UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE

"DISEÑO DE UN SISTEMA DE DETECCIÓN TEMPRANA DE INCENDIOS FORESTALES PARA EL GRAN VALPARAÍSO BASADA EN INTERNET OF THINGS, FOG COMPUTING Y REDES MESH"

DAVID IGNACIO ÁLVAREZ ROJAS

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

PROFESOR GUÍA: LUIS EDUARDO BASTÍAS ALARCÓN
PROFESOR CORREFERENTE: LUZ MAIRET CHOURIO ACEVEDO

Octubre 2025

CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: DISEÑO DE UN SISTEMA DE DETECCIÓN TEMPRANA DE INCENDIOS FORESTALES PARA EL GRAN VALPARAÍSO ~~BASADA EN INTERNET OF THINGS, FOG COMPUTING Y REDES MESH~~

Nombre del candidato(a): DAVID IGNACIO ÁLVAREZ ROJAS

Carrera / Grado: INGENIERO CIVIL EN INFORMÁTICA

Campus: CASA CENTRAL **Departamento:** DEPARTAMENTO DE INFORMÁTICA

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, LUIS EDO. BASTIAS A., en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad **(embargo)** por **(marcar una opción):**

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 03/11/25 **Firma:**

Estudiante o Candidato(a):

Fecha: 29/10/2025 **Firma:**

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

DEDICATORIA

A todas las personas cuyas vidas han sido irrevocablemente marcadas por el fuego. A quienes han perdido sus hogares, sus barrios, sus recuerdos y, trágicamente, a sus seres queridos en los devastadores incendios forestales que azotan a nuestra región.

De manera muy especial, dedico esta memoria a las víctimas de la catástrofe de febrero de 2024 en Viña del Mar, Quilpué y Villa Alemana.

Este trabajo no nació en el vacío de una biblioteca; nació del humo, del sonido de las sirenas y de un profundo sentimiento de urgencia.

No me cuento entre quienes sufrieron la pérdida material de su hogar o el dolor irreparable de perder a un ser amado. La fortuna quiso que el fuego no llegara a mi puerta. Sin embargo, esta memoria es una respuesta directa al horror y la impotencia que sentí durante esos días.

Fue la vivencia en carne y hueso de la fragilidad. Fue ser testigo de cómo el cielo se teñía de un naranjo apocalíptico, de respirar un aire cargado de cenizas y de sentir la vibración del pánico colectivo. Fue la angustia de la incertidumbre, el dolor de ver a mi ciudad, a mis vecinos, sufriendo de una manera tan brutal.

El gatillante de esta investigación fue la impotencia. La impotencia de ver cómo el esfuerzo de toda una vida podía ser borrado en cuestión de minutos. Pero, sobre todo, fue el miedo. Y aunque yo no lo perdí todo, mucha gente sí lo hizo.

Esta memoria es mi intento de transformar esa impotencia y ese miedo en acción. Es mi respuesta, desde la ingeniería, a la pregunta que me persiguió durante esas noches: "¿Qué podemos hacer para que esto no vuelva a pasar?". Es un intento de canalizar esa angustia hacia una herramienta constructiva, una solución que pueda, algún día, dar a otros la oportunidad que tantos no tuvieron: el tiempo para reaccionar.

En memoria de quienes ya no están, en honor a la increíble resiliencia de quienes hoy se levantan de entre las cenizas, y con la humilde esperanza de que este trabajo sirva como un aporte para construir un futuro más seguro para nuestras comunidades..

AGRADECIMIENTOS

Este trabajo es la culminación de un largo y, a ratos, arduo camino. Un viaje que habría sido imposible de completar en solitario. Hoy, al mirar atrás, comprendo que este logro no me pertenece por completo, sino que es el resultado del amor, la paciencia y el apoyo incondicional de personas extraordinarias.

A mi madre, Denisse Rojas. Mamá, tú has sido mi pilar fundamental e inquebrantable, no solo durante esta carrera, sino desde el primer día en que comencé a soñar. Quiero honrar tu apoyo incondicional que me ha sostenido desde que soy un niño. La vida no siempre nos ha puesto las cosas fáciles; hemos enfrentado tormentas, malos ratos y dificultades que parecían insuperables. Pero en medio de cada desafío, siempre hemos estado el uno para el otro, demostrando que nuestro vínculo es más fuerte que cualquier adversidad. Gracias por tus sacrificios silenciosos, por tu fuerza inagotable y por creer en mí con una fe absoluta, incluso en aquellos momentos en que yo mismo dudaba de mis capacidades. Tu resiliencia ha sido mi más grande inspiración y tu amor, la base sobre la que pude construir cada pequeño éxito. Este título es el fruto de tu esfuerzo incansable tanto como del mío; gracias por darme las herramientas, el valor y el ejemplo para nunca rendirme. Este logro te pertenece.

A mi pareja, Maysa Aguila. Amor, qué puedo decir que abarque la inmensidad de mi gratitud. Gracias por tu paciencia infinita durante incontables noches de estudio, por tu "aguante" inquebrantable en los momentos de estrés y por ser el faro que me guiaba en medio de la frustración. Tu amor fue mi refugio. Gracias por tomar mi mano, por escucharme y por recordarme lo que realmente importa.

A ambas, gracias por sostenerme. Esta memoria lleva sus nombres escritos en cada página.

RESUMEN

Esta memoria aborda la crítica vulnerabilidad de las Zonas de Interfaz Urbano-Forestal (ZIUF) del Gran Valparaíso frente a incendios forestales catastróficos, exacerbada por factores climáticos y una compleja topografía que limitan la efectividad de los sistemas de detección tradicionales. Se diseña la arquitectura completa de un sistema de detección temprana que integra sinérgicamente tecnologías de Internet de las Cosas (IoT), Fog Computing y Redes Mesh para superar las barreras de latencia, cobertura y resiliencia. El sistema se basa en una red de sensores autónomos y de bajo consumo que capturan una "multi-firma" del fuego (radiación IR, gases, partículas y variables termohigrométricas). Los datos son procesados en el borde de la red por Nodos Fog, los cuales ejecutan un algoritmo heurístico para el análisis de riesgo y la confirmación de ignición, garantizando una alerta en minutos sin depender de una conexión constante a la nube. La arquitectura, detallada mediante el modelo C4, específica una solución resiliente, escalable y costo-efectiva, concluyendo con un plan de verificación para una implementación piloto y explorando futuras mejoras, como la integración de Edge Al, para fortalecer la capacidad de respuesta ante desastres en la región.

Palabras Clave:

Detección Temprana, Incendios Forestales, Zonas de Interfaz Urbano-Forestal, Internet de las Cosas, Fog Computing, Redes Mesh, Arquitectura de Sistemas, Gran Valparaíso.

ABSTRACT

This thesis addresses the critical vulnerability of the Wildland-Urban Interface (WUI) areas of Gran Valparaíso to catastrophic wildfires, a risk exacerbated by climatic factors and complex topography that limit the effectiveness of traditional detection systems. It presents the complete architectural design of an early detection system that synergistically integrates Internet of Things (IoT), Fog Computing, and Mesh Networks technologies to overcome latency, coverage, and resilience barriers. The system is based on a network of autonomous, low-power sensor nodes that capture a multi-signature profile of a fire (IR radiation, gases, particulates, and thermo-hygrometric variables). Data is processed at the network edge by Fog Nodes, which run a heuristic algorithm for risk analysis and ignition confirmation, ensuring an alert within minutes without relying on a constant cloud connection. The architecture, detailed using the C4 model, specifies a resilient, scalable, and cost-effective solution. The work concludes with a verification plan for a pilot implementation and explores future enhancements, such as the integration of Edge AI, to strengthen disaster response capabilities in the region.

Keywords:

Early Detection, Wildfires, Wildland-Urban Interface, Internet of Things, Fog Computing, Mesh Networks, System Architecture, Gran Valparaíso.

GLOSARIO

ACID: Atomicidad, Consistencia, Aislamiento y Durabilidad.

AI: Artificial Intelligence (Inteligencia Artificial).

AMV: Área Metropolitana de Valparaíso.

ANN: Artificial Neural Network (Red Neuronal Artificial).

API: Application Programming Interface (Interfaz de Programación de Aplicaciones).

AWS: Amazon Web Services.

C4: Context, Containers, Components, Code (Modelo de visualización de arquitectura de software).

CAP: Common Alerting Protocol (Protocolo de Alerta Común).

CAPEX: Capital Expenditure (Gasto de Capital).

CBOR: Concise Binary Object Representation.

CIGIDEN: Centro de Investigación para la Gestión Integrada del Riesgo de Desastres.

CO: Monóxido de Carbono.

CO_2: Dióxido de Carbono.

CONAF: Corporación Nacional Forestal.

CPS: Cyber-Physical System (Sistema Ciberfísico).

CR2: Center for Climate and Resilience Research.

DDD: Domain-Driven Design (Diseño Dirigido por el Dominio).

ENSO: El Niño-Southern Oscillation (El Niño-Oscilación del Sur).

FLOPs: Floating-Point Operations per Second (Operaciones de Punto Flotante por Segundo).

FMEA: Failure Mode and Effects Analysis (Análisis de Modos de Fallo y Efectos).

FWI: Fire Weather Index (Índice Meteorológico de Incendios).

HMI: Human-Machine Interaction (Interacción Humano-Máquina).

IoT: Internet of Things (Internet de las Cosas).

IP: Ingress Protection (Grado de Protección de Ingreso).

IR: Infrarrojo.

ITREND: Instituto para la Resiliencia ante Desastres.

JSON: JavaScript Object Notation.

LEO: Low Earth Orbit (Órbita Terrestre Baja).

LoRa: Long Range (Largo Alcance).

LoRaWAN: Long Range Wide Area Network (Red de Área Amplia de Largo Alcance).

LPWAN: Low-Power Wide-Area Network (Red de Área Amplia de Baja Potencia).

LSTM: Long Short-Term Memory (Memoria a Corto y Largo Plazo).

M2M: Machine to Machine (Máquina a Máquina).

MAC: Media Access Control (Control de Acceso al Medio).

MBSE: Model-Based Systems Engineering (Ingeniería de Sistemas Basada en Modelos).

MCU: Microcontroller Unit (Unidad Microcontroladora).

MODIS: Moderate Resolution Imaging Spectroradiometer.

MQTT: Message Queue Telemetry Transport.

NLoS: No Line of Sight (Sin Línea de Visión).

NPU: Neural Processing Unit (Unidad de Procesamiento Neuronal).

ONG: Organización No Gubernamental.

OMS: Organización Mundial de la Salud.

OPEX: Operational Expenditure (Gasto Operacional).

OPS: Organización Panamericana de la Salud.

OTA: Over-The-Air (Por el Aire).

PHY: Physical Layer (Capa Física).

$PM_{2.5}$: Material Particulado fino con diámetro aerodinámico menor a 2.5 micrómetros.

PoC: Proof of Concept (Prueba de Concepto).

QoS: Quality of Service (Calidad de Servicio).

RDBMS: Relational Database Management System (Sistema de Gestión de Bases de Datos Relacionales).

RF: Requerimiento Funcional.

RNF: Requerimiento No Funcional.

RSS: Really Simple Syndication.

SBC: Single-Board Computer (Ordenador Monoplaca).

SENAPRED: Servicio Nacional de Prevención y Respuesta ante Desastres.

SIG: Sistema de Información Geográfica.

SINAPRED: Sistema Nacional de Prevención y Respuesta ante Desastres.

SoC: System on a Chip (Sistema en un Chip).

SPA: Single-Page Application (Aplicación de Página Única).

SUBTEL: Subsecretaría de Telecomunicaciones de Chile.

SVM: Support Vector Machine (Máquina de Vectores de Soporte).

TCO: Total Cost of Ownership (Costo Total de Propiedad).

TCP/IP: Transmission Control Protocol/Internet Protocol.

TinyML: Tiny Machine Learning.

TLS: Transport Layer Security (Seguridad de la Capa de Transporte).

TSDB: Time Series Database (Base de Datos de Series Temporales).

TVOC: Total Volatile Organic Compounds (Compuestos Orgánicos Volátiles Totales).

UAV: Unmanned Aerial Vehicle (Vehículo Aéreo No Tripulado).

ULP: Ultra-Low Power (Ultra Bajo Consumo).

VIIRS: Visible Infrared Imaging Radiometer Suite.

WMNs: Wireless Mesh Networks (Redes Inalámbricas de Malla).

WSN: Wireless Sensor Networks (Redes de Sensores Inalámbricos).

XML: Extensible Markup Language.

YOLO: You Only Look Once.

ZIUF: Zonas de Interfaz Urbano-Forestal.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA

1.1 MOTIVACIÓN Y RELEVANCIA

El Área Metropolitana de Valparaíso (AMV), comúnmente conocida como Gran Valparaíso, un área de gran importancia para Chile, enfrenta una vulnerabilidad crítica y creciente ante incendios forestales catastróficos. Esta amenaza se ve exacerbada por una compleja combinación de factores, incluyendo un clima mediterráneo propenso a la sequía estival, una topografía abrupta de cerros y quebradas, y una persistente megasequía intensificada por el cambio climático (González et al., 2020). La tragedia de febrero de 2024, el desastre socionatural más grave en Chile desde el terremoto de 2010, evidenció que las estrategias de respuesta tradicionales son insuficientes ante la magnitud de los incendios en la Zona de Interfaz Urbano-Forestal (ZIUF) (Martínez et al., 2024; Gobierno de Chile, 2024).

