eventos meteorológicos pasados con sus respectivas actuaciones. Estos eventos se podrán filtrar por fecha, nivel de alerta o tipo de evento.
FG-10	Acceso a informes técnicos	El sistema deberá permitir visualizar y descargar informes y estadísticas generadas por servicios de emergencia y científicos. Se podrán filtrar por rango de fechas, tipo de reporte, entidad que lo ha emitido, reportes relativos a un cierto evento…
FG-11	Publicar información para la ciudadanía	Subir comunicados no urgentes al apartado de “recomendaciones generales”, sobre medidas preventivas u otras recomendaciones de seguridad asociados a un tipo de evento. También se aceptarán o denegarán propuestas de recomendaciones enviadas por los usuarios de emergencias.

3.3 Requisitos de Rendimiento

Esta sección detalla los requisitos de rendimiento del Sistema Inteligente de Prevención y Respuesta ante Eventos Climáticos (SIPREC), incluyendo capacidad de usuarios simultáneos, transacciones por segundo, almacenamiento de datos y velocidad de respuesta.

3.3.1 Carga Esperada del Sistema

ID	Parámetro	Descripción
CE-01	Usuarios simultáneos	El sistema debe estar preparado para atender un mínimo de 200.000 usuarios conectados, con posibilidad de escalar a mayor capacidad en caso de expansión regional o nacional.

CE-02	Transacciones por segundo (TPS)	El sistema debe poder manejar picos de hasta 500 transacciones por segundo, incluyendo lecturas de sensores, generación de alertas, acceso a mapas y envío de notificaciones.
CE-03	Capacidad de recepción de datos	El sistema debe ser capaz de recibir, validar y almacenar datos de más de 10.000 sensores simultáneamente activos, distribuidos en distintas regiones geográficas.

3.3.2 Tiempo de Respuesta

ID	Parámetro	Descripción
TE-01	Carga del dashboard principal	El usuario debe poder visualizar información en menos de 10 segundos.
TE-02	Generación de alertas	El sistema debe emitir alertas en menos de 10 segundos después de detectar una amenaza.
TE-03	Descarga de reportes	Un informe detallado debe estar disponible en menos de 20 segundos.

3.3.3 Requisitos de Almacenamiento de Datos

ID	Función	Descripción
RE-01	Datos climáticos	El sistema almacenará datos históricos climáticos por un período mínimo de 5 años, si fuese posible al menos 10, con acceso rápido a registros recientes (últimos 30 días) y recuperación diferida para periodos anteriores. Se estima que la base de datos almacenará más de 500 millones de registros de sensores al año, considerando actualizaciones cada pocos minutos por sensor.
RE-02	Historial de alertas	Se guardarán las alerta, reportes y recomendaciones hechas, asociadas a un cierto evento, por un periodo mínimo de 5 años.
RE-03	Registros de auditoría	Todos los registros de auditoría se guardarán por al menos 2 años, al menos 5 si fuese posible.

3.3.4 Escalabilidad y Disponibilidad

ID	Parámetro	Requerimiento
ED-01	Escalabilidad	El sistema deberá ser escalable horizontalmente y deberá ser capaz de soportar un incremento del 100% en el número de usuarios simultáneos y en la frecuencia de eventos procesados sin que se degrade el rendimiento del sistema, manteniendo los tiempos de respuesta definidos.
ED-02	Disponibilidad	El sistema deberá garantizar una disponibilidad mínima aproximada del 99,5% anual, con un máximo de 8,76 horas de inactividad no planificada por año, excluyendo mantenimientos programados.
ED-03	Redundancia	El sistema deberá estar desplegado en infraestructura con servidores redundantes ubicados en al menos tres regiones geográficas distintas, a fin de asegurar continuidad operativa, resiliencia ante desastres y balanceo de carga geográfico.
ED-04	Recuperación ante fallos	En caso de fallo crítico, el sistema deberá contar con un mecanismo automático de recuperación que permita restaurar el servicio en un tiempo inferior a 10 minutos, sin pérdida de datos críticos.

3.4 Restricciones de Diseño

Esta sección describe las limitaciones y restricciones que deben considerarse en el diseño del SIPREC. Estas restricciones pueden deberse a estándares tecnológicos, hardware disponible y normativas vigentes.

3.4.1 Restricciones Tecnológicas

ID	Restricción	Descripción
TR-01	Compatibilidad con plataformas	La aplicación web debe ser accesible en navegadores modernos (Chrome, Firefox, Edge) y en dispositivos móviles de gama media o baja, con procesadores limitados, 2 GB de RAM y sistemas operativos con versiones mínimas Android 8.0 y iOS 13.
TR-02	Lenguajes de programación	El backend debe estar desarrollado en Python (FastAPI) o Node.js, mientras que el frontend

		utilizará React o Angular.
TR-03	Base de datos	Se utilizará un sistema de gestión de bases de datos relacional (PostgreSQL) como repositorio principal de datos estructurados, y un sistema de almacenamiento no relacional (MongoDB) para almacenamiento de eventos en tiempo real
TR-04	Integración con sistemas externos	Según lo visto en apartados anteriores, el sistema debe poder interoperar con varios sistemas externos
TR-05	Tolerancia a fallos	Se requiere infraestructura de microservicios y balanceo de carga para evitar colapsos del sistema en momentos críticos.
TR-06	Gestión de restricciones en los sensores	El diseño debe tener en cuenta que los sensores IoT pueden tener restricciones de conectividad, alimentación y frecuencia de muestreo, por lo que el sistema debe tolerar latencias, pérdidas de señal o datos faltantes.

3.4.2 Otras restricciones

ID	Restricción	Descripción
OR-01	Modo off-line	El sistema debe diseñarse para operar en entornos con baja o intermitente conectividad, permitiendo sincronización diferida y uso offline en las aplicaciones móviles.
OR-02	Normalización de la base de datos	La base de datos del sistema debe estar normalizada (al menos hasta 3FN) para asegurar integridad y evitar redundancia de datos, pero podrá incorporar mecanismos de de normalización en vistas o réplicas para consultas de alto volumen.

3.4.2 Cumplimiento normativo y estándares aplicables

El sistema desarrollado deberá cumplir al menos los siguientes estándares y reglamentos:

ID	Normativa/Estándar	Descripción
CE-01	ISO 27001	Seguridad de la información y protección de datos.
CE-02	ISO 27017	Seguridad en servicios en la nube: directrices para

		proveedores y clientes de servicios cloud.
CE-03	GDPR (Reglamento Europeo de Protección de Datos)	Protección de datos personales de los usuarios europeos.
CE-04	ISO 22320	Gestión de emergencias y resiliencia en crisis.
CE-05	ISO 19115	Estándar para metadatos geoespaciales: esencial si trabajas con mapas, zonas de riesgo y capas GIS.
CE-06	ISO 25010	Calidad del software y atributos del sistema.
CE-07	WCAG 2.1 Nivel AA	La interfaz, según el RD 1112/2018, debe cumplir al menos con el estándar WCAG 2.1 Nivel AA, garantizando acceso a personas con discapacidad visual, auditiva o motriz.
CE-08	RD 1112/2018	Normativa nacional sobre accesibilidad en servicios digitales del sector público.
CE-09	EN 301 549	Requisito obligatorio en la UE para la accesibilidad en TIC, tanto en web como en apps móviles.
CE-10	OWASP Top 10	Buenas prácticas para prevenir las vulnerabilidades más comunes en aplicaciones web y móviles (inyección, XSS, etc.).
CE-11	TLS 1.3 o superior	Estándar para cifrado seguro de comunicaciones. Requisito mínimo para transmisión de datos confidenciales.