La recurrencia de estos eventos devastadores subraya la necesidad urgente de explorar e integrar nuevas tecnologías que puedan fortalecer las capacidades de prevención y alerta temprana, permitiendo una respuesta más rápida y efectiva que proteja vidas, viviendas y ecosistemas.

Esta propuesta se alinea con los esfuerzos nacionales por fortalecer la resiliencia ante desastres. El diseño busca contribuir a los objetivos de instituciones como el ITREND (Instituto para la Resiliencia ante Desastres), que promueven la generación de conocimiento y soluciones para robustecer las capacidades del país frente a amenazas socionaturales. Asimismo, el sistema propuesto se concibe como una herramienta tecnológica complementaria a las capacidades operativas de organismos clave como la Corporación Nacional Forestal (CONAF) y el Servicio Nacional de Prevención y Respuesta ante Desastres (SENAPRED).

1.2 CONTEXTO DEL PROBLEMA

Chile, dada su diversidad geográfica y climática, enfrenta recurrentes amenazas ambientales que impactan sus ecosistemas, economía y sociedad (González et al., 2020). Entre las más críticas se encuentran los incendios forestales y una persistente megasequía, cuya frecuencia e intensidad han aumentado notablemente en la última década. Este incremento se atribuye a una compleja interacción de factores, incluyendo el cambio climático global, cambios en el uso del suelo (como la expansión de plantaciones forestales y el crecimiento urbano hacia zonas de vegetación), y la actividad humana, que es causa directa o indirecta de la mayoría de las igniciones (González et al., 2020; Gobierno de Chile, 2024; Gil & Cruz Florencia, 2024).

Desde la década de 2010, el país enfrenta un aumento dramático en la frecuencia y severidad de los incendios forestales, destacando la aparición recurrente de "megaincendios" (eventos >10.000 ha) y temporadas de riesgo cada vez más extensas

(González et al., 2020; Gil & Cruz Florencia, 2024; Gonzales & Lara, 2024). Esta alarmante tendencia se vincula a tres factores convergentes:

1. Una **megasequía** sin precedentes que afecta la zona centro-sur desde 2010, provocando un intenso estrés hídrico en la vegetación y aumentando drásticamente su inflamabilidad (Centro de Ciencia del Clima y la Resiliencia [CR2], 2015; Goffin et al., 2023).

2. El **cambio climático** global, que intensifica la frecuencia de olas de calor bajo condiciones meteorológicas críticas (factor "30-30-30") (Cordero et al., 2024).

3. La influencia de fenómenos de variabilidad natural como **El Niño Oscilación del Sur (ENSO)**, cuyas fases cálidas se correlacionan fuertemente con las temporadas de mayor área quemada en Chile Central (Cordero et al., 2024; Martínez et al., 2024).

Las proyecciones climáticas indican que esta vulnerabilidad se agravará, creando condiciones progresivamente más favorables para incendios de gran magnitud (Gil & Cruz Florencia, 2024).

1.2.2 El Gran Valparaíso y la Interfaz Urbano-Forestal (ZIUF)

El Gran Valparaíso, que incluye comunas como Valparaíso, Viña del Mar, Quilpué y Villa Alemana, se sitúa como una de las zonas más críticamente afectadas por estos fenómenos a nivel nacional (Alegría Tardón, 2020; Martínez et al., 2024). Su combinación de un clima mediterráneo propenso a la sequía, una compleja geomorfología de cerros y quebradas, y una alta vulnerabilidad social, crea un escenario de riesgo extremo.

Las ZIUF, donde el tejido urbano se mezcla con vegetación inflamable, son el epicentro del desastre. A nivel nacional, aunque ocupan sólo un 5% del territorio, concentran el 80% de la población y el 60% de los incendios (González et al., 2020). En el AMV, estas zonas se caracterizan por:

- **Vulnerabilidad Socioeconómica:** Presencia de grupos vulnerables y asentamientos informales con limitada capacidad de respuesta (Alegría Tardón, 2020).

- **Topografía Compleja:** Comunidades densamente pobladas en laderas y quebradas de difícil acceso, lo que acelera la propagación del fuego y dificulta la evacuación (Martínez et al., 2024).

- **Infraestructura Precaria:** Construcciones de materiales ligeros y altamente inflamables (Aguirre et al., 2024).

- **Accesibilidad Limitada:** Calles estrechas y trazados irregulares que colapsan durante emergencias, impidiendo el acceso de vehículos de respuesta (Chávez et al., 2024).

- **Continuidad de Combustible:** Proximidad crítica entre viviendas, vegetación seca, especies invasoras y microbasurales (Gil & Cruz Florencia, 2024).

Eventos como el Gran Incendio de Valparaíso (2014), la "Tormenta de Fuego" (2017) y, particularmente, el Mega-Incendio de 2024 ilustran esta amenaza. Este último evento, el desastre socionatural más grave desde el terremoto de 2010, dejó un saldo de 135 fallecidos, más de 8.000 hogares afectados y costos directos que superan los US $723 millones (Gobierno de Chile, 2024; Gonzales & Lara, 2024). La rápida propagación, exacerbada por factores climáticos extremos, y las dificultades en la respuesta, evidencian que la ventana de oportunidad para una acción efectiva en las ZIUF es extremadamente reducida.

El problema central es, por tanto, la **extrema vulnerabilidad del Gran Valparaíso a incendios catastróficos en sus ZIUF y la falta de sistemas de alerta temprana suficientemente rápidos, precisos y adaptados a este complejo escenario** (Martínez et al., 2024; Gil & Cruz Florencia, 2024).

1.3 CONSECUENCIAS E IMPACTO DEL PROBLEMA

Las consecuencias de estos incendios son devastadoras y abarcan múltiples dimensiones (Urzúa & Cáceres, 2011; González et al., 2020):

1.3.1 Impacto Ambiental

- **Emisiones Atmosféricas:** Liberación de grandes cantidades de Dióxido de Carbono (CO_2) y Material Particulado fino con diámetro aerodinámico menor a 2.5 micrómetros ($PM_{2.5}$) que afectan la calidad del aire y contribuyen al cambio climático (Gil & Cruz Florencia, 2024).
- **Pérdida de biodiversidad:** Destrucción de hábitats críticos, afectando flora, fauna y la biota del suelo, comprometiendo la resiliencia de los ecosistemas (Certini et al., 2021).
- **Degradación del Suelo:** Erosión y pérdida de fertilidad, aumentando la susceptibilidad a la desertificación (González, 2017).
- **Alteración de Ciclos Hidrológicos:** Aumento de la escorrentía superficial que puede generar inundaciones y contaminar cuerpos de agua (González, 2017).

1.3.2 Impacto Social

- **Pérdida de Vidas Humanas:** Trágicas pérdidas, como las 135 muertes registradas en el evento de 2024 (Martínez et al., 2024).
- **Impacto en la Salud Física y Mental:** Graves problemas respiratorios y cardiovasculares por exposición al humo, y profundos impactos en la salud mental

(estrés postraumático, ansiedad) (Organización Panamericana de la Salud [OPS] & Organización Mundial de la Salud [OMS], 2025).

- **Desplazamiento y Deterioro Comunitario:** Migración forzada por destrucción de viviendas, generando desarraigo y afectando la cohesión social (Gonzales & Lara, 2024).

1.3.3 Impacto Económico

Evaluar el impacto económico real es desafiante, pues incluye pérdidas directas (bienes, infraestructura), costos de supresión, y daños a recursos naturales y servicios ecosistémicos intangibles (Rodríguez y Silva et al., 2012; González et al., 2020).

- **Costos Directos e Indirectos:** Enormes gastos en supresión, recuperación y reconstrucción, además de las pérdidas intangibles de servicios ecosistémicos.
- **Impacto Sectorial:** Daños severos en infraestructura crítica (energía, telecomunicaciones), turismo, y pérdida de empleos en negocios locales (Martínez et al., 2024; Subsecretaría de Telecomunicaciones [SUBTEL], 2024).

1.4 ACTORES INVOLUCRADOS

La gestión de incendios involucra una compleja red de actores cuya coordinación es fundamental:

- **Gobierno y Organismos Públicos:** CONAF (entidad técnica rectora), SENAPRED (organismo coordinador nacional) y Municipalidades (gestión del riesgo a nivel local).
- **Primera Respuesta y Seguridad:** Cuerpos de Bomberos, Carabineros de Chile y las Fuerzas Armadas.
- **Comunidades Locales:** Residentes, familias afectadas y organizaciones vecinales.
- **Sector Privado y Sociedad Civil:** Empresas forestales, empresas de servicios básicos y ONGs.
- **Investigación y Desarrollo: I**nstituciones académicas como el Centro de Investigación para la Gestión Integrada del Riesgo de Desastres (CIGIDEN) y el CR2, junto a desarrolladores de tecnologías.

La gestión efectiva requiere superar la fragmentación institucional y transitar desde un enfoque predominantemente reactivo hacia uno preventivo y coordinado (Gil & Cruz Florencia, 2024).

1.5 ESTADO DEL ARTE Y BRECHA TECNOLÓGICA

A nivel global, la detección temprana se considera un factor crítico para una gestión eficaz, lo que ha impulsado una vasta investigación en soluciones tecnológicas (Özel et al., 2024). Sin embargo, la aplicación de estas tecnologías en el complejo escenario de las ZIUF del AMV enfrenta desafíos y limitaciones significativas:

- **Limitaciones de Métodos Tradicionales y Cobertura Incompleta** (González et al., 2020; Martínez et al., 2024, Alegría Tardón, 2020).
- **Costos Elevados de Sistemas Avanzados** (Gil & Cruz Florencia, 2024).
- **Retraso en la Detección Satelital y Falta de Capacidad Microlocal** (González et al., 2020).
- **Factores Sistémicos como la fragmentación institucional y una planificación territorial deficiente** (Martínez et al., 2024; Gil & Cruz Florencia, 2024).

A continuación, se detallan las características y limitaciones de los principales sistemas de detección.

1.5.1 Sistemas de Detección Satelital

Utilizan sensores en órbita como el Espectrorradiómetro de imágenes de resolución moderada (MODIS) y la Sonda de radiómetro de imágenes infrarrojas visibles (VIIRS) para identificar anomalías térmicas (Gupta et al., s.f.; Veraverbeke et al., 2014).

Limitaciones Clave:

- **Latencia:** Retraso de 2 a 3 horas, inviable para una respuesta inicial rápida en la ZIUF (González Saggia, 2023).
- **Resolución Espacial**: El tamaño del píxel (375m a 1km) dificulta la detección de incendios pequeños (<1 ha) (Poblete, 2024).
- **Obstrucciones**: Nubes o humo denso pueden ocultar los focos de calor. (Poblete, 2024).

1.5.2 Sistemas de Detección Aérea

Uso de aeronaves o Vehículos Aéreos No Tripulados (UAV), comúnmente conocidos como drones, con cámaras visuales y térmicas para una vigilancia dirigida (González et al., 2020, Godoy Anfossi, 2022).

Limitaciones Clave:

- **Costo:** Costos operativos y de mantenimiento muy altos para una vigilancia continua.
- **Operatividad:** Restringida por condiciones meteorológicas y autonomía de vuelo.
- **Logística*:*** Requiere personal capacitado e infraestructura de apoyo.

1.5.3 Control en Tierra

Abarcan desde la vigilancia humana hasta sistemas tecnológicos desplegados en el terreno.

- **Vigilancia Humana:** Pilar histórico, pero con alcance limitado y "puntos ciegos" por la topografía (González et al., 2020).
- **Sistemas Automáticos:**
    1. **Redes de Sensores Inalámbricos (Wireless Sensor Networks, WSN):** Utilizan sensores de temperatura, humedad, gases o partículas desplegados in situ (González Saggia, 2023). Su principal ventaja es la detección hiperlocal y su inmunidad a las condiciones de visibilidad.
    2. **Vigilancia con Cámaras y Visión por Computador:** El campo más activo. Utiliza redes de cámaras y algoritmos de Deep Learning para detectar humo y llamas (Özel et al., 2024). A pesar de su potencial, son vulnerables a la oclusión por niebla o humo denso (Pang et al., 2023).

1.5.4 Brecha Tecnológica y Oportunidad de Diseño

El análisis del estado del arte revela que la principal brecha tecnológica es la falta de un sistema que combine simultáneamente:

- **Respuesta inmediata (baja latencia).**
- **Alta fiabilidad en cualquier condición de visibilidad (24/7).**
- **Resiliencia operativa en topografías complejas con infraestructura de comunicaciones precaria.**
- **Costo-efectividad que permita un despliegue denso en las zonas de mayor riesgo.**

Esta memoria aborda esta brecha mediante el diseño de una arquitectura basada en la integración sinérgica del Internet de las Cosas (IoT), Fog Computing y Redes Inalámbricas de Malla (Wireless Mesh Networks, WMNs). Este enfoque, centrado en una red de

sensores físicos, busca ofrecer una capa de detección primaria robusta y complementaria a otros sistemas de vigilancia.

1.6 OBJETIVOS

1.6.1 Objetivo General

Diseñar la arquitectura de un sistema de detección temprana de incendios forestales para las Zonas de Interfaz Urbano-Forestal del Gran Valparaíso, generando un documento de diseño técnico que especifique sus componentes y que sirva como base para un futuro prototipado.

1.6.2 Objetivos Específicos

1. **Especificar** los requerimientos funcionales y no funcionales para un sistema de detección temprana adaptado al contexto de las Zonas de Interfaz Urbano-Forestal del Gran Valparaíso
2. **Elaborar** los modelos de arquitectura que definan la estructura de contenedores, componentes y sus interacciones, para satisfacer los requerimientos del sistema.
3. **Definir** la selección de los componentes del sistema, con el fin de satisfacer los requerimientos del sistema.
4. **Diseñar** el modelo de datos que dará persistencia al sistema y definir los flujos de información que materializan las interacciones entre los componentes de la arquitectura.
5. **Evaluar** y proponer una arquitectura conceptual para la lógica de detección de incendios del sistema, sentando las bases para su futuro desarrollo e implementación.

1.7 ALCANCE DEL TRABAJO

Frente al desafío expuesto, la presente memoria de título propone el diseño arquitectónico de un sistema de detección temprana de incendios forestales, concebido específicamente para las complejas condiciones de las ZIUF del AMV.

El alcance de esta memoria se limita al **diseño arquitectónico**; la implementación física y el desarrollo completo del software quedan fuera de sus objetivos. Este trabajo, por lo tanto, constituye una propuesta de solución desde la ingeniería, enfocado en la fase de diseño y especificación, y sentando las bases para una futura implementación piloto.

CAPÍTULO 2: MARCO CONCEPTUAL

El presente capítulo establece las bases teóricas y conceptuales que sustentan la propuesta de un sistema de detección temprana de incendios forestales en Chile mediante el uso de **Internet de las Cosas (IoT), Fog Computing y Redes Mesh**. Estos conceptos son esenciales para el desarrollo de una solución eficaz y técnicamente viable que aborde el problema identificado.

2.1 INTERNET DE LAS COSAS

El **Internet de las Cosas (IoT)** se define como un paradigma en el que objetos físicos, equipados con sensores, software y otras tecnologías, se conectan e intercambian datos con otros dispositivos y sistemas a través de Internet. Esta interconexión transforma objetos cotidianos en una red inteligente que habilita el monitoreo distribuido del mundo físico para la toma de decisiones, la automatización de procesos y el control remoto de activos (Buyya & Dastjerdi, 2016). Específicamente en la gestión de desastres, como la vigilancia de incendios forestales, el IoT ofrece un enorme potencial al permitir el monitoreo en tiempo real del ecosistema forestal, aprovechando su capacidad para percibir, analizar y transmitir datos críticos desde el terreno (Sairi et al., 2023).

2.1.2 ARQUITECTURA DE REFERENCIA

Aunque las aplicaciones de IoT son diversas, la mayoría de los sistemas comparten una arquitectura conceptual estructurada en capas, que describe el flujo de datos desde su captura en el mundo físico hasta su presentación al usuario. Una arquitectura de referencia típica, especialmente en contextos industriales y de misión crítica, se puede organizar en las siguientes cuatro capas funcionales, que servirán como mapa para el resto de este capítulo (Buyya & Dastjerdi, 2016; Industry IoT Consortium, 2022):

1. **Capa de Percepción (o de Dispositivos):** Es la capa más baja, donde los "objetos" o nodos sensores interactúan con el entorno. Su función es recolectar datos físicos (como temperatura, humedad o gases) a través de sensores y, en algunos casos, actuar sobre el entorno mediante actuadores (Sairi et al., 2023). Esta capa representa el puente entre el mundo físico y el digital.

2. **Capa de Red (o de Comunicación):** Es responsable de la transmisión segura y eficiente de los datos recolectados por la capa de percepción. Esta capa abarca las tecnologías de conectividad (ej. LoRa, Wi-Fi), las topologías de red (ej. Mesh) y los protocolos de mensajería (ej. MQTT) que permiten la comunicación entre los dispositivos y los sistemas centrales (Buyya & Dastjerdi, 2016).

3. **Capa de Procesamiento (o de Cómputo):** Aquí es donde los datos son procesados para extraer información de valor. Esta capa puede estar distribuida, abarcando

desde el procesamiento en el borde de la red (Edge/Fog Computing) para decisiones de baja latencia, hasta el análisis avanzado en la nube (Cloud Computing) para el almacenamiento masivo y el procesamiento de grandes volúmenes de datos (Buyya & Dastjerdi, 2016).

4. **Capa de Aplicación y Persistencia:** Es la capa superior, responsable de presentar la información a los usuarios finales a través de interfaces, almacenar los datos a largo plazo en bases de datos y permitir la integración con otros sistemas de gestión de emergencias (Industry IoT Consortium, 2022).

2.2 CAPA DE PERCEPCIÓN

La capa de percepción es la base de cualquier sistema IoT, ya que constituye la interfaz directa con el mundo físico. Su función principal es recolectar datos del entorno a través de una red de dispositivos distribuidos, conocidos como nodos sensores. En el contexto de la detección de incendios, los sistemas de sensores terrestres basados en IoT son un enfoque complementario y prometedor que permite superar las limitaciones de los métodos tradicionales (como la visibilidad restringida en torres de vigilancia o la baja resolución temporal de los satélites), gracias a la proximidad de los sensores a los posibles puntos de ignición (Chan et al., 2024).

2.2.1: Redes de Sensores Inalámbricos (WSN):

Una Red de Sensores Inalámbrica o *Wireless Sensor Network* (WSN) es un conjunto de nodos distribuidos espacialmente, autónomos y equipados con sensores para monitorear condiciones físicas o ambientales. Estos nodos recolectan datos y los transmiten de forma colaborativa a través de la red hacia una ubicación central (Buyya & Dastjerdi, 2016). La efectividad de una WSN depende críticamente del diseño de sus nodos sensores, los cuales constan de varios componentes clave (Chan et al., 2024):

- **Unidad de Procesamiento:** Es el cerebro del nodo, usualmente un microcontrolador (MCU). Para aplicaciones de IoT que requieren un balance entre rendimiento y bajo consumo, se utilizan Sistemas en un Chip (SoC) como el ESP32-S3. Este tipo de microcontrolador integra procesadores, memoria y periféricos, y es reconocido por sus modos de ultra bajo consumo (Ultra-Low Power, ULP), como el *deep sleep*, cruciales para extender la vida útil de la batería.(Espressif Systems, 2025).

- **Unidad de Sensado:** Corresponde al conjunto de sensores encargados de medir las variables de interés. La selección de estos componentes es específica para cada aplicación.

- **Unidad de Comunicación:** Es el transceptor de radio (por ejemplo, un módulo LoRa) que permite al nodo enviar y recibir datos, definiendo el alcance y el consumo energético de la comunicación (Chan et al., 2024).

- **Unidad de Alimentación:** Provee la energía para la operación del nodo. Dado que los nodos suelen desplegarse en lugares remotos, la gestión de la energía es el desafío de diseño más crítico. Las soluciones van desde baterías de larga duración hasta sistemas de recolección de energía (energy harvesting), como paneles solares, para lograr una operación autónoma (Tan & Panda, 2011).

2.2.3 Sensores y Fusión de Datos

El concepto de "multi-firma" es una implementación práctica de una estrategia más amplia conocida como **fusión de información multisensorial**. Esta se define como el proceso de combinar datos provenientes de múltiples sensores para obtener una inferencia más precisa, completa y fiable de la que se podría lograr utilizando cada sensor de forma individual (Díaz-Ramírez et al., 2012; Liang et al., 2024). En aplicaciones de detección de eventos, la fusión de información es fundamental, ya que explota la sinergia entre distintas fuentes de datos para mejorar la calidad de la decisión final (Nakamura et al., 2007).

El objetivo principal de la fusión de datos en la detección de incendios es doble: **aumentar la sensibilidad** a eventos reales, permitiendo una detección más rápida, y **reducir la susceptibilidad a falsas alarmas** causadas por fuentes no ígneas (Gottuk et al., 2002; Choi & Jung, 2024). Por ejemplo, un sensor de humo puede activarse por vapor o polvo, pero la probabilidad de que estos fenómenos ocurran simultáneamente con un aumento anómalo de la temperatura y la presencia de monóxido de carbono (CO) es extremadamente baja (Gottuk et al., 2002). Existen diversas metodologías para realizar esta fusión, que se pueden clasificar en tres niveles principales (Liang et al., 2025):

- **Fusión a Nivel de Datos:** Se combinan los datos brutos de los sensores antes de cualquier procesamiento.
- **Fusión a Nivel de Características:** Se extraen características relevantes de cada sensor y luego se fusionan para el análisis.
- **Fusión a Nivel de Decisión:** Cada sensor (o subconjunto de sensores) toma una decisión preliminar, y luego estas decisiones se combinan para llegar a un veredicto final.

El enfoque de "multi-firma" propuesto en esta memoria se alinea con una **fusión a nivel de decisión**, donde los datos de cada sensor se procesan para generar una inferencia (ej. "hay llama", "hay humo", "el calor es anómalo") que, al ser combinada mediante un algoritmo, permite una clasificación robusta y fiable del evento.Para esta arquitectura, se fundamenta la elección de un conjunto de sensores que captura las tres huellas principales de la combustión de biomasa:

- **Radiación Infrarroja (IR) - La Llama**: La combustión genera una intensa radiación infrarroja, la cual es un indicador clave en la detección de incendios (Kadir et al., 2023). Sensores IR específicos pueden detectar esta firma térmica, permitiendo

una confirmación positiva de la presencia de llama, incluso a distancia (Kadir et al., 2023).

- **Anomalías Termo-Higrométricas - El Calor:** Un fuego incipiente provoca un aumento abrupto de la temperatura y un descenso igualmente brusco de la humedad relativa en su microentorno. Aunque estos indicadores son fundamentales, en entornos abiertos pueden verse fuertemente influenciados por las condiciones meteorológicas, lo que podría enmascarar la señal de un incendio pequeño (Chan et al., 2024). Por ello, el análisis de las tasas de cambio de estas dos variables es un indicador poderoso, pero debe ser usado en conjunto con otros para ser fiable (Khan et al., 2025).
- **Productos de Combustión - El Humo:** La quema de vegetación libera una compleja mezcla de gases y partículas. La detección de estos subproductos es crucial, ya que la mayoría de las fuentes de falsas alarmas (como el vapor de agua o el polvo) no producen monóxido de carbono (CO), lo que lo convierte en una firma muy atractiva para la discriminación (Gottuk et al., 2002).
    - **Material Particulado (PM2.5):** Es un componente principal del humo y su detección es un indicador fiable de la presencia de un incendio. Su monitoreo es, además, de vital importancia para la salud pública (Chan et al., 2024; Zhang & Pan, 2024).
    - **Gases (CO y CO_2):** El monóxido de carbono (CO) y el dióxido de carbono (CO_2) son subproductos directos de la combustión. El análisis de la concentración de estos gases, especialmente en correlación con las otras variables, mejora la fiabilidad de la detección. Experimentos de campo demuestran que, tras una ignición, las concentraciones de CO_2 y Compuestos Orgánicos Volátiles Totales (TVOC) muestran picos claros y rápidos, a diferencia de los cambios más lentos en temperatura y humedad, lo que los convierte en indicadores excelentes para la detección temprana (Chan et al., 2024; Gottuk et al., 2002).

2.3 CAPA DE RED

2.3.1 Redes Inalámbricas de Malla (WMNs)

Las **Redes Inalámbricas de Malla (Wireless Mesh Networks - WMNs)** son una topología de red donde los nodos se conectan directamente entre sí de forma dinámica y no jerárquica (Parvin, 2019). A diferencia de las topologías centralizadas como la estrella (común en LoRaWAN estándar), en una red de malla, cada nodo puede actuar como repetidor, retransmitiendo datos para otros nodos (Saldamli et al., 2019) . Esta capacidad de **comunicación multi-salto (multi-hop)** permite extender significativamente el alcance

de la red más allá de la cobertura de un único punto central y crear rutas redundantes (Parvin, 2019; Wonget al., 2024) .

Las principales ventajas de las WMNs son su **robustez** y **resiliencia**. Si un nodo falla o un enlace de comunicación se interrumpe, la red puede **auto-repararse (self-healing)** encontrando automáticamente rutas alternativas a través de otros nodos (Saldamli et al., 2019; Parvin, 2019) . Esto las hace ideales para despliegues en entornos complejos, con obstáculos o sin línea de visión directa (NLoS), como las quebradas y la topografía accidentada del AMV (RNF-04).

Aunque LoRaWAN estándar utiliza una topología de estrella, la tecnología **LoRa** (la capa física) también puede ser utilizada para implementar **redes de malla** (Wong et al., 2024) . Existen diversos protocolos, tanto propietarios (como Wirepas Mesh) como de código abierto (como Meshtastic), que implementan lógicas de enrutamiento sobre LoRa para crear redes mesh multi-salto (Suryadevara & Dutta, 2022; Wirepas, s. f.) . Estos enfoques buscan combinar el largo alcance y bajo consumo de LoRa con la resiliencia y cobertura extendida de una topología de malla, ofreciendo una solución prometedora para redes de sensores inalámbricos (WSN) en aplicaciones como la monitorización ambiental y la detección temprana de incendios en áreas remotas o de difícil acceso (Saldamli et al., 2019; Wong et al., 2024). Sin embargo, el diseño del protocolo de enrutamiento es crucial, ya que enfoques simples como la inundación (*flooding*) pueden volverse ineficientes en redes densas ((Joy & Branch, 2024); Wong et al., 2024) .