3.5 Atributos del Sistema

Esta sección detalla los atributos de calidad, mantenibilidad, seguridad y escalabilidad del sistema SIPREC

3.5.1 Fiabilidad

ID	Requisito	Descripción
AF-01	Recuperación ante desastres	La arquitectura deberá prever un plan de contingencia y recuperación ante fallos (disaster recovery) que incluya replicación de datos, recuperación automatizada y pruebas periódicas del sistema.

AF-02	Tolerancia a fallos	El sistema deberá garantizar tolerancia a fallos, asegurando que ante fallos de componentes individuales (sensores, nodos, microservicios), el sistema global siga operativo.

3.5.1 Mantenibilidad

ID	Requisito	Descripción
AM-01	Modularidad	El sistema deberá estar desarrollado con una arquitectura modular y buenas prácticas de codificación, para facilitar la identificación y corrección de errores
AM-02	Microservicios	El sistema deberá implementarse bajo una arquitectura basada en microservicios, permitiendo la actualización, mantenimiento y despliegue de módulos individuales (por ejemplo, alertas, sensores, reportes) sin afectar la disponibilidad ni el funcionamiento del resto del sistema.
AM-03	Modificación de configuraciones	Las configuraciones clave (umbrales de alerta, parámetros regionales, acceso de usuarios) deberán poder modificarse sin necesidad de recompilar el sistema.
AM-04	Código limpio y documentado	Uso de herramientas como Swagger para APIs y estándares de documentación (Doxygen, JSDoc).
AM-05	Pruebas automatizadas	Implementación de pruebas unitarias, de integración y de carga en cada actualización.
AM-06	Logs de eventos	Registro detallado de todas las acciones en el sistema para auditoría y depuración.

3.5.2 Portabilidad

ID	Requisito	Descripción
AP-01	Compatibilidad con sistemas operativos	La base de código deberá ser multiplataforma, con clientes móviles disponibles para Android (versión 8.0 o superior) e iOS (versión 13 o superior), y una interfaz web compatible con los principales navegadores, Windows, MAC y Linux (Ubuntu, CentOS, Debian).
AP-02	Despliegue en la nube	Compatible con AWS, Azure y Google Cloud para garantizar flexibilidad en la infraestructura.
AP-03	Accesibilidad	Interfaces optimizadas para navegadores web y aplicaciones

	desde cualquier dispositivo	móviles Android/iOS.

3.5.3 Protección de datos

ID	Requisito	Descripción
PD-01	Defensa contra ataques	Implementación de firewalls, detección de intrusos (IDS/IPS) y protección contra ataques comunes como inyección, CSRF, XSS o DDoS.
PD-02	Encriptación de la información	Toda la comunicación deberá estar encriptada, incluyendo la recepción de los datos de los sensores. Se debe usar cifrado simétrico AES-256 en la base de datos y TLS 1.3 o superior en todas las comunicaciones.
PD-03	Compartir datos personales	Los datos personales no podrán compartirse con terceros ni utilizarse para fines distintos a los de los objetivos del sistema.
PD-04	Librerías y dependencias	Se utilizarán librerías y dependencias actualizadas, evitando vulnerabilidades conocidas
PD-05	Cifrado de las claves	Las claves de acceso, tokens de sesión y credenciales no deberán almacenarse nunca en texto plano ni en el frontend. Deberán mantenerse en almacenamiento cifrado y gestionado de forma segura.
PD-06	Copias de seguridad automáticas	SIPREC deberá generar respaldos de la base de datos al menos diariamente, con retención de versiones anteriores durante al menos 30 días

3.5.4 Autenticación y control de acceso

ID	Requisito	Descripción
CA-01	Doble factor de autenticación	Los usuarios institucionales (autoridades, centros meteorológicos, personal de emergencia) deberán autenticarse mediante doble factor de autenticación (2FA), utilizando aplicaciones móviles de verificación o tokens físicos.

CA-02	Control de accesos	Solo los usuarios autorizados pueden acceder a datos sensibles y modificar configuraciones.
CA-03	RBAC	El sistema deberá implementar un modelo de control de acceso basado en roles (RBAC), que limite el acceso a funcionalidades y datos según el perfil del usuario.
CA-04	Tiempo de sesión	Las sesiones deberán expirar tras un periodo de inactividad configurable (por defecto, 15 minutos), en cumplimiento con la política de seguridad del sistema

3.5.5 Control de Permisos por Tipo de Usuario

Para garantizar la seguridad operativa del sistema, se debe restringir el acceso a determinadas funcionalidades según el perfil del usuario autenticado. A continuación se especifican algunos de los permisos fundamentales:

- Autoridades Gubernamentales y Municipales
    - Autorizados a: verificar mensajes y alertas antes de ser puestos al público, gestionar alertas, gestionar permisos de otros usuarios institucionales, visualizar y coordinar recursos, generar informes estratégicos.
    - Restringidos de: modificar algoritmos internos de predicción o acceder a configuraciones técnicas del sistema base.

- Centros Meteorológicos y Científicos
    - Autorizados a: acceder y exportar datos crudos, ajustar y añadir modelos predictivos, consultar históricos completos, y proponer un cambio relacionado con la gestión de alertas y recomendaciones.
    - Restringidos de: enviar mensajes públicos (crear o eliminar alertas, subir recomendaciones…) sin confirmación de una autoridad, quienes tendrán que aceptar primero la propuesta, o gestionar recursos operativos.

- Personal de Gestión de Emergencias
    - Autorizados a: recibir alertas, visualizar mapas operativos, registrar incidencias de campo, proponer recomendaciones de actuación, enviar alertas urgentes de protocolos de actuación.
    - Restringidos de: modificar configuraciones globales del sistema o emitir recomendaciones sin validación previa.

- Usuarios Generales

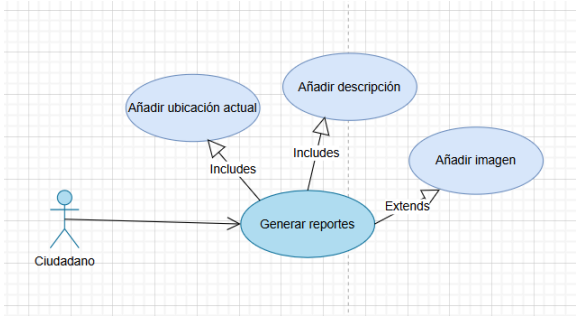
- Autorizados a: recibir alertas, consultar información pública, enviar reportes, acceder a guías de actuación y recomendaciones, tanto urgentes como generales.
- Restringidos de: acceder a datos sensibles, manipular configuraciones o consultar información operativa interna.

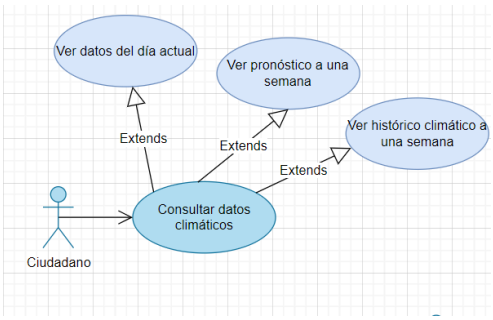
La información detallada de las funciones que puede realizar cada usuario se detalla en el punto 3.2

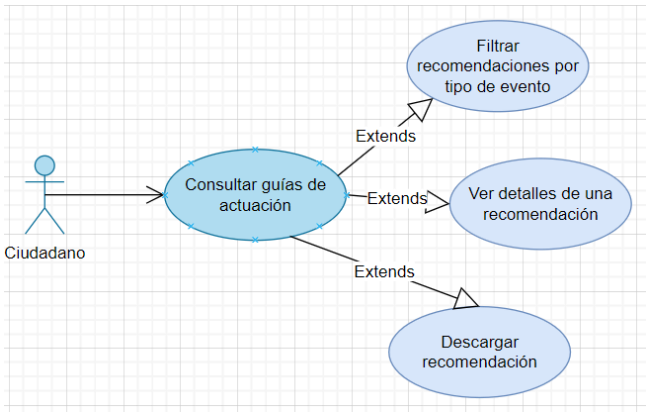
4. DIAGRAMAS DE CASOS DE USO

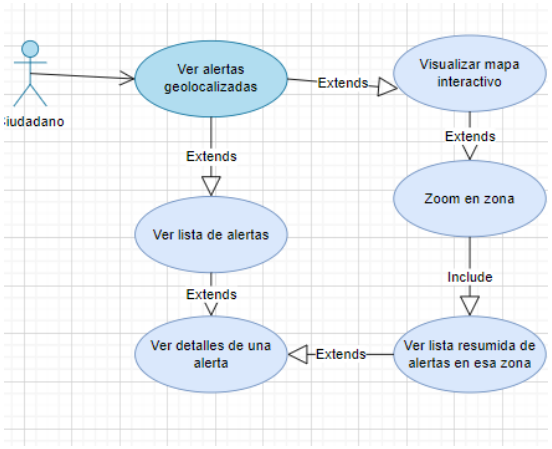
A continuación, se pueden consultar los diagramas de casos de uso de cada actor. En él, se representan las acciones que puede realizar cada tipo de usuario en la aplicación de una manera visual. Para los usuarios verificados solamente se añadieron las funciones que tienen diferencias respecto a las de los usuarios generales, pero hay que tener en cuenta que además de estas funciones, podrán utilizar todas las funciones básicas de la interfaz principal al igual que cualquier ciudadano.