2.3.2 Tecnologías de Radio de Largo Alcance y Bajo Consumo (LPWAN)

Para que los sistemas IoT sean viables en aplicaciones de monitoreo a gran escala y en áreas remotas, como la detección de incendios forestales, la tecnología de comunicación debe cumplir con dos requisitos fundamentales: **largo alcance** y **bajo consumo de energía**. Las tecnologías tradicionales como Wi-Fi o Zigbee, aunque efectivas en corto alcance, no son adecuadas para cubrir extensas áreas forestales debido a sus limitaciones de distancia y a la necesidad de una infraestructura densa (Salaria & Singh, 2025). Por otro lado, aunque las redes celulares (como 3G/4G) ofrecen una amplia cobertura, su consumo energético es demasiado elevado para dispositivos alimentados por baterías que necesitan operar durante largos períodos sin intervención, lo que las hace poco adecuadas para este tipo de aplicación (Salaria & Singh, 2025; Brito et al., 2021).

Las tecnologías de Red de Área Amplia de Baja Potencia o ***Low-Power Wide-Area Network (LPWAN)*** surgen como la solución ideal para este desafío, ya que están diseñadas específicamente para optimizar el balance entre el alcance de la comunicación, la vida útil de la batería y el costo del dispositivo (Brito et al., 2021).

2.3.2.1 LoRa y LoRaWAN

Dentro del ecosistema LPWAN, la combinación de LoRa y LoRaWAN se ha consolidado como una de las más prometedoras y utilizadas para aplicaciones de monitoreo ambiental.

- **LoRa (Long Range)**: Es una tecnología de modulación de espectro ensanchado patentada que opera en la capa física (PHY). Su principal ventaja es que permite comunicaciones de muy largo alcance (hasta varios kilómetros en zonas rurales) con un consumo de energía extremadamente bajo, además de ser robusta frente a las interferencias (Salaria & Singh, 2025). A diferencia de otras técnicas, LoRa permite desacoplar la velocidad de datos y el ancho de banda, ofreciendo una alta flexibilidad para optimizar la red según las necesidades de la aplicación (Brito et al., 2021).

- **LoRaWAN (Long Range Wide Area Network)**: Es el protocolo de la capa de control de acceso al medio (MAC) que opera sobre la capa física LoRa. LoRaWAN define la arquitectura de la red, los formatos de los paquetes y los procedimientos de comunicación. Está diseñado con una topología de estrellas, donde los nodos finales (sensores) se comunican directamente con uno o varios *gateways* (pasarelas). A su vez, estos *gateways* retransmiten los mensajes a un servidor de red centralizado, que se encarga de gestionar la red y enrutar los datos a las aplicaciones finales (Brito et al., 2021). Esta arquitectura simplifica el diseño de los nodos finales, permitiendo que sean de bajo costo y tengan una autonomía de batería muy prolongada (Salaria & Singh, 2025).

La elección de LoRaWAN para un sistema de vigilancia de incendios forestales se justifica por su capacidad para crear redes escalables y de bajo costo en terrenos complejos, garantizando que los datos de los sensores puedan ser transmitidos de manera fiable desde ubicaciones remotas y de difícil acceso (Salaria & Singh, 2025; Brito et al., 2021).

2.3.3 Mensajería en IoT

La comunicación en un sistema IoT distribuido requiere protocolos de mensajería eficientes que puedan operar en redes con ancho de banda limitado y en dispositivos con recursos restringidos. Para ello, los protocolos de la capa de aplicación deben ser ligeros y estar optimizados para el intercambio de datos entre miles o millones de dispositivos.

2.3.3.1 PUBLISH - SUBSCRIBE

El paradigma de **publicación/suscripción (*Publish/Subscribe o Pub/Sub*)** es un patrón de mensajería asíncrono que desacopla a los productores de información (publicadores) de los consumidores de esa información (suscriptores). En este modelo, los publicadores no envían mensajes directamente a los suscriptores, sino que clasifican los mensajes en "tópicos" (o temas) y los envían a un intermediario conocido como *broker* (Lazidis et al., 2022). Los suscriptores, por su parte, manifiestan su interés en uno o más tópicos y

reciben todos los mensajes publicados en ellos por parte del *broker*, sin necesidad de conocer la identidad de los publicadores (Eugster et al., 2003).

Este desacoplamiento en espacio (los participantes no necesitan conocerse), tiempo (no necesitan estar activos simultáneamente) y sincronización (las operaciones no se bloquean) es una de sus características más potentes. Dicha arquitectura mejora drásticamente la escalabilidad, flexibilidad y modularidad de los sistemas distribuidos, lo que la convierte en un modelo ideal para las aplicaciones IoT, donde un gran número de dispositivos deben comunicarse de manera eficiente y dinámica (Lazidis et al., 2022; Eugster et al., 2003).

2.3.3.2 MQTT

***Message Queuing Telemetry Transport* (MQTT)** es un protocolo de mensajería ligero, basado en el modelo publicación/suscripción, que se ha convertido en un estándar de facto para la comunicación en el ecosistema IoT. Fue diseñado para operar sobre TCP/IP y optimizado para redes con ancho de banda limitado, alta latencia o poca fiabilidad, así como para dispositivos con recursos de procesamiento y energía restringidos (Al Enany et al., 2021). Su arquitectura se basa en un *broker* central que gestiona la distribución de mensajes entre los clientes (publicadores y suscriptores).

Una de las características más importantes de MQTT es su soporte para tres niveles de **Calidad de Servicio (*Quality of Service - QoS*)**, que garantizan la entrega de mensajes según la criticidad de la aplicación (Al Enany et al., 2021; Bender et al., 2021; Lazidis et al., 2022):

- **QoS 0 (At most once / Como máximo una vez)**: El mensaje se envía una sola vez sin confirmación de entrega. Es el modo más rápido pero menos fiable, conocido como "fire and forget".
- **QoS 1 (At least once / Al menos una vez)**: El mensaje se envía hasta que se recibe una confirmación de entrega, lo que garantiza que llegará al menos una vez, aunque podría llegar duplicado.
- **QoS 2 (Exactly once / Exactamente una vez)**: Es el nivel más fiable y seguro. Utiliza un protocolo de enlace de cuatro pasos para garantizar que el mensaje se entregue exactamente una vez.

El rendimiento y la eficiencia de un sistema MQTT dependen en gran medida del *broker* utilizado. Evaluaciones de implementaciones de código abierto, como ***Eclipse Mosquitto***, han demostrado que los *brokers* modernos son capaces de manejar un alto rendimiento con un bajo consumo de recursos, lo que valida su idoneidad para implementaciones de IoT a gran escala (Bender et al., 2021).

2.3.4 Desafíos de Seguridad en Redes de Sensores para Aplicaciones Críticas

Si bien la conectividad es fundamental, en un sistema de misión crítica como la detección de incendios, la seguridad y la integridad de los datos son primordiales. Las WSN, por su naturaleza distribuida y su despliegue en entornos no controlados, son intrínsecamente vulnerables a dos tipos principales de amenazas: fallos de funcionamiento de los sensores y ataques maliciosos (Haque & Soliman, 2025). Un nodo sensor puede transmitir datos incorrectos debido a un fallo de hardware, pero también puede ser comprometido por un actor externo para inyectar datos falsos, interceptar información o ejecutar ataques de denegación de servicio (Mohapatra & Shrimali, 2023; Haque & Soliman, 2025).

Ambos escenarios comprometen la fiabilidad del sistema, pudiendo resultar en falsas alarmas —con el consecuente desperdicio de recursos de emergencia— o, peor aún, en la no detección de un incendio real. Por lo tanto, un marco de detección robusto no solo debe identificar anomalías en los datos, sino también ser capaz de **distinguir entre un fallo de hardware y una intrusión de seguridad** (Haque & Soliman, 2025).

Esta necesidad de seguridad se extiende a los protocolos de comunicación. El protocolo MQTT, al operar sobre TCP/IP, **no proporciona mecanismos de seguridad por defecto**; la comunicación viaja en texto plano, exponiendo credenciales (usuario/contraseña) y datos a posibles ataques de intermediario (*Man-in-the-Middle*) (Alkhafajee et al., 2021). Para mitigar este riesgo, es imperativo utilizar un canal de comunicación cifrado. La solución estándar de la industria es encapsular el tráfico MQTT dentro de una capa de **Seguridad de la Capa de Transporte (TLS)**, la misma tecnología que protege las comunicaciones web (HTTPS). El uso de MQTT sobre TLS (MQTTS) garantiza la **autenticación, confidencialidad e integridad** de toda la información intercambiada entre los clientes y el *broker* (Alkhafajee et al., 2021).

Más allá del cifrado, un enfoque avanzado para asegurar la fiabilidad de la red es la implementación de un **Modelo de Confianza** (*Trust Model*). Este paradigma evalúa continuamente la fiabilidad de cada nodo sensor calculando una **puntuación de confianza** (*trust score*) basada en su comportamiento histórico y actual (Khan et al., 2025). Factores como la consistencia de los datos, la energía restante y el éxito en la comunicación se utilizan para determinar si la información de un nodo es fidedigna. Este mecanismo permite al sistema **identificar y aislar de forma proactiva a los nodos defectuosos o maliciosos**, mejorando significativamente la precisión y la robustez general del sistema de detección (Khan et al., 2025).

2.3.5 Serialización Eficiente de Datos en IoT

En redes IoT, especialmente aquellas que utilizan tecnologías LPWAN con ancho de banda limitado y donde la eficiencia energética de los nodos sensores es crítica (RNF-02), el formato utilizado para serializar (codificar) los datos antes de la transmisión es fundamental (Popić et al., 2016). Mientras que formatos basados en texto como JSON son

legibles por humanos y ampliamente utilizados en APIs web, su sobrecarga (repetición de claves de texto) los hace ineficientes para comunicaciones M2M (Machine-to-Machine) en entornos restringidos (Viotti & Kinderkhedia, 2022).

Los formatos de serialización binaria ofrecen una alternativa mucho más compacta, reduciendo significativamente el tamaño del *payload* (carga útil) y, por lo tanto, el tiempo en el aire (ToA) y el consumo de energía (Popić et al., 2016; Viotti & Kinderkhedia, 2022). Dos estándares prominentes en este ámbito son:

- **CBOR (Concise Binary Object Representation):** Un formato binario diseñado para ser una extensión de JSON, buscando una codificación extremadamente compacta sin necesidad de esquemas predefinidos (Bormann & Hoffman, 2020).
- **Protocol Buffers (Protobuf):** Un formato binario desarrollado por Google que utiliza un esquema (*schema*) predefinido para definir la estructura de los mensajes (Google, 2025). Este esquema permite una codificación aún más compacta al reemplazar las claves de texto con identificadores numéricos y facilita la validación de datos y la compatibilidad entre versiones (Popić et al., 2016; Google, 2025).

La elección entre JSON, CBOR o Protobuf implica un *trade-off* entre legibilidad, flexibilidad y eficiencia (Viotti & Kinderkhedia, 2022). Para sistemas IoT de misión crítica que requieren robustez y optimización del ancho de banda y la energía, los formatos binarios basados en esquemas como Protobuf suelen ser preferidos (Popić et al., 2016; Google, 2025).

2.4 CAPA DE PROCESAMIENTO

Una vez que los datos son recolectados por la capa de percepción y transmitidos por la capa de red, deben ser procesados para extraer información útil y tomar decisiones. Tradicionalmente, en arquitecturas IoT, este procesamiento se centralizaba en la **Nube (Cloud Computing)**. La Nube ofrece recursos virtualmente ilimitados para el almacenamiento masivo de datos históricos, el análisis complejo (*Big Data*) y el entrenamiento de modelos de inteligencia artificial, aprovechando economías de escala (Buyya et al., 2009) .

Sin embargo, enviar todos los datos brutos a la Nube introduce **latencia** debido a la distancia de comunicación y consume un **ancho de banda** considerable, lo cual es problemático para aplicaciones de misión crítica como la detección temprana de incendios, que requieren respuestas casi en tiempo real (Bonomi et al., 2012; Shi et al., 2016) . Para superar estas limitaciones, surge el paradigma del **Edge Computing** (Computación en el Borde), que busca acercar el procesamiento al lugar donde se generan los datos (Shi et al., 2016) . El **Fog Computing** (Computación en la Niebla) es una forma específica de Edge Computing que extiende la Nube creando una capa intermedia de nodos (como *gateways* o *routers*) ubicados entre los dispositivos IoT y la Nube centralizada (Bonomi et al., 2012; Yi et al., 2015) .

2.4.1 *Fog Computing*

La computación en la niebla o **Fog Computing** es un paradigma de computación distribuida que extiende los servicios de la nube (*Cloud Computing*) hacia el borde de la red (*edge*). Su objetivo es acercar las capacidades de cómputo, almacenamiento y red a los dispositivos que generan los datos, formando un continuo entre la Nube y las "Cosas" (Bonomi et al., 2012; Yi et al., 2015). En lugar de enviar todos los datos brutos a un centro de datos centralizado para su análisis, el modelo *Fog* permite que el procesamiento se realice en nodos intermedios, como *gateways*, *routers* o dispositivos dedicados en el borde.

2.4.1.1 Características y Ventaja

- **Baja Latencia y Tiempo Real**: Una de sus ventajas fundamentales es que, al procesar los datos cerca de su origen, se reduce drásticamente el tiempo de respuesta. Esto es crucial para aplicaciones críticas que dependen del tiempo, como los sistemas de alerta temprana, donde las decisiones deben tomarse en milisegundos (Bonomi et al., 2012; Yi et al., 2015).

- **Reducción del tráfico de red**: Al procesar, filtrar y agregar datos localmente en los nodos *Fog*, se minimiza el volumen de información que necesita ser enviado a la nube. Esto optimiza el uso del ancho de banda, un recurso que a menudo es limitado y costoso en despliegues remotos de IoT (Dastjerdi et al., en Buyya & Dastjerdi, 2016). En el contexto de la detección de incendios, esto permite que las redes de sensores (WSN) operen de manera más eficiente mediante estrategias de enrutamiento jerárquico asistidas por la niebla (Moussa et al., 2022).

- **Baja Latencia y Procesamiento en Tiempo Real**: La carga de procesamiento se distribuye entre múltiples nodos *Fog*, lo que mejora la escalabilidad del sistema en su conjunto. Además, estos nodos pueden operar de manera autónoma, permitiendo que el sistema de detección local siga funcionando y generando alertas incluso si la conexión a la nube se interrumpe, aumentando así la resiliencia y fiabilidad del sistema (Yi et al., 2015).

2.4.1.2 Arquitectura

La arquitectura de *Fog Computing* típicamente incluye tres capas funcionales que gestionan el flujo de datos desde el entorno físico hasta los servicios de alto nivel (Buyya & Dastjerdi, 2016; Industry IoT Consortium, 2022):

- **Capa de Dispositivos (Edge)**: Sensores y actuadores que recolectan datos del entorno y ejecutan acciones.

- **Capa de Niebla (Fog Layer)**: Nodos intermedios (como los *gateways*) que reciben datos de los dispositivos, realizan procesamiento local, filtrado, almacenamiento temporal y ejecutan la lógica de detección en tiempo real.

- **Capa de Nube (Cloud Layer)**: Proporciona almacenamiento masivo a largo plazo, procesamiento avanzado para análisis de *Big Data* y entrenamiento de modelos de inteligencia artificial.

2.4.1.3 Aplicación a la Detección de Incendios

El paradigma de *Fog Computing* es ideal para un sistema de detección temprana de incendios. Permite que los nodos *Fog*, ubicados estratégicamente cerca de las redes de sensores, analicen los flujos de datos ambientales en tiempo real. Estos nodos pueden fusionar información de múltiples fuentes para validar eventos, aplicar algoritmos de detección y generar alertas locales con una latencia mínima (Bonomi et al., 2012; Yi et al., 2015). Esta capacidad de respuesta inmediata es crítica en las ZIUF, donde cada segundo es crucial para permitir una intervención rápida y evitar la propagación del fuego (Moussa et al., 2022).

2.4.2 Arquitectura de Microservicios

La arquitectura de microservicios es un enfoque para desarrollar una aplicación como un **conjunto de servicios pequeños, autónomos y especializados**, cada uno ejecutándose en su propio proceso y comunicándose a través de mecanismos ligeros como APIs (Newman, 2015). Este estilo arquitectónico descompone el sistema en torno a las capacidades de negocio, permitiendo que cada servicio sea desarrollado, desplegado y escalado de forma independiente.

Este enfoque es particularmente relevante para las plataformas de *backend* de IoT, que por su naturaleza deben ser altamente escalables y resilientes. Adoptar microservicios permite, por ejemplo, **escalar el "Servicio de Ingesta de Datos"** para soportar miles de nodos sensores sin afectar el rendimiento del "Servicio de Gestión de Dispositivos" o la "API de Alertas", ya que cada uno opera con recursos independientes. Esta separación mejora la tolerancia a fallos —un error en un servicio no compromete a toda la plataforma— y facilita la evolución del sistema, alineándose con la naturaleza distribuida de los dispositivos IoT (Nguyen et al., 2022).

2.5 CAPA DE APLICACIÓN Y PERSISTENCIA

2.5.1 Persistencia de Datos

En un sistema de IoT, la persistencia de datos aborda el almacenamiento a largo plazo de la información generada. Dada la naturaleza diversa de los datos —desde mediciones de alta frecuencia de sensores hasta metadatos estructurales de los dispositivos—, no existe una solución única. Por ello, una arquitectura robusta debe emplear diferentes tipos de bases de datos, cada una optimizada para un propósito específico.

2.5.1.1 Bases de Datos de Series Temporales (TSDB)

Los datos generados por los sensores en un sistema IoT son, por naturaleza, **series temporales**: secuencias de mediciones indexadas en el tiempo. Las Bases de Datos de Series Temporales o ***Time Series Databases*** **(TSDB)** son sistemas especializados y optimizados para el almacenamiento y análisis de este tipo de datos, caracterizados por su alto volumen y velocidad de ingesta (Liu et al., 2024).

A diferencia de las bases de datos tradicionales, las TSDB están diseñadas para manejar cargas de trabajo con un alto volumen de escrituras y consultas que analizan rangos de tiempo, como agregaciones, promedios o detección de anomalías. En el contexto de la detección de incendios, una TSDB es fundamental para almacenar eficientemente las lecturas de temperatura, humedad y gases, y permitir consultas rápidas para el análisis en tiempo real. Estudios comparativos de rendimiento han demostrado que soluciones como **Apache IoTDB** ofrecen un rendimiento de ingesta y una eficiencia de almacenamiento significativamente superiores a otras alternativas como InfluxDB, especialmente a medida que aumenta la cantidad de dispositivos en la red, lo que las hace adecuadas para sistemas IoT escalables. (Liu et al., 2024).

2.5.1.2 Bases de Datos Relacionales y GeoEspaciales

Mientras las TSDB se encargan de los datos de medición, las **bases de datos relacionales (RDBMS)** son la opción preferida para almacenar los datos estructurales del sistema. Estos datos incluyen información transaccional y metadatos que no cambian con alta frecuencia, como la configuración de los dispositivos, la información de los usuarios, los roles y el registro de las alertas generadas (Amazon Web Services, s.f.-a).

Para esta función, **PostgreSQL** se destaca como un sistema de gestión de bases de datos objeto-relacional de código abierto, reconocido por su robustez, extensibilidad y estricto cumplimiento de las propiedades **ACID** (Atomicidad, Consistencia, Aislamiento, Durabilidad), garantizando la integridad de los datos (Poljak et al., 2017; The PostgreSQL Global Development Group, 2025). Su rendimiento superior en cargas de trabajo complejas lo convierte en una base sólida para la lógica de negocio del sistema (Amazon Web Services, s.f.-a).

Sin embargo, los datos en un sistema de detección de incendios tienen un componente geográfico inherente: la ubicación de cada nodo sensor es crítica. Para cualquier análisis espacial que vaya más allá de simplemente visualizar puntos en un mapa, el uso de una base de datos con capacidades espaciales es indispensable (Tjukanov, 2018). Es aquí donde la extensión PostGIS se vuelve fundamental. PostGIS transforma a PostgreSQL en un potente y completo Sistema de Información Geográfica (SIG), convirtiéndola en el estándar de la industria para soluciones espaciales de código abierto (The PostGIS Development Group, s. f.). Esta combinación permite no solo almacenar la ubicación de los nodos, sino también realizar consultas espaciales complejas de alto rendimiento, como análisis de

proximidad, consultas por radio o definición de geo-cercas, que son la base para contextualizar y localizar las alertas generadas por el sistema.

2.5.2 Estándares de Interoperabilidad y Notificación

Para que un sistema de IoT sea eficaz y pueda integrarse con otros sistemas o notificar a los usuarios, debe basarse en estándares de comunicación abiertos y ampliamente aceptados. La interoperabilidad se define como la capacidad de un sistema para soportar la integración de dispositivos de hardware con diferentes sistemas operativos y protocolos de manera fluida. En el contexto de la gestión de desastres, donde múltiples agencias y tecnologías deben colaborar, la interoperabilidad no es solo una ventaja técnica, sino un requisito fundamental.

2.5.2.1 Protocolo de Alerta Común (CAP)

Para la difusión de alertas de emergencia, el estándar internacional de facto es el **Protocolo de Alerta Común (Common Alerting Protocol - CAP)**. CAP es un formato de datos estándar basado en XML, diseñado para intercambiar alertas y advertencias públicas entre todo tipo de sistemas. Fue desarrollado para abstraer los elementos esenciales de un mensaje de advertencia de las tecnologías de entrega subyacentes, simplificando así la integración de diversos sistemas de difusión. El modelo de datos de CAP permite encapsular información crítica en un formato estructurado, incluyendo:

- **Qué está sucediendo:** Descripción del evento, urgencia, severidad y certeza.
- **Dónde está ocurriendo:** Definición del área afectada mediante polígonos geoespaciales, círculos o geocódigos predefinidos.
- **Qué hacer:** Instrucciones recomendadas para la población.

La adopción de CAP por parte del sistema de detección propuesto asegura que las alertas generadas sean interoperables y puedan ser consumidas de manera nativa por plataformas del Sistema Nacional de Prevención y Respuesta ante Desastres (SINAPRED), sistemas de radiodifusión, aplicaciones móviles y otros canales de notificación, cumpliendo con las mejores prácticas internacionales recomendadas para la comunicación de riesgos.

2.5.2.2 APIs RESTful y RSS

- **APIs RESTful:** Una Interfaz de Programación de Aplicaciones (API) que sigue los principios REST (Representational State Transfer) se ha consolidado como un estándar de facto para la comunicación entre sistemas distribuidos en la web. Permite que diferentes componentes del sistema (desde los Nodos Fog hasta las aplicaciones web) se comuniquen de forma estandarizada y sin estado.

- **RSS (Really Simple Syndication)**: Es un formato de sindicación web basado en XML, diseñado para publicar contenido que se actualiza con frecuencia. Para el sistema de detección, un *feed* RSS constituye un canal de notificación público y de bajo acoplamiento. Al publicar las alertas validadas en un *feed* RSS 2.0, se facilita que organismos de emergencia, medios de comunicación y el público en general puedan suscribirse y recibir notificaciones de manera automática y estandarizada.

2.5.2.3 API GraphQL para Consultas Flexibles

Si bien las APIs RESTful son un estándar para la comunicación entre sistemas, para interfaces de usuario complejas como los *dashboards* de monitoreo en tiempo real, el patrón REST puede llevar a problemas de *over-fetching* (recibir más datos de los necesarios) o *under-fetching* (necesitar múltiples peticiones para obtener toda la información) (China, 2025). **GraphQL** surge como una alternativa o complemento a REST, ofreciendo un lenguaje de consulta para APIs que permite a los clientes solicitar exactamente los datos que necesitan y nada más (China, 2025).

Una característica clave de GraphQL es su soporte nativo para **Suscripciones** (*Subscriptions*), un mecanismo basado en WebSockets que permite al servidor enviar actualizaciones de datos en tiempo real a los clientes suscritos (Hasura, 2025).

CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

3.1 MARCO METODOLÓGICO Y DE DISEÑO

El diseño de un sistema de detección temprana de incendios, distribuido en tres niveles (Edge, Fog, Cloud) y con un mandato de seguridad vital, constituye un desafío de **Sistema Ciberfísico (CPS)** (Greer et al., 2019). En estos sistemas, los componentes de hardware, el software embebido, las redes de comunicación y las plataformas en la nube están profundamente entrelazados (Bonomi et al., 2012). Una arquitectura de esta magnitud no puede abordarse con una sola metodología, sino que exige un marco híbrido y riguroso que gestione la complejidad de todos los dominios simultáneamente (Gräßler et al., 2021).

La arquitectura propuesta en esta memoria se ha desarrollado utilizando un **marco metodológico híbrido y multi-paradigma** para garantizar la trazabilidad, robustez y fiabilidad que un sistema de seguridad vital demanda.

3.1.1 Marco Metodológico Híbrido

La arquitectura del sistema se deriva de un enfoque híbrido que aplica tres metodologías estándar de la industria en sus respectivos niveles de abstracción:

1. **Gobernanza General:** El ciclo de vida completo del sistema (hardware y software) se rige por la **Ingeniería de Sistemas Basada en Modelos (*MBSE*)** (Ansys, 2025). Este enfoque utiliza un modelo digital cohesivo como la "única fuente de la verdad" (Shevchenko, 2020) para conectar requisitos, diseño y análisis. El proceso sigue el **Modelo en V**, un estándar para el desarrollo de sistemas de misión crítica (Smith, 2025). El Modelo en V impone una disciplina de Verificación y Validación (V&V) paralela a cada fase de diseño, asegurando que la fiabilidad no sea un pensamiento tardío, sino una característica diseñada desde el inicio (Gräßler et al., 2021).

2. **Descomposición del Sistema:** Dentro del marco MBSE, la arquitectura se descompone inicialmente utilizando los principios de *CBD* (Jonsson, 2016). El sistema se estructura en componentes lógicos y tecnológicamente agnósticos (ej. "Componente de Gestión de Energía", "Componente de Red de Malla", "Componente de Persistencia Temporal"). Esta abstracción permite analizar las responsabilidades y las interacciones de cada bloque antes de comprometerse con una tecnología específica.

3. **Descomposición del Software:** Para la alta complejidad del software, especialmente en el backend de la Nube y la lógica del Fog, se aplica la metodología de **Diseño Dirigido por el Dominio (DDD)** (Laribee, 2009). Se utilizan los patrones de **Contextos Delimitados (Bounded Contexts)** (De la Torre et al., 2022) para identificar y aislar los subdominios de negocio (ej. "Gestión de Alertas", "Gestión de Dispositivos", "Analítica de Riesgo"). Estos contextos definen los

límites naturales para nuestros **microservicios** (Microsoft, s.f), asegurando que cada servicio tenga una alta cohesión y un bajo acoplamiento.