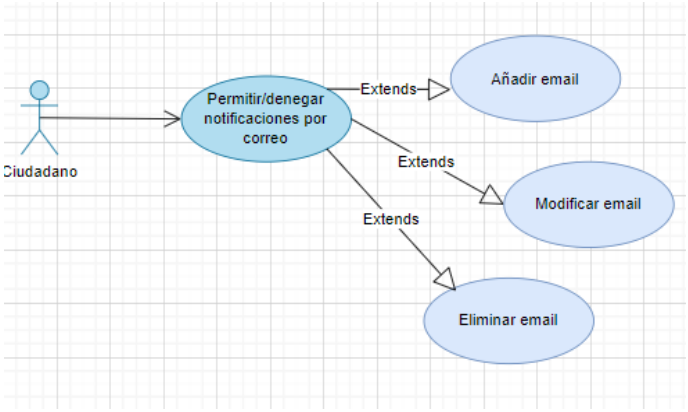
4.1 Ciudadanos

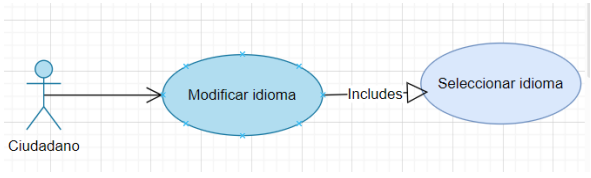




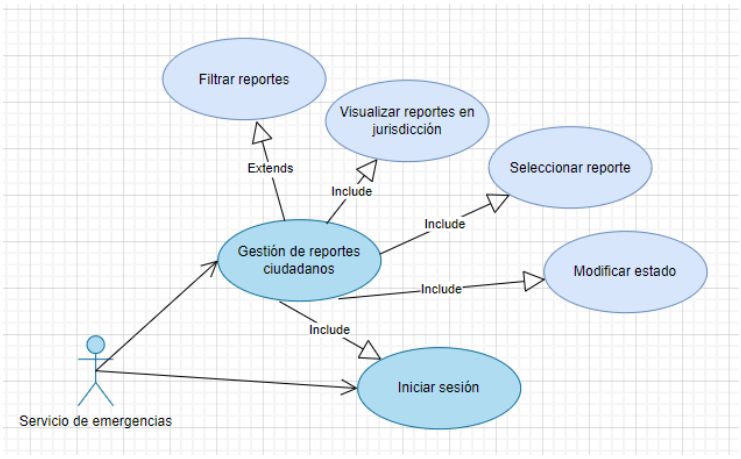


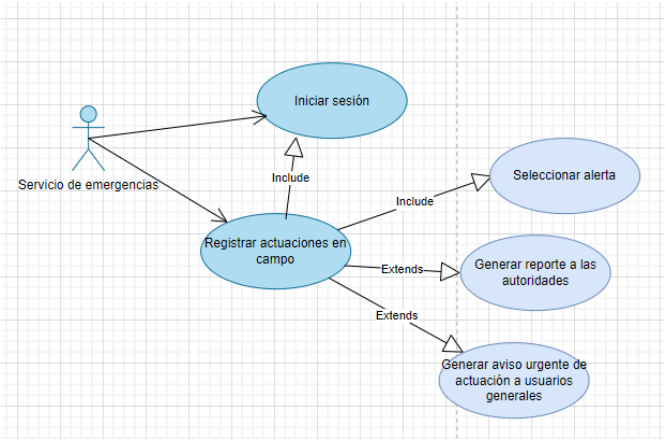


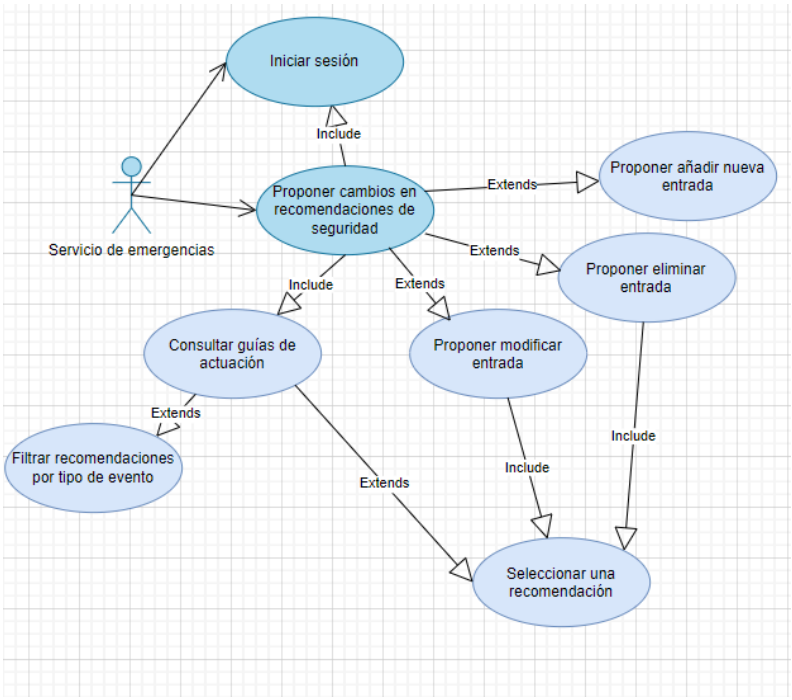


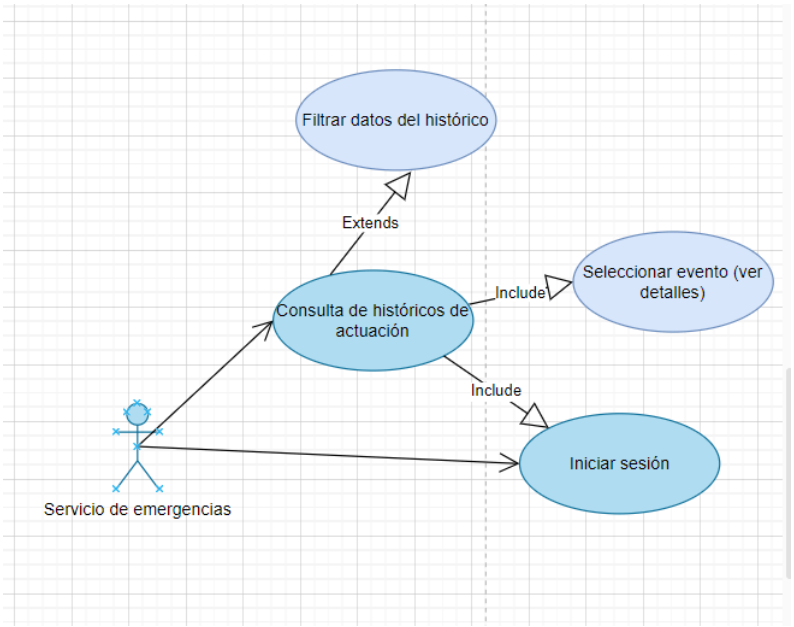


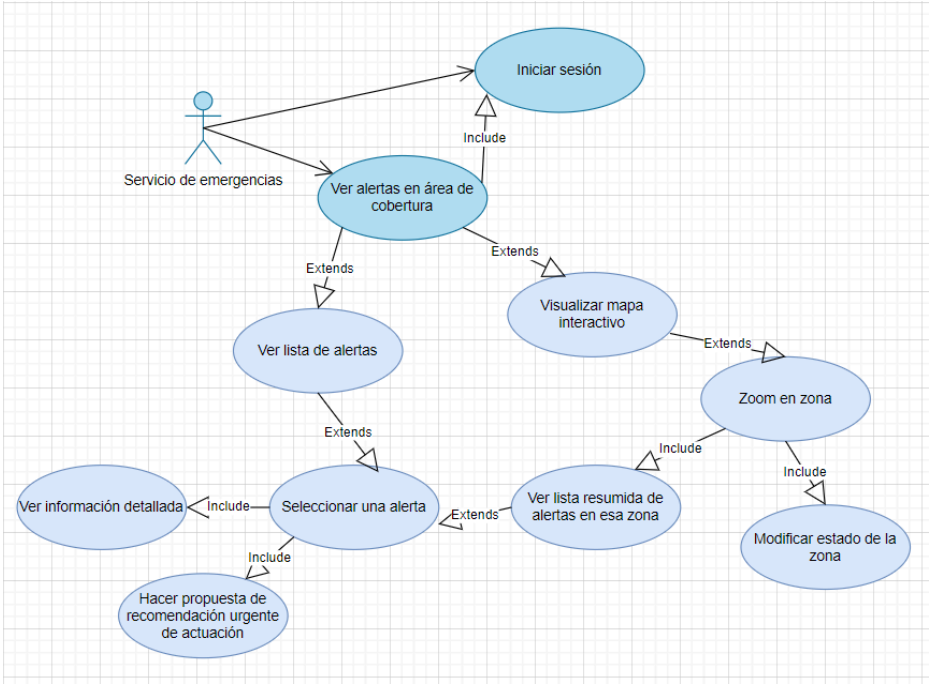
4.2 Servicios de emergencia



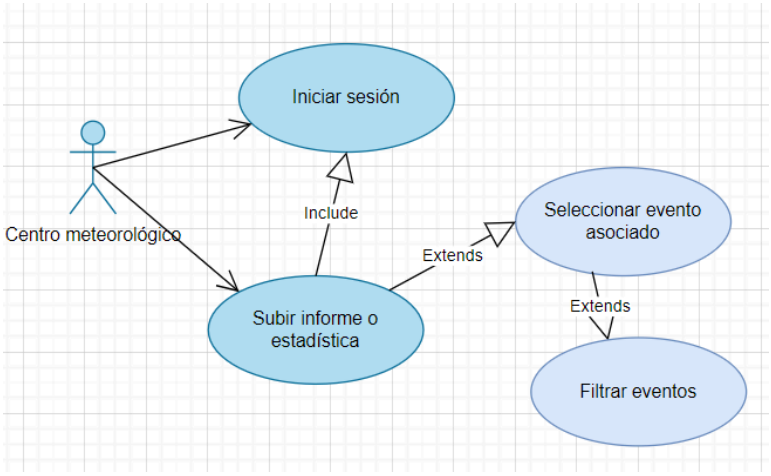


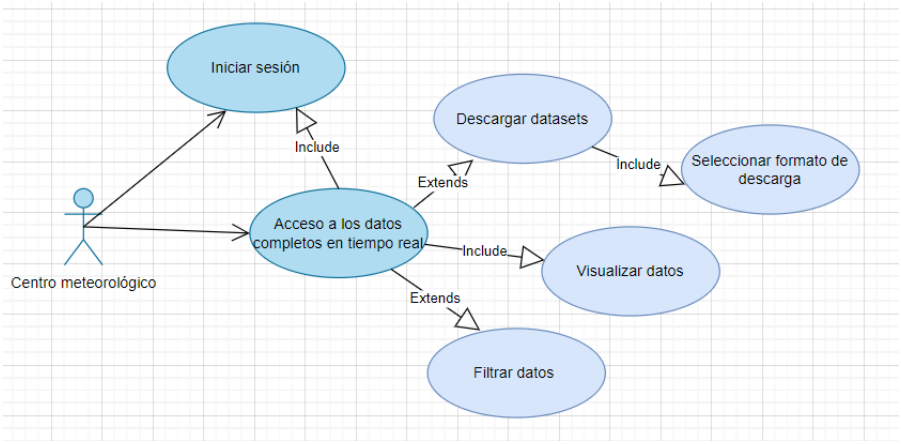


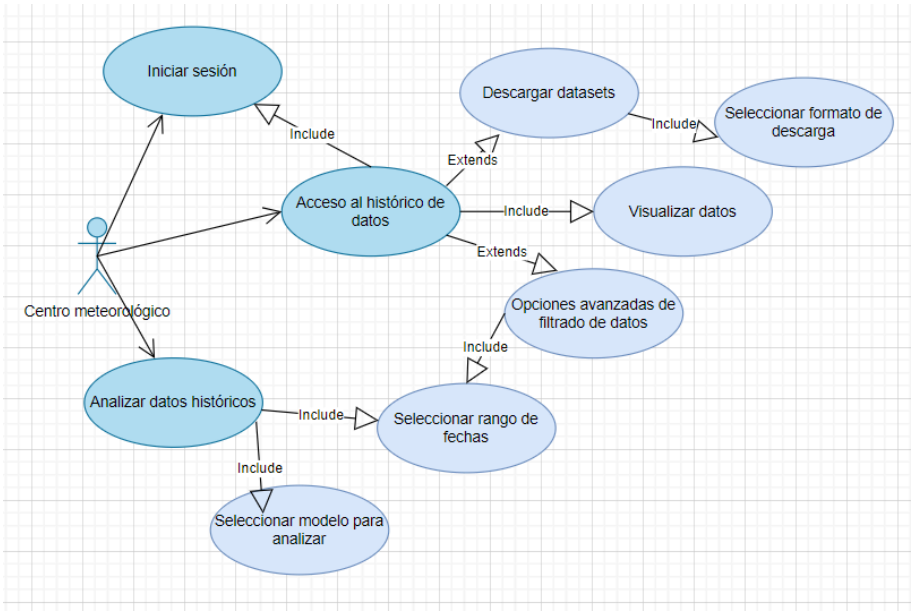

Filtrar datos del histórico
Extends
Consulta de históricos de actuación
Include
Seleccionar evento (ver detalles)
Include
Iniciar sesión
Servicio de emergencias