3.1.2 Estándar de Justificación de Decisiones

En un sistema de misión crítica, las decisiones arquitectónicas deben ser explícitas, auditables y defendibles. Cada decisión tecnológica clave presentada en este capítulo se justificará formalmente utilizando un análisis estructurado de compensaciones (*trade-offs*), alineado con el estándar **ISO/IEC/IEEE 42010**, que exige abordar las "preocupaciones" (*concerns*) de los "interesados" (*stakeholders*) (iso-architecture.org, 2025). Las dos "preocupaciones" principales que guían nuestro análisis son:

1. **Fiabilidad:** Se aplica un *FMEA* (Análisis de Modos de Fallo y Efectos) proactivo a cada componente. El diseño debe mitigar los modos de fallo de alta severidad. Por ejemplo, el FMEA de la lógica de detección (Gas+IR) identificó un punto ciego en la "combustión latente" , lo que obliga a incluir un sensor de Partículas (PM) para mitigar este riesgo .

2. **Viabilidad Económica:** Las decisiones no se basan en el coste de adquisición (*CAPEX*), sino en el *TCO* (Análisis de Coste Total de Propiedad) a 10-15 años. Esto incluye OPEX (costos de mantenimiento, energía, red). 3.2 MODELO DE VISUALIZACIÓN

Para comunicar la arquitectura de forma clara y profesional a diferentes audiencias, se adopta se utilizará el **Modelo C4** (Contexto, Contenedores, Componentes, Código) (Brown, s. f.). C4 es el estándar de la industria para describir la arquitectura *lógica* del software, permitiendo "hacer zoom" desde la visión general del sistema (Nivel 1) hasta los contenedores desplegables (Nivel 2) y los módulos internos (Nivel 3).

3.3 REQUERIMIENTOS DEL SISTEMA

El diseño de un sistema de misión crítica comienza con un conjunto de requerimientos claros, rigurosos y medibles. Estos requerimientos se derivan del análisis del problema y se rigen por el marco metodológico y los mandatos de diseño definidos en la sección anterior.

Los requerimientos se dividen en dos categorías: **Requerimientos Funcionales (RF)**, que describen *qué* debe hacer el sistema, y **Requerimientos No Funcionales (RNF)**, que definen *cómo de bien* debe hacerlo y establecen los atributos de calidad y las restricciones de diseño.

3.3.1 Requerimiento Funcionales

Los requerimientos funcionales definen las capacidades fundamentales del sistema, desde la captura de datos hasta la notificación.

ID	Nombre	Descripción
RF-01	Adquisición de Datos Multi-Firma	El Nodo Sensor debe ser capaz de recolectar datos de múltiples modalidades de detección de incendios: químicas (CO, COV), de partículas (PM2.5) y energéticas (Llama IR).
RF-02	Transmisión de Red Resiliente	El sistema debe transmitir los datos de los sensores a través de una topología de red en malla (mesh) auto-reparable y de múltiples saltos.
RF-03	Operación Autónoma del Nodo	El Nodo Sensor debe operar de forma autónoma, gestionando su propia recolección de energía (solar) y su almacenamiento (supercondensador) sin intervención humana.
RF-04	Detección de Anomalías en el Borde (Edge)	El Nodo Sensor (Edge) debe ejecutar lógica local para analizar sus propios datos, detectar anomalías y tomar la decisión primaria de generar una alerta.
RF-05	Procesamiento en la Niebla (Fog)	El Nodo Fog debe agregar datos de múltiples sensores, ejecutar lógica heurística regional (ej. correlación con FWI) y almacenar alertas en búfer en caso de fallo del backhaul.
RF-06	Contextualización de Datos	El sistema debe ser capaz de enriquecer los datos de los sensores con fuentes externas, como datos meteorológicos (para FWI) e información geoespacial (zonas de riesgo).
RF-07	Generación de Alertas Estructuradas	Al detectar un evento de alta confianza, el sistema debe generar una alerta estructurada que incluya tipo de evento, ubicación, nivel de confianza y datos de los sensores.
RF-08	Notificación Interoperable a Actores	El sistema debe notificar las alertas críticas a los actores externos (SENAPRED, CONAF, Bomberos) utilizando un estándar nacional abierto.
RF-09	Almacenamiento de Información	El sistema debe almacenar de forma persistente los datos históricos de series temporales (telemetría) y los datos operativos (metadatos de dispositivos, alertas, usuarios).
RF-10	Interfaz de Monitoreo Centralizada	El sistema debe proveer una interfaz de usuario (Dashboard) para la visualización geoespacial en tiempo real del estado de la red, los sensores y las alertas activas.
RF-11	Administración del Sistema	El sistema debe permitir a los Administradores gestionar el ciclo de vida de los dispositivos (aprovisionamiento, monitoreo, actualizaciones OTA) y las cuentas de usuario.

Tabla 1: Requerimientos Funcionales

3.3.2 Requerimientos No Funcionales

Los RNF son los atributos de calidad que definen el rendimiento y la robustez del sistema. Son las restricciones de diseño más críticas y cada una se justifica por un análisis de ingeniería previo.

ID	Nombre	Descripción
RNF-01	Baja Latencia de Alerta	El tiempo desde la detección de una ignición por un sensor hasta la generación de una alerta procesable en el Nodo Fog debe ser < 2 minutos (Objetivo: < 30 segundos).
RNF-02	Autonomía Energética	El Nodo Sensor debe tener una vida útil operativa de 10-15 años sin mantenimiento físico (reemplazo de batería).
RNF-03	Alta Disponibilidad	Los servicios centrales en la nube deben mantener una disponibilidad de ≥ 99.9%.
RNF-04	Resiliencia Operacional	El sistema debe ser tolerante a fallos de red, hardware e infraestructura terrestre.
RNF-05	Precisión de Detección	El sistema debe maximizar la Tasa de Verdaderos Positivos (>95%) y minimizar Falsos Positivos (<5%). Crucialmente, debe mitigar Falsos Negativos conocidos.
RNF-06	Robustez Ambiental	Los encapsulados de los dispositivos de campo deben cumplir con un estándar mínimo de IP67.
RNF-07	Escalabilidad	La arquitectura de backend debe escalar horizontalmente para soportar una ingesta de >100,000 dispositivos y cargas de consulta elevadas.
RNF-08	Mantenibilidad (TCO)	El diseño debe minimizar el OPEX de mantenimiento (complejidad de firmware, logística, visitas de campo).
RNF-09	Interoperabilidad	El sistema debe intercambiar alertas con agencias nacionales (SENAPRED, CONAF) usando estándares abiertos.
RNF-10	Usabilidad	La interfaz de usuario debe ser intuitiva y capaz de renderizar datos geoespaciales de alta densidad (>10,000 puntos) en tiempo real.
RNF-11	Seguridad Integral	Todas las comunicaciones deben ser cifradas (TLS 1.3, AES-256)[1]. Los datos en reposo deben ser cifrados.
RF-12	Auditabilidad	El sistema debe registrar eventos críticos (generación de alertas, acciones de usuario) en un log inmutable.

Tabla 2: Requerimientos No Funcionales

[1]AES-256 y TLS son estándares para garantizar la confidencialidad e integridad de los datos en sistemas IoT (Buyya & Dastjerdi, 2016; Alkhafajee et al., 2021).

Estos RNF se traducen en criterios de aceptación medibles que el diseño final debe cumplir:

ID	Criterio de Aceptación
RF-01	La latencia de extremo a extremo (Ignición -> Alerta en Dashboard) debe ser < 2 minutos[2].
RF-02	El Nodo Sensor debe operar 10 años sin mantenimiento de batería.
RF-04	El protocolo de red debe garantizar >99.9%[3] de entrega de paquetes en un entorno de alta densidad (100 nodos/gateway).
RF-05	La lógica de fusión debe demostrar una tasa de Falsos Negativos < 1%[4] para incendios de combustión latente (smoldering) en pruebas controladas.
RF-07	El backend debe demostrar la capacidad de ingerir >10,000 mensajes/segundo y escalar horizontalmente para mantener la latencia de ingesta p99 por debajo de 500ms.
RF-09	El sistema debe generar alertas válidas según el estándar CAP v1.2 y entregarlas vía Webhook a un endpoint de prueba.
RF-10	El frontend debe mantener >30 FPS al renderizar 50,000 marcadores de sensores dinámicos en un mapa interactivo.

Tabla 3: Criterio de Aceptación

3.4 ARQUITECTURA DEL SISTEMA

Habiendo establecido el marco metodológico y los requisitos de ingeniería, esta sección aplica el estándar de visualización definido (el Modelo Híbrido C4-Cloud) para describir la arquitectura de la solución (Brown, s. f.). La arquitectura se presenta en una secuencia jerárquica de "zoom", comenzando por el contexto de más alto nivel y detallando progresivamente los contenedores lógicos, los componentes tecnológicos específicos y, finalmente, el modelo de despliegue físico.

3.4.1 Nivel 1: Diagrama de Contexto

El Diagrama de Contexto (Nivel 1) sitúa al "Sistema de Detección de Incendios" como una única "caja negra" en el centro de su ecosistema operativo (Brown, 2025a). Este diagrama identifica a los actores (personas) y los sistemas de software externos clave que interactúan con él:

[2] Basada en el rendimiento de una arquitectura comparable presentada por Moussa et al. (2022).
[3] Estándar industrial para sistemas de misión crítica, según principios de la Arquitectura de Referencia del Internet Industrial (Industry IoT Consortium, 2022).
[4] Sistemas parecidos reportan tasas de precisión superiores al 98% (Liang et al., 2024).

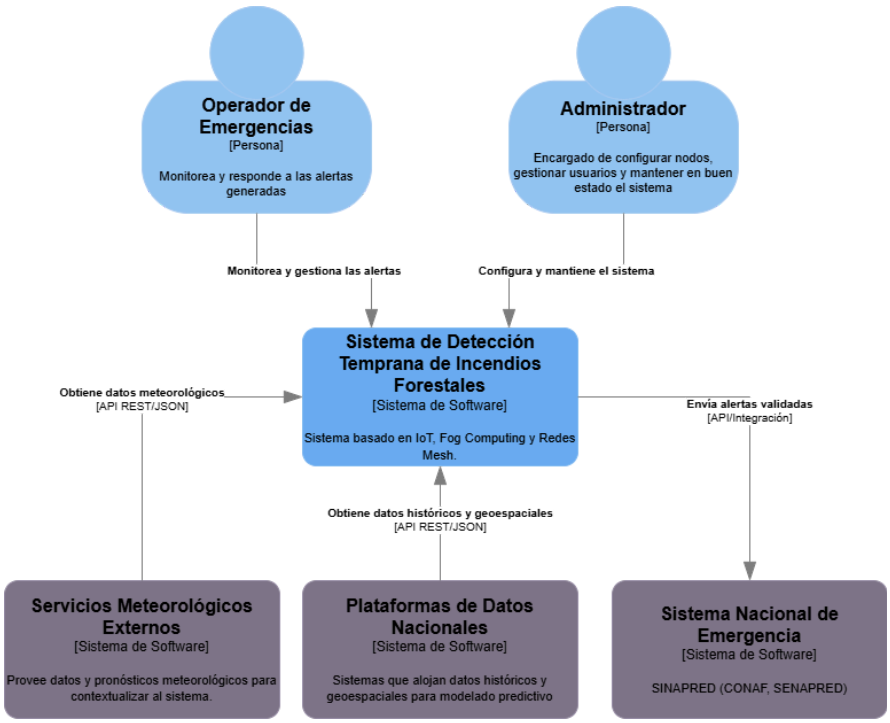


Figura 1: Diagrama C4 Nivel 1

- **Actores:**
    - **Operador de Emergencias:** Usuario principal que monitorea el estado de la red, recibe y gestiona las alertas generadas.
    - **Administrador del Sistema:** Usuario técnico responsable de aprovisionar nodos, gestionar usuarios y supervisar la salud de la infraestructura.
- **Sistemas Externos:**
    - **Sistemas Nacionales de Emergencia:** Representa a las agencias receptoras de alertas críticas. La interoperabilidad con estos sistemas, como la CONAF, el **SENAPRED** y **Bomberos de Chile**, es un requisito fundamental, gestionado a través de estándares abiertos (OASIS, 2010).
    - **Servicios Meteorológicos Externos:** APIs de pronóstico que proporcionan datos de observación (ej. precipitación) necesarios para que el Nodo Fog calcule índices de riesgo hiperlocal, como el Índice Meteorológico de Incendios (FWI) (Van Wagner, 1987).
    - **Plataformas de Datos Nacionales:** Sistemas (en la Nube) que alojan conjuntos de datos estratégicos para el modelado predictivo, como los datos históricos de incendios de CONAF (Vidal-Silva et al., 2025) y los datos geoespaciales (topografía, vegetación).

3.4.2 Nivel 2: Diagrama de Contenedores

El Diagrama de Contenedores (Nivel 2) descompone la "caja negra" del sistema en sus principales unidades lógicas y desplegables (Brown, s. f.). Siguiendo los principios de Diseño Basado en Componentes (CBD), estos contenedores son agnósticos a la implementación específica (Jonsson, 2016):

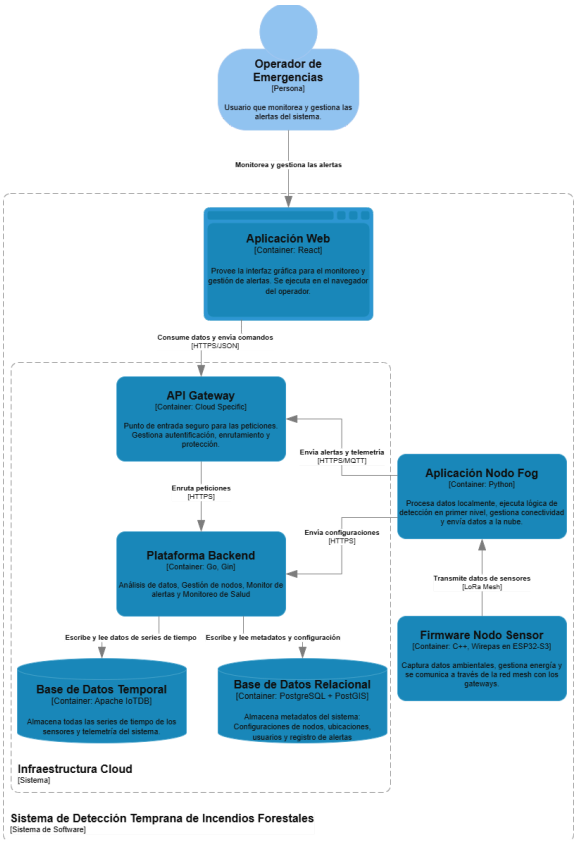


Figura 2: Diagrama C4 Nivel 2

1. **Firmware Nodo Sensor (Borde):** Aplicación de software embebido que se ejecuta en el MCU del nodo.

2. **Red de Malla (Fabric):** Protocolo de red que proporciona conectividad resiliente y multisalto entre los nodos sensores y el Nodo Fog.

3. **Aplicación Nodo Fog (Niebla):** Fog Computing es usado para disminuir la latencia en alertas tempranas y reducir el ancho de banda.

4. **Plataforma Backend (Nube):** Conjunto de microservicios que gestionan la ingesta de datos y la lógica de negocio.

5. **Persistencia Temporal (TSDB) (Nube):** Base de datos optimizada para datos de series temporales de telemetría.

6. **Persistencia Operacional (RDBMS) (Nube):** Base de datos relacional para metadatos, usuarios, zonas geoespaciales y alertas.
7. **API de Frontend (Nube):** Interfaz que expone los datos a los clientes.
8. **Aplicación Web (Frontend) (Nube):** Aplicación de página única (SPA) que se ejecuta en el navegador del operador.

3.4.3 Nivel 3: Diagrama de Componentes

El Nivel 3 detalla los componentes internos clave y justifica la selección de la *clase* de tecnología para cada uno, basándose en los Requerimientos No Funcionales (RNF) y los principios de diseño establecidos.

Firmware Nodo Sensor

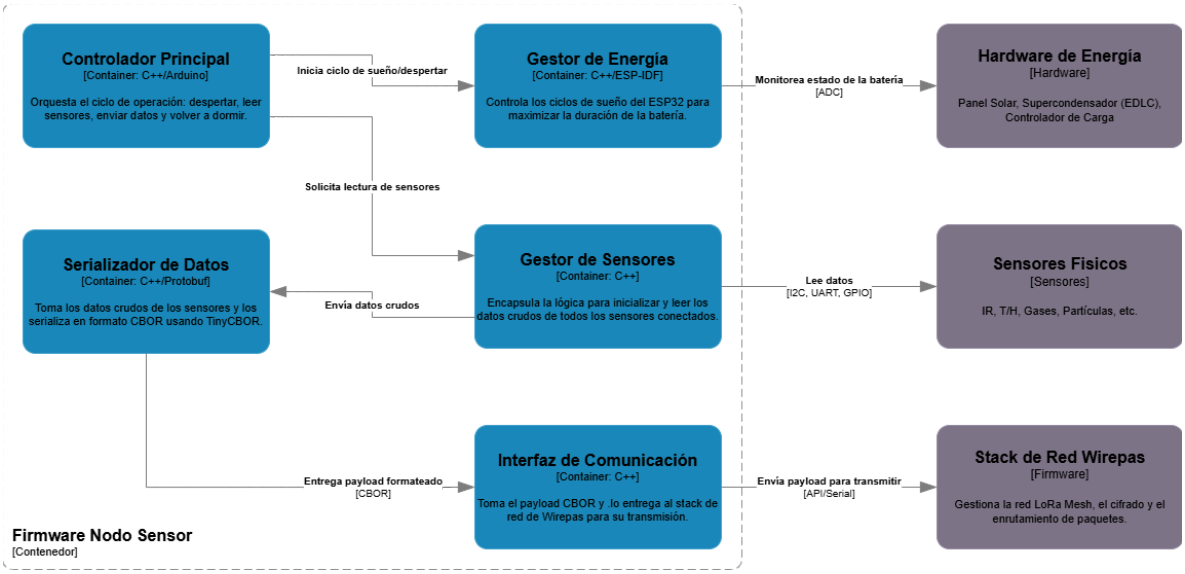


Figura 3: Diagrama C4 Nivel 3 Nodo Sensor

- **MCU: Un Microcontrolador (MCU/SoC) de bajo consumo con capacidades de aceleración de IA.**
    - La selección de un **MCU** es fundamental para WSN debido a las estrictas **restricciones de energía**, costo y tamaño inherentes (Buyya & Dastjerdi, 2016). Los nodos sensores suelen operar con baterías o recolección de energía en ubicaciones remotas, haciendo del **bajo consumo energético** el desafío de diseño más crítico (Chan et al., 2024; Buyya & Dastjerdi, 2016). Se requiere un MCU avanzado que ofrezca un equilibrio entre capacidad de procesamiento y modos de **ULP** para cumplir con el RNF-02 (Chan et al., 2024). Los modos ***deep sleep*** de los MCU permiten reducir el consumo a unos pocos microamperios (µA) al apagar la CPU y la mayoría de los

periféricos (Espressif Systems, 2025). Esta capacidad es **esencial** para lograr años de operación autónoma.

- **Sensores: Una suite de sensores físicos (fusión de Gas + Partículas + Llama IR).**
    - Se elige la detección basada en sensores físicos (RF-01) sobre alternativas remotas (cámaras, satélites) por su capacidad única de detectar un incendio en su fase incipiente (combustión latente), la ventana de tiempo más temprana posible (Dryad Networks, 2025a; Zhang & Pan, 2024). La fusión de múltiples firmas (*multisensor-fusion*) es una estrategia comprobada para reducir falsas alarmas (Gottuk et al., 2002). El RNF-05 (mitigar falsos negativos) exige una suite de 3 factores (Gas + Partículas + IR), ya que la detección de partículas (PM) es una mitigación obligatoria para el modo de fallo de "combustión latente" (*smoldering*), que no produce una firma IR de llama clara (Zhang & Pan, 2024).
- **Alimentación: Sistema de recolección solar con almacenamiento en Supercondensador (EDLC).**
    - Cumple con RNF-02 (Autonomía 10-15 años). Se requiere una solución de recolección de energía (solar). El análisis de fiabilidad climática y TCO prefiere los EDLC sobre las baterías LiFePO4. Los EDLC son inmunes al fallo por carga a temperaturas bajo cero, un modo de fallo catastrófico para las baterías de iones de litio en el entorno operativo (EATON, 2024; KYOCERA AVX, 2025; Naumann et al., 2018).

Protocolo

- **Una topología de Red de Malla (Mesh):** Se selecciona una topología Mesh para garantizar la conectividad resiliente. A diferencia de la topología estrella (como LoRaWAN estándar), donde cada nodo debe tener línea de visión directa con un gateway, una red mesh permite la comunicación multi-salto (*multi-hop*). Esto extiende significativamente la cobertura y supera obstrucciones, crucial en topografías complejas como las quebradas de Valparaíso que crean "zonas de sombra".

Aplicación Nodo Fog

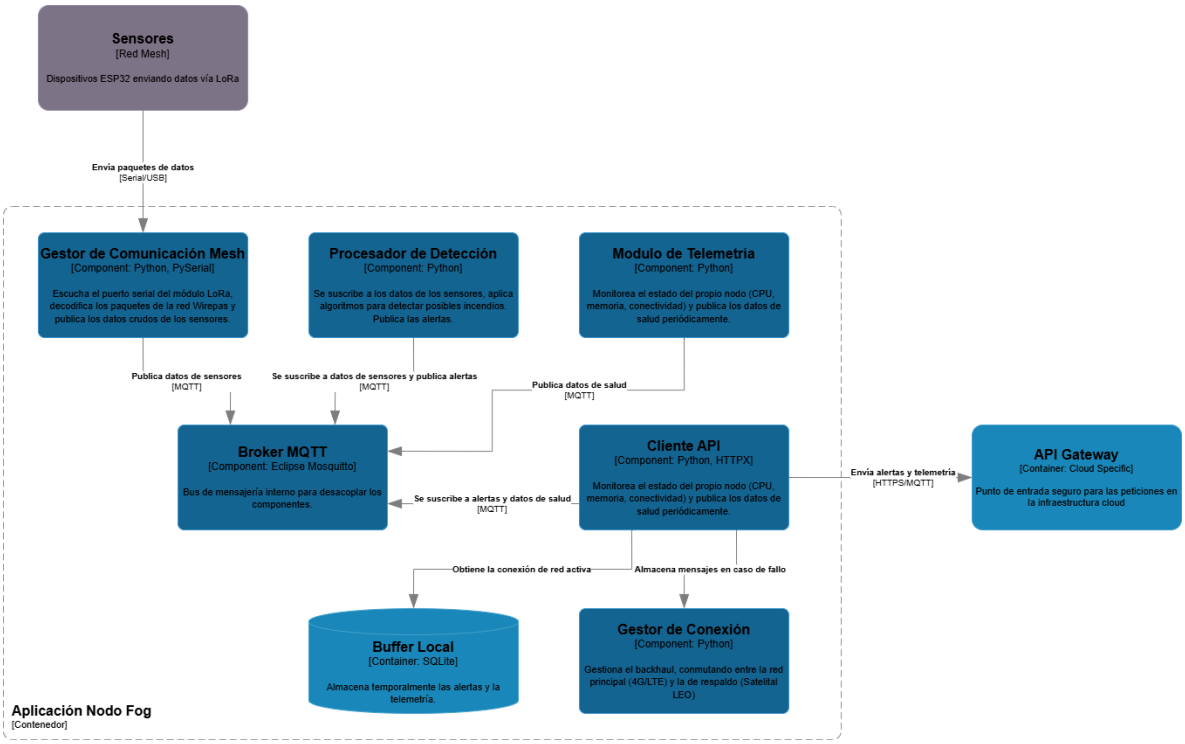


Figura 4: Diagrama C4 Nivel 3 Nodo Fog

Se adopta un enfoque de **Fog Computing**, procesando datos en el **Nodo Fog** (gateway) en lugar de enviarlos directamente a la nube (Bonomi et al., 2012). Esto es crucial para la **baja latencia** requerida en alertas tempranas, al procesar cerca de los sensores (Bonomi et al., 2012; Yi et al., 2015; Shi et al., 2016). Además, **reduce el uso de ancho de banda** al enviar sólo datos relevantes a la nube (Yi et al., 2015; Moussa et al., 2022; Shi et al., 2016) y aumenta la **resiliencia** al permitir la **operación autónoma** local incluso sin conexión a Internet (Yi et al., 2015; Moussa et al., 2022).

- **SBC: Un Ordenador Monoplaca (SBC)**
    - Se requiere un SBC para el Nodo Fog (RNF-05) capaz de ejecutar una pila de software compleja (Bonomi et al., 2012). Se debe seleccionar un SBC con almacenamiento **eMMC soldado**, el cual ofrece **fiabilidad superior** gracias a su **controlador integrado** que gestiona activamente la NAND flash con ***wear leveling*** y ***ECC***, optimizando la vida útil (SmartSemi, 2023). Las tarjetas SD estándar carecen de esta gestión avanzada, por lo que se consideran inaceptables para una operación desatendida a largo plazo debido a su menor **resistencia inherente** (SmartSemi, 2023).

- **Backhaul: Un backhaul celular como enlace principal y un backhaul satelital como enlace de respaldo.**
    - RNF-04. 4G/LTE ofrece cobertura madura y coste-efectividad (nperf, s.f). Un enlace satelital LEO proporciona **diversidad de ruta completa** (inmunidad a fallos de infraestructura terrestre) con un TCO disruptivamente bajo, esencial para la resiliencia en desastres (Aufranc, 2022).