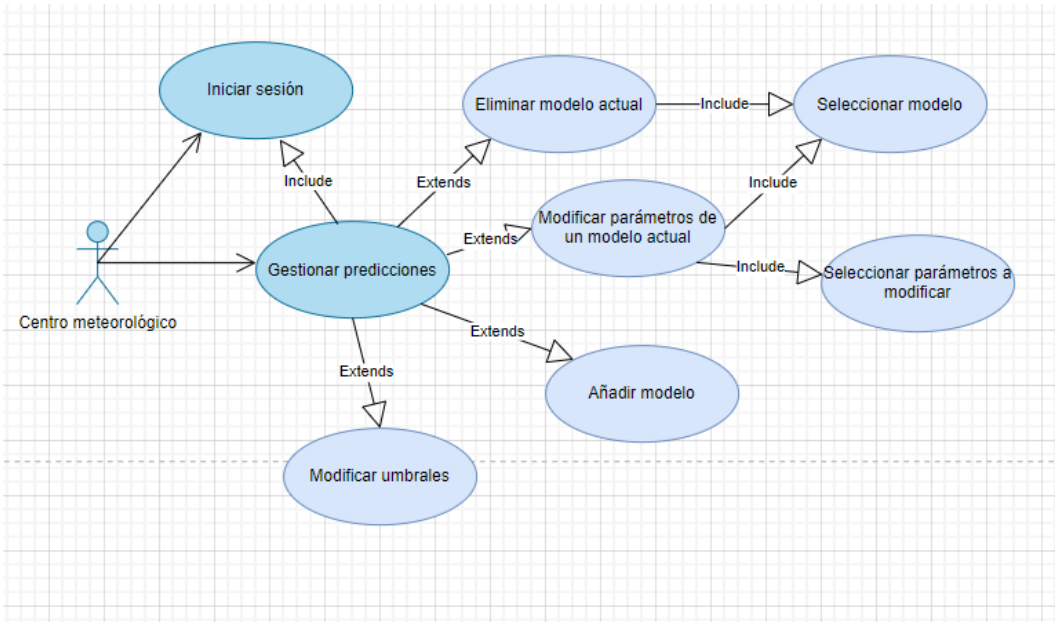

Iniciar sesión
Include
Servicio de emergencias
Ver alertas en área de cobertura
Extends
Extends
Visualizar mapa interactivo
Ver lista de alertas
Extends
Zoom en zona
Extends
Include
Include
Ver información detallada
Include
Seleccionar una alerta
Extends
Ver lista resumida de alertas en esa zona
Modificar estado de la zona
Include
Hacer propuesta de recomendación urgente de actuación

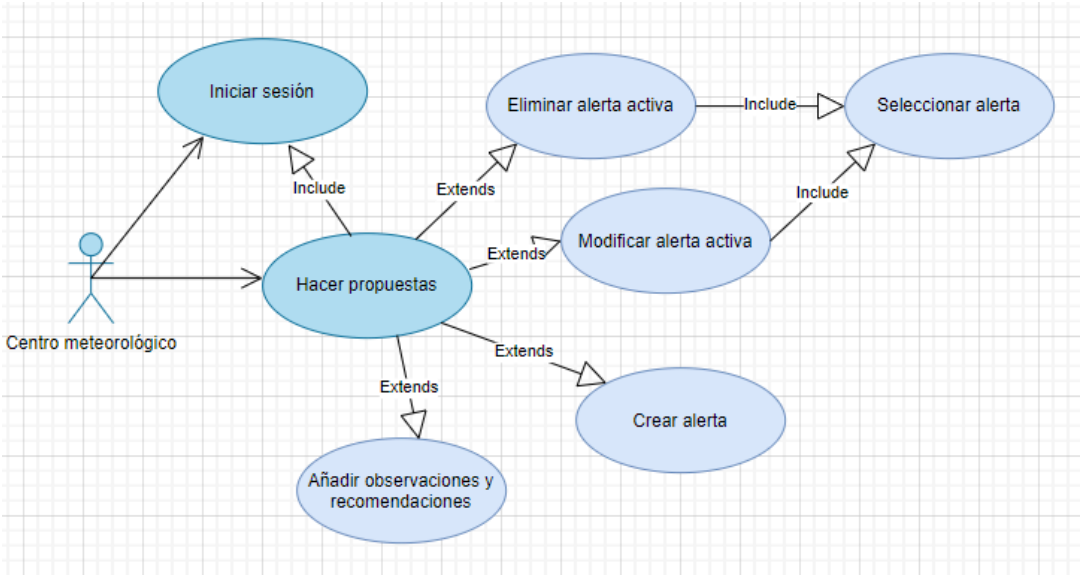
4.3 Centros meteorológicos



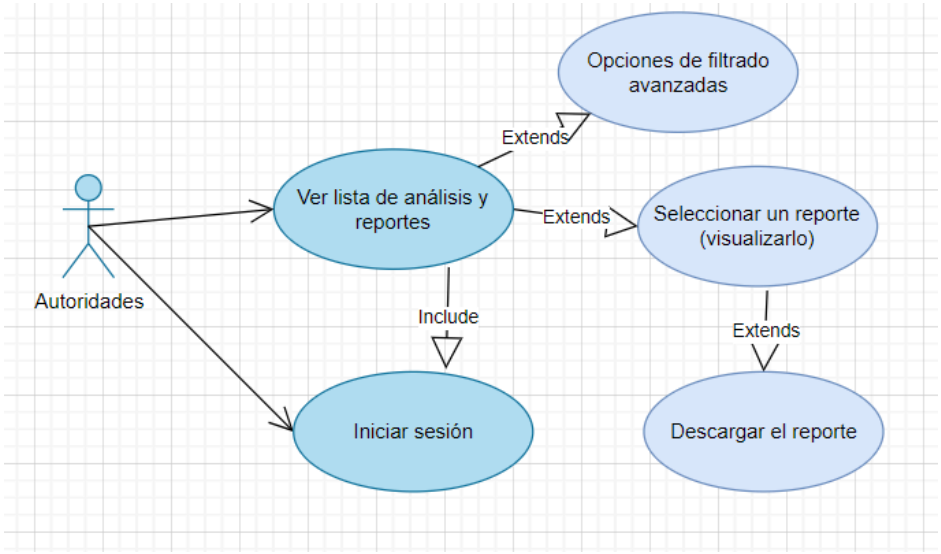


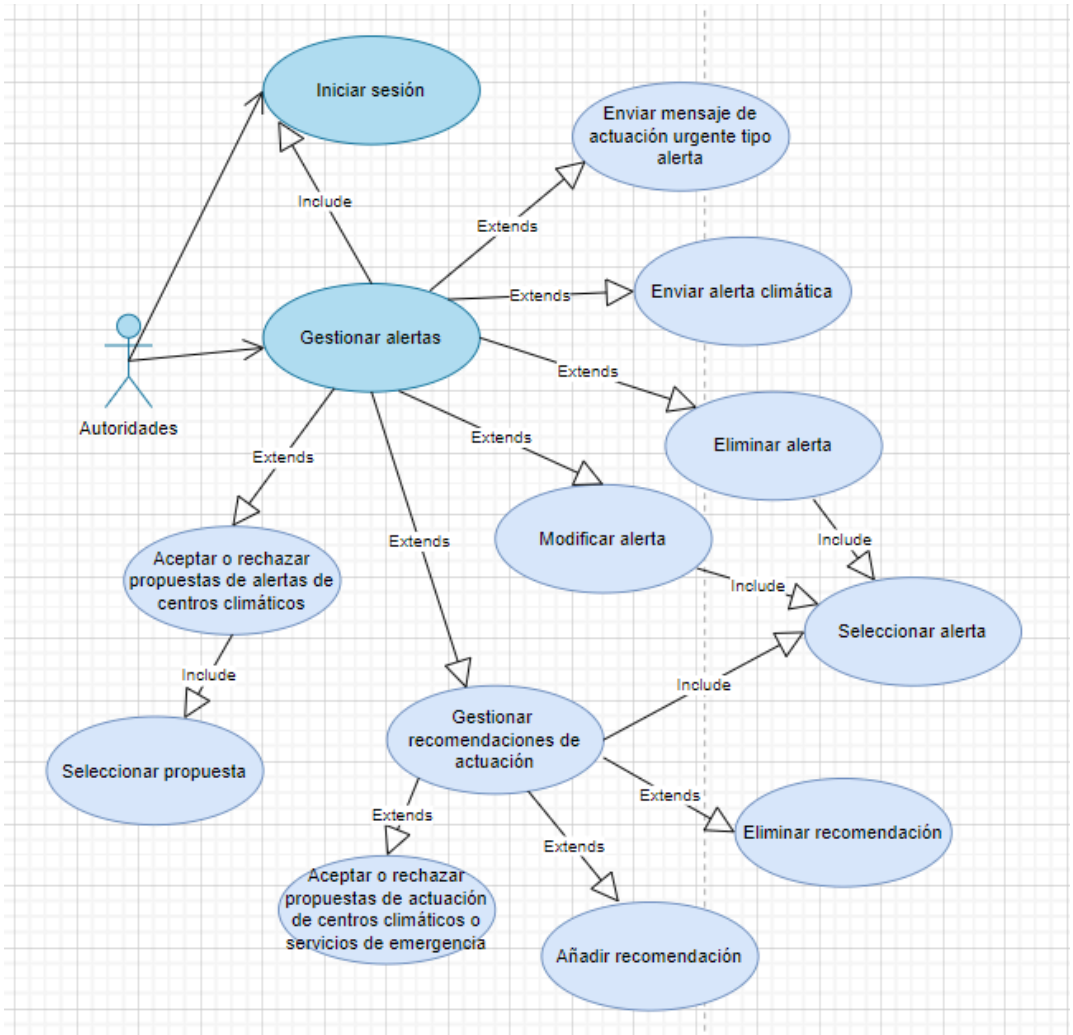


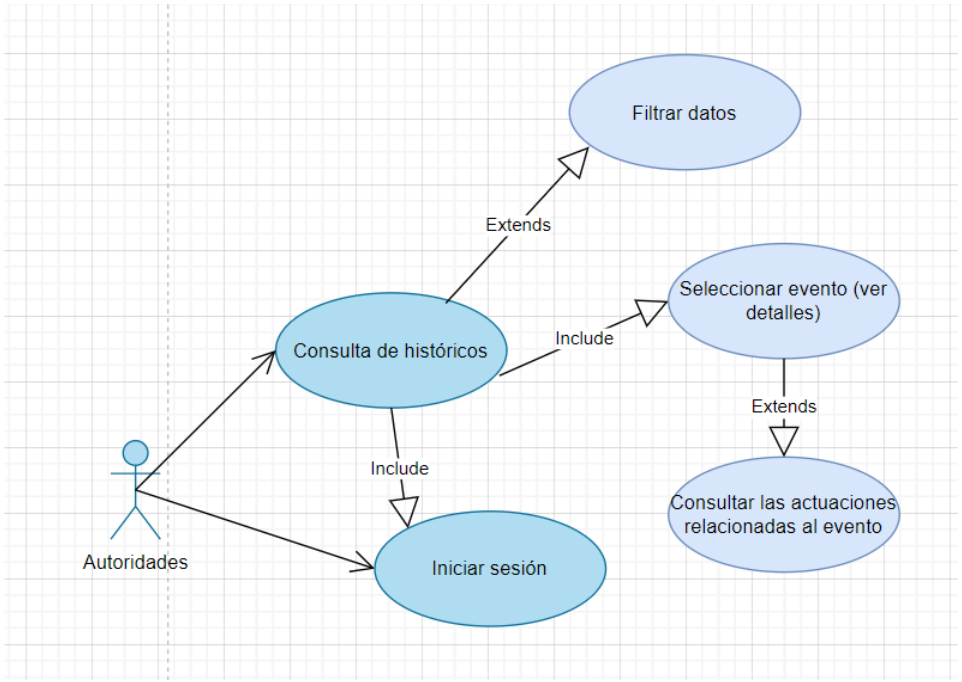

Iniciar sesión
Eliminar modelo actual
Include
Seleccionar modelo
Include
Extends
Include
Extends
Modificar parámetros de un modelo actual
Centro meteorológico
Gestionar predicciones
Include
Seleccionar parámetros a modificar
Extends
Extends
Añadir modelo
Extends
Modificar umbrales

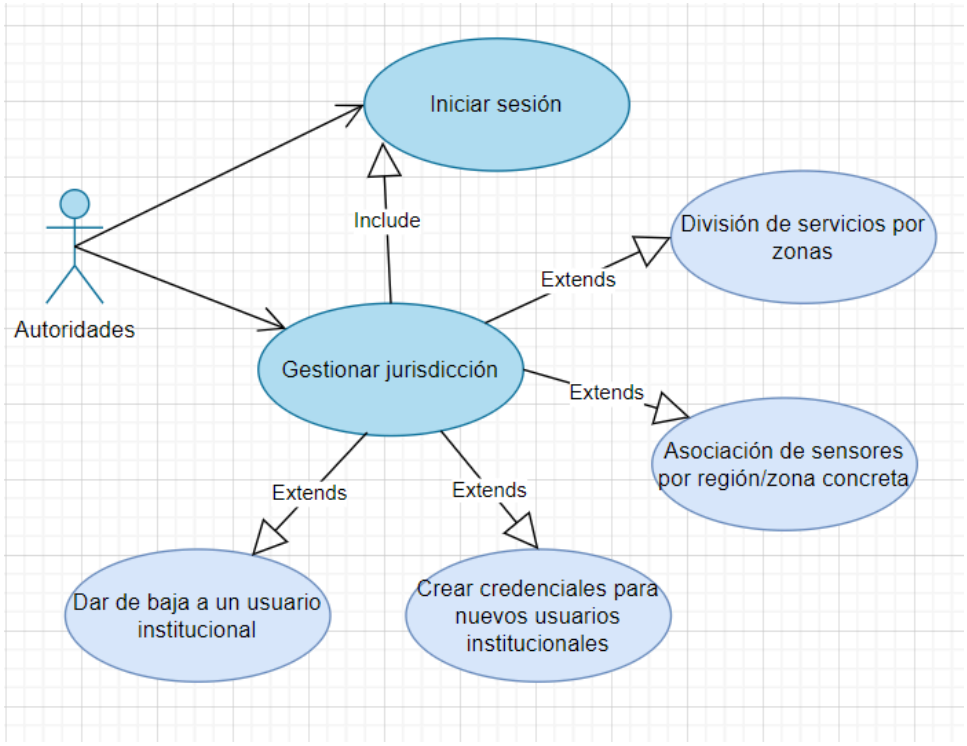

Iniciar sesión
Eliminar alerta activa
Include
Seleccionar alerta
Include
Extends
Include
Extends
Modificar alerta activa
Centro meteorológico
Hacer propuestas
Extends
Extends
Crear alerta
Extends
Añadir observaciones y recomendaciones