Plataforma Backend

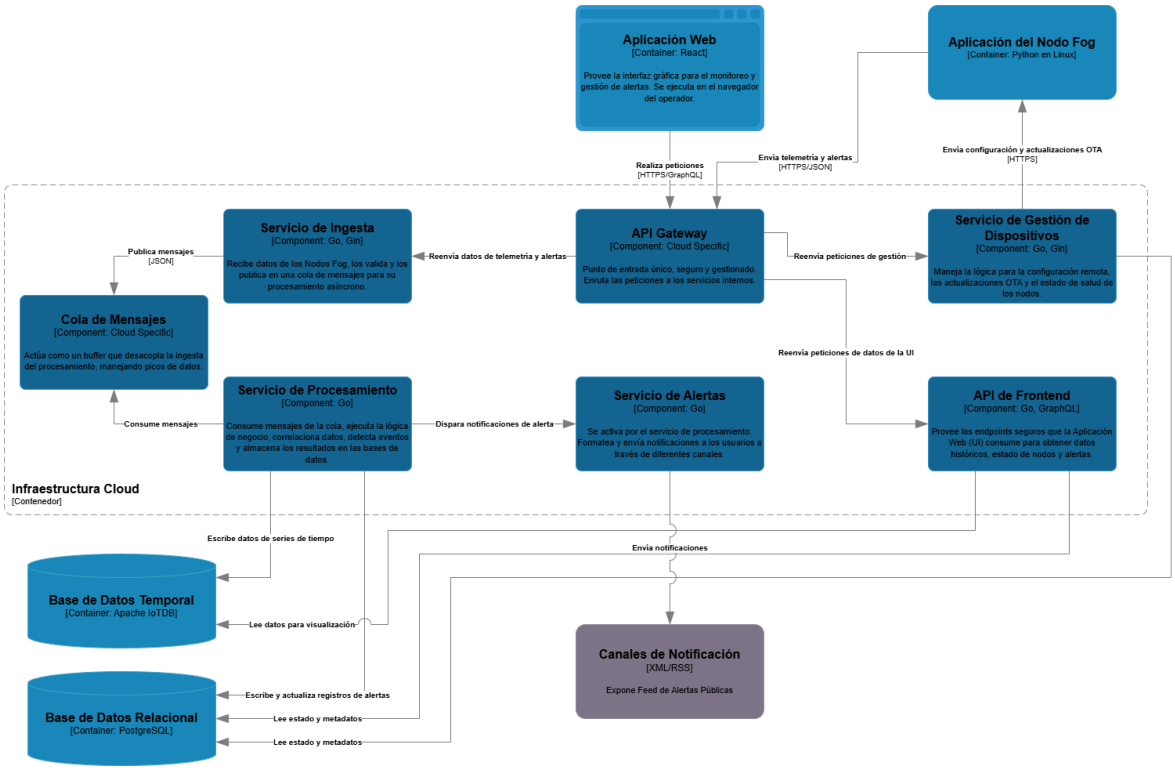


Figura 5: Diagrama C4 Nivel 3 Backend

- **Arquitectura: Microservicios Orientados a Eventos (Serverless).**
    - Se adopta una arquitectura de **microservicios**, descomponiendo el backend en servicios **pequeños y autónomos** (Newman, 2015; Amazon Web Services, s.f.). Esto permite **escalabilidad independiente** (RNF-07), **mayor resiliencia** (RNF-04) al aislar fallos, y **desarrollo/despliegue más ágil** (RNF-08) (Newman, 2015; Amazon Web Services, s.f.). El enfoque es adecuado para plataformas **IoT** distribuidas (Nguyen et al., 2022) y se complementa con orientación a eventos para bajo acoplamiento.

- **Lenguaje: Un lenguaje compilado y concurrente.**

- RNF-07 y RNF-08. El modelo de concurrencia ligera es esencial para la ingesta de alta concurrencia de IoT (Sichevskyi, 2025). La eficiencia de recursos (CPU/memoria) de un lenguaje compilado reduce el TCO de la infraestructura en la nube (Luong, 2022).

- **Bases de Datos**

  - **Una TSDB con escalabilidad horizontal nativa y de código abierto**Los datos generados por los sensores son inherentemente **series temporales** (mediciones indexadas por tiempo). Para su almacenamiento y análisis eficiente (RNF-09), se requiere una **Base de Datos de Series Temporales (TSDB)** (McBride & Reynolds, 2020). Las TSDBs están **optimizadas** para cargas de trabajo con **alta velocidad de ingesta** y **consultas basadas en rangos de tiempo**, superando a las RDBMS tradicionales en este dominio (McBride & Reynolds, 2020; Liu et al., 2024).

  - **Un RDBMS objeto-relacional con capacidades geoespaciales avanzadas.**

    - Se requiere un **RDBMS** para gestionar datos transaccionales y de estado (dispositivos, usuarios, alertas) con garantías **ACID** (RNF-09, RNF-11, RNF-12) (Amazon Web Services, s.f.-a). Adicionalmente, se necesita soporte **geoespacial** (RNF-06) para almacenar y consultar ubicaciones eficientemente, permitiendo análisis espaciales complejos (Tjukanov, 2018). Se requiere soporte para el tipo *GEOGRAPHY* para cálculos geodésicos precisos (The PostGIS Development Group, s. f.).

- **API de Frontend: Una API basada en GraphQL.**

  - RNF-10. Superior a REST para dashboards complejos, ya que elimina el over-fetching y under-fetching (China, 2025). Su soporte nativo para Suscripciones (Subscriptions) es la tecnología habilitante clave para las alertas y actualizaciones de estado en tiempo real (Hasura, 2025).

- **Aplicación Web: Librería de UI con un ecosistema maduro de visualización geoespacial.**

  - Se especifica una **Single-Page Application (SPA)** para el frontend. En una SPA, se carga una única página HTML inicial y el contenido se actualiza dinámicamente sin recargas completas (Alam, 2024). Esto proporciona una **experiencia de usuario fluida, rápida y responsiva**, similar a la de una aplicación de escritorio, lo cual es crucial para la **usabilidad** (RNF-10) en interfaces de monitoreo en tiempo real (Alam, 2024). Se requiere una librería de visualización acelerada por WebGL para cumplir el criterio de rendimiento con alta densidad de datos (RNF-10).

3.5 SELECCIÓN DE TECNOLOGÍAS

Mientras que la sección anterior justificó las *clases* de tecnología requeridas, esta sección detalla las *implementaciones específicas* seleccionadas para cumplir con los requisitos del sistema, diferenciando la selección óptima para producción de la selección pragmática para las pruebas de laboratorio iniciales.

3.5.1 Despliegue en Producción

La selección para producción se optimiza para el TCO a 10-15 años, la máxima fiabilidad (RNF-04, RNF-05) y la escalabilidad (RNF-07).

Categoría	Componente	Precio (USD)
MCU	ESP32-S3-WROOM-1-N8R8	$4.65
Gestión de Energía	TI BQ25570 PMIC	$5.18
	Supercondensador EDLC	
Sensor de Gas	Bosch BME688	$6.65
Sensor de Partículas	Bosch BMV080	$45.00
Sensor de Llama IR	KEMET QFCE	$18.00
Protocolo Mesh	Wirepas Mesh	N/A
SUBTOTAL NODO SENSOR		**$79.48**

Tabla 4: Costo Nodo Sensor Producción

Categoría	Componente	Precio (USD)
SBC	Radxa CM3J + Carrier Board	$105.00
Backhaul Primario	Quectel EG25-G (4G/LTE)	$60.00
Backhaul Secundario	Swarm M138 Kit (Satelital)	$198.00
SUBTOTAL NODO FOG		**$363.00**

Tabla 5: Costo Nodo Fog Producción

Firmware Nodo Sensor:

- **MCU (ESP32-S3)**. Proporciona la potencia de cómputo de doble núcleo y extensiones de IA necesarias para la lógica de fusión en el borde y la futura ejecución de modelos de IA (Espressif Systems, 2025).

- **Gestión de Energía (TI BQ25570 + Supercondensador)**: El PMIC de nano-potencia TI BQ25570 gestiona la recolección de energía solar. El almacenamiento en Supercondensador EDLC se elige sobre las baterías de litio por su inmunidad a fallos catastróficos a bajas temperaturas y su vida útil de 10-15 años, satisfaciendo el requisito de autonomía (RNF-02).

- **Sensores (BME688, BMV080, QFCE):** El sensor de gas Bosch BME688 y el de partículas Bosch BMV080 de alta gama aseguran la precisión y un alto tiempo medio entre fallos (MTTF). El sensor de llama IR KEMET QFCE es indispensable para la confirmación positiva de ignición.

- **Red de Malla (Wirepas Mesh):** Para el despliegue en producción, se requiere un protocolo de red mesh de grado industrial que garantice alta fiabilidad, escalabilidad masiva y eficiencia energética (RNF-04, RNF-07). Se selecciona Wirepas Mesh[5] porque utiliza un protocolo de enrutamiento descentralizado y optimizado, diseñado específicamente para redes IoT a gran escala, densas y de bajo consumo, superando las limitaciones inherentes a enfoques más simples como la inundación básica (Wirepas, s.f; Wong et al., 2024).

- **SBC (Radxa CM3J):** Seleccionado por su rango de temperatura industrial (-40°C a 85°C), almacenamiento **eMMC integrado** (fiabilidad crítica, RNF-04) y su **Unidad de Procesamiento Neuronal (NPU)** de 1 TOPS para Edge AI avanzado en el futuro.

- **Backhaul (Quectel EG25-G + Swarm M138):** Combinación híbrida de 4G/LTE (primario) y satelital LEO (respaldo) que garantiza la máxima resiliencia y diversidad de ruta (RNF-04).

Plataforma Backend (Nube):

- **Lenguaje/Framework (Go con el framework Gin).** Para cumplir los requisitos RNF-07 y RNF-08, se elige un lenguaje compilado con un modelo de concurrencia eficiente. Benchmarks independientes demuestran consistentemente que Go (usando Gin o Fiber) ofrece un **rendimiento significativamente superior** en cargas de trabajo de API REST en comparación con Python (usando FastAPI), a menudo por un **orden de magnitud** (TechEmpower, 2024).

- **TSDB (Apache IoTDB):** Se selecciona Apache IoTDB, una TSDB nativa de **código abierto**, por su **rendimiento superior en ingesta y mayor eficiencia de almacenamiento** en comparación con alternativas *open-core* como InfluxDB o TimescaleDB, especialmente a medida que aumenta el número de dispositivos (Liu et al., 2024; Wang et al., 2023). Esto cumple con el requisito de escalabilidad (RNF-07) y evita el *vendor lock-in* (Liu et al., 2024).

[5] Wirepas Mesh es una tecnología propietaria con un modelo de licenciamiento, factor a considerar en el TCO. Sin embargo, es una elección adecuada para cumplir los exigentes requisitos de una aplicación crítica.

- **RDBMS (PostgreSQL)**: Se selecciona **PostgreSQL** por su reconocida **robustez y conformidad ACID** (Amazon Web Services, s.f.-a), complementado con la extensión **PostGIS** para capacidades **geoespaciales avanzadas** estándar en la industria *open source*, incluyendo soporte para el tipo *GEOGRAPHY* (Tjukanov, 2018; The PostGIS Development Group, s. f.).
- **API: GraphQL** (implementado con una librería como *gqlgen* para Go).
- **Frontend: React** (con **Apollo Client** para datos, **Zustand** para estado local, y **deck.gl** para visualización geoespacial).

3.5.2 Selección para Pruebas de Laboratorio

La selección para el piloto (PoC) prioriza la velocidad de desarrollo, la facilidad de depuración y el bajo coste inicial (CAPEX) sobre la optimización a largo plazo.

Categoría	Componente	Precio (USD)
MCU	Heltec Wireless Stick Lite V3	$11.12
Módulo de Carga	TP4056	$0.80
Batería	18650 (3500mAh)	$3.79
Sensor de Gas	Bosch BME688	$13.00
Sensor de Partículas	Plantower PMS5003	$25.00
Sensor de Llama IR	KY-026	$1.50
Protocolo Mesh	Meshtastic	N/A
SUBTOTAL NODO SENSOR		**$55.21**

Tabla 6: Costo Nodo Sensor Desarrollo

Categoría	Componente	Precio (USD)
SBC	Raspberry Pi 4B (4GB)	$55.00
Almacenamiento	MicroSD Industrial 32GB	$8.00
Backhaul Primario	ZTE MF833V 4G/LTE	$20.00
SUBTOTAL NODO FOG		**$83.00**

Tabla 7: Costo Nodo Fog Desarrollo

- **MCU (Heltec Wireless Stick Lite V3):** Esto es más económico y ofrece una compatibilidad inherente con el ecosistema de **Meshtastic** y el potencial de cómputo Edge AI del ESP32-S3.

- **Gestión de Energía (TP4056 + 18650):** Se reemplaza la compleja solución de recolección de energía por un módulo de carga **TP4056** de ultra bajo costo ($0.80 USD) y una batería recargable **18650** ($3.79 USD). Esto simplifica las pruebas de laboratorio, donde la autonomía a largo plazo es secundaria.

- **Sensores (BME688, PMS5003, KY-026):** Se utiliza un **BME688** genérico ($13.00 USD). Los sensores **Plantower PMS5003** (Partículas) y el **Módulo IR Genérico** (Llama) son alternativas de bajo costo que mantienen la funcionalidad básica para validar la lógica de multifirma.

- **Red de Malla (Meshtastic):** Su naturaleza de código abierto, comunidad activa y facilidad de configuración en hardware accesible (Meshtastic, s.f) lo convierten en la opción *de facto* para agilizar el desarrollo y las pruebas iniciales con bajo costo. Sin embargo, no es una selección óptima para producción, ya que opera usando *managed flooding* (TheBentern & Guvwaf, 2024; Suryadevara & Dutta, 2022). Las limitaciones de los protocolos basados en inundación en redes densas están bien documentadas (Wong et al., 2024; Joy & Branch, 2024), así como las vulnerabilidades de seguridad de su modelo PSK (Messina et al., 2024).

- **SBC (Raspberry Pi 4B):** Su ecosistema y comunidad inigualables reducen el "coeficiente de fricción" del desarrollo y la depuración del software del Fog. El SBC utiliza **MicroSD** en lugar de eMMC, un compromiso aceptable para el entorno no crítico del piloto.

- **Backhaul (ZTE MF833V):** Esta solución