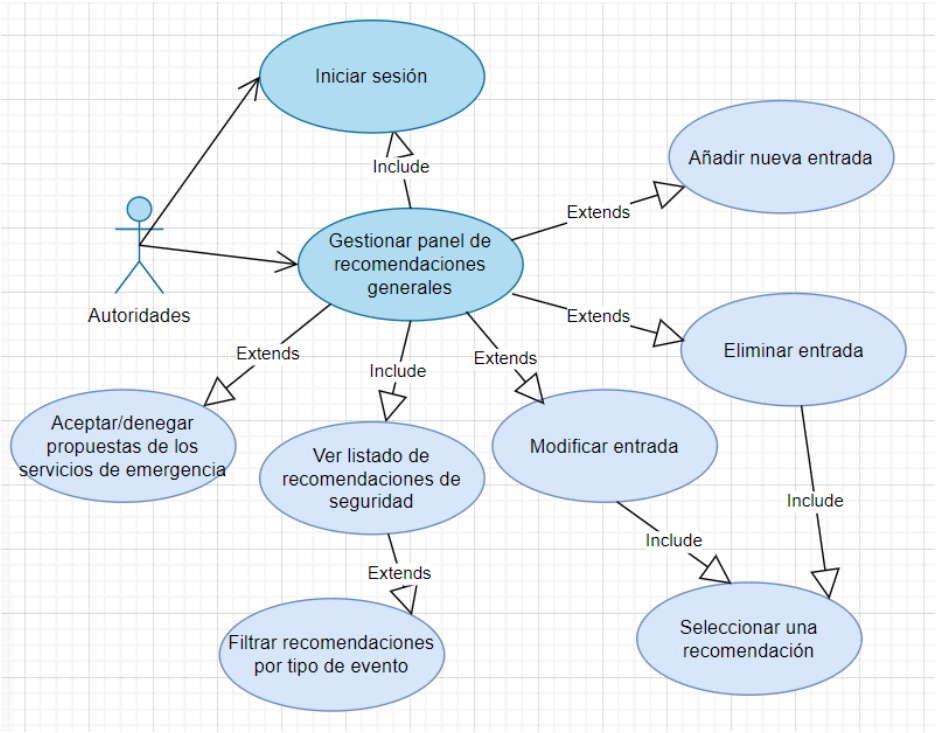
4.4. Autoridades municipales y gubernamentales

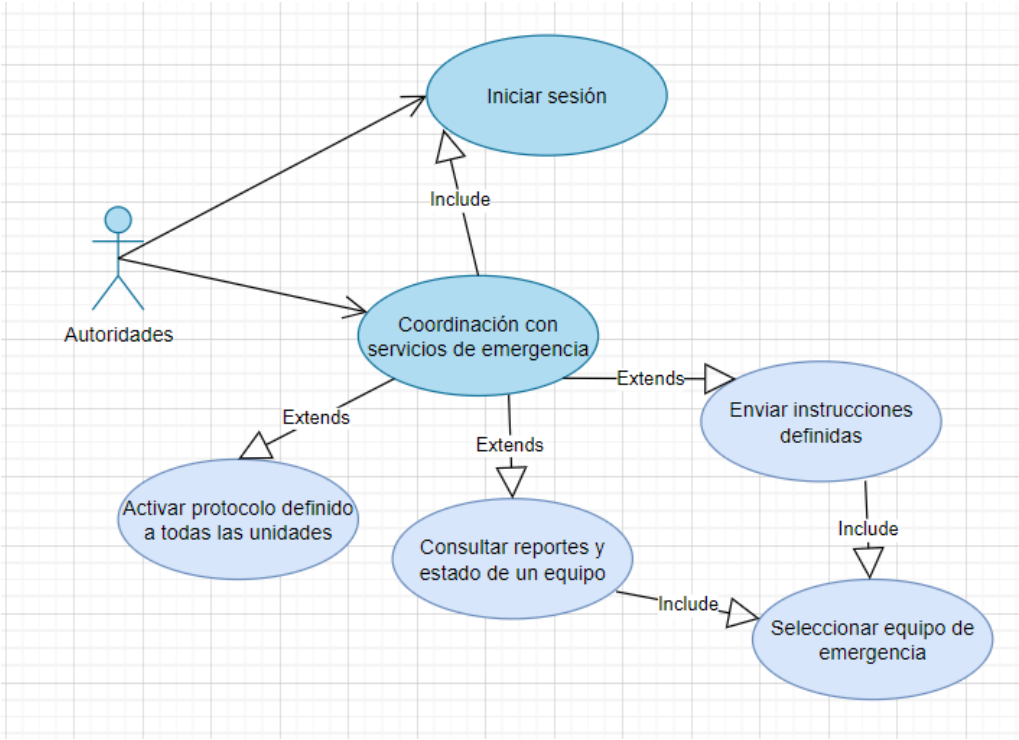


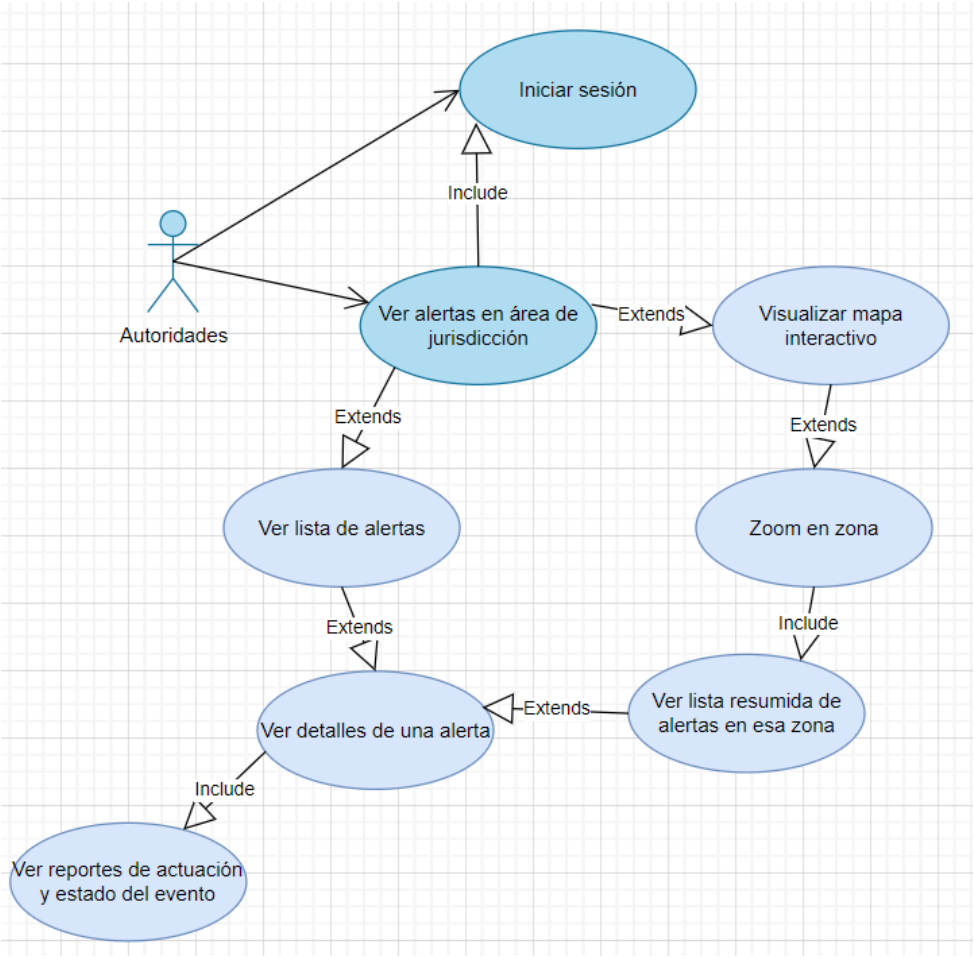



Filtrar datos
Extends
Seleccionar evento (ver detalles)
Consulta de históricos
Include
Extends
Include
Consultar las actuaciones relacionadas al evento
Autoridades
Iniciar sesión


Iniciar sesión
Include
División de servicios por zonas
Extends
Autoridades
Gestionar jurisdicción
Extends
Asociación de sensores por región/zona concreta
Extends
Extends
Dar de baja a un usuario institucional
Crear credenciales para nuevos usuarios institucionales


Iniciar sesión
Include
Añadir nueva entrada
Extends
Autoridades
Gestionar panel de recomendaciones generales
Extends
Eliminar entrada
Extends
Include
Extends
Aceptar/denegar propuestas de los servicios de emergencia
Ver listado de recomendaciones de seguridad
Modificar entrada
Include
Include
Extends
Filtrar recomendaciones por tipo de evento
Seleccionar una recomendación


Iniciar sesión
Include
Autoridades
Coordinación con servicios de emergencia
Extends
Enviar instrucciones definidas
Extends
Extends
Activar protocolo definido a todas las unidades
Consultar reportes y estado de un equipo
Include
Include
Seleccionar equipo de emergencia

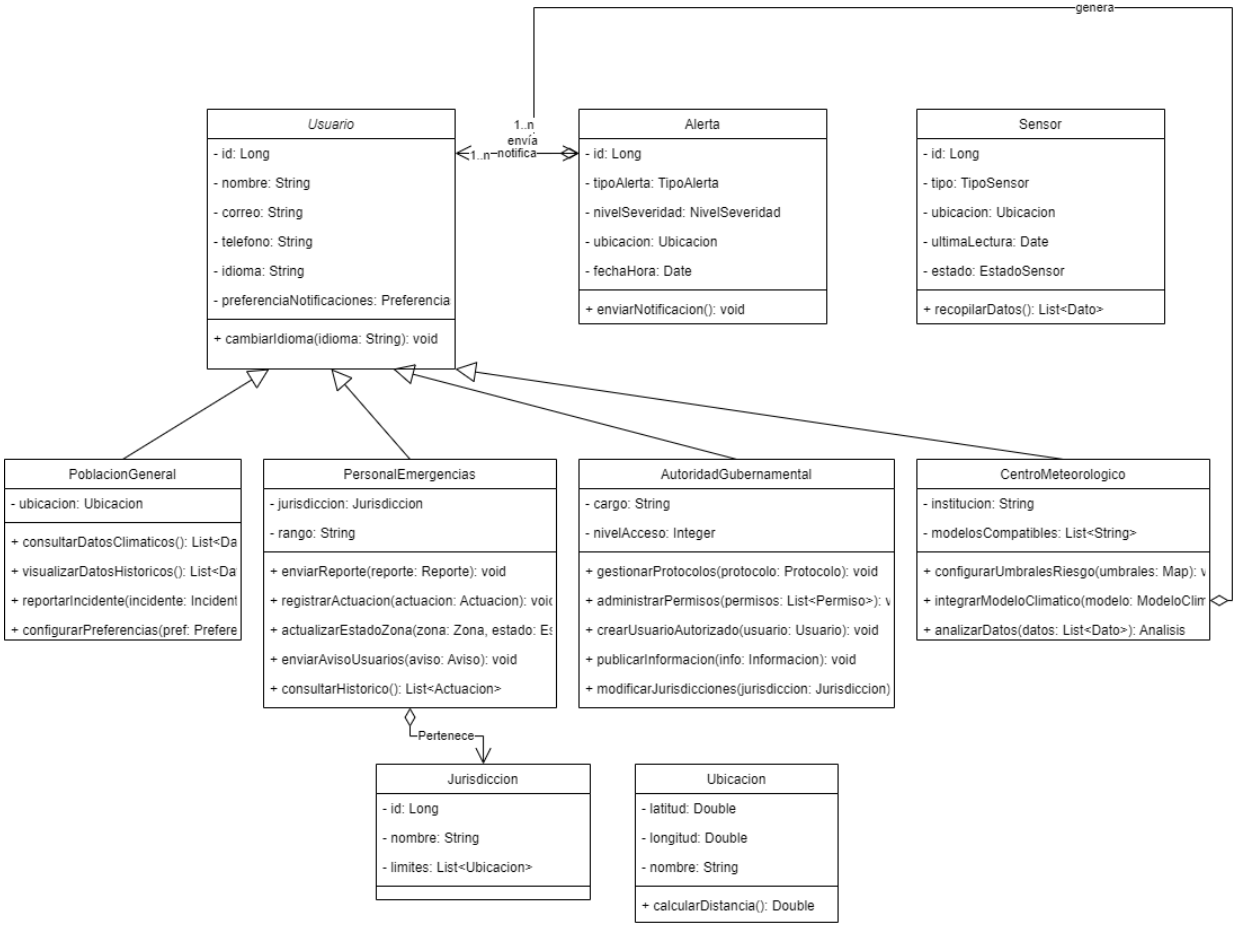


5. DIAGRAMAS DE SECUENCIA

Debido a la gran extensión de los mismos, los diagramas de secuencia se encuentran adjuntos al documento en el archivo subido al blackboard

6. DIAGRAMAS DE CLASES

A continuación, se adjunta el diagrama de clases de nuestra aplicación.



7. Conclusiones

El desarrollo del Sistema Inteligente de Prevención y Respuesta ante Eventos Climáticos (SIPREC) supone un avance en la gestión de emergencias y la eliminación de riesgos asociados a fenómenos climáticos. A través de la integración de datos ambientales en tiempo

real, predicciones meteorológicas avanzadas y mecanismos de notificación automática, SIPREC ofrece una solución robusta y escalable para la prevención y respuesta ante desastres naturales.

El sistema ha sido diseñado considerando las necesidades y características de diversos actores, desde la población general hasta autoridades gubernamentales y centros meteorológicos, garantizando una interacción eficiente y segura. La implementación de tecnologías avanzadas y el cumplimiento de normativas internacionales de seguridad y protección de datos aseguran que SIPREC sea una herramienta confiable y efectiva en situaciones críticas.

Además, la modularidad y escalabilidad del sistema permiten su adaptación y expansión futura, facilitando la incorporación de nuevas funcionalidades. SIPREC no solo mejora la capacidad de respuesta ante emergencias, sino que también promueve la colaboración y la toma de decisiones, contribuyendo así a la reducción del impacto de desastres naturales y a la protección de vidas en las comunidades afectadas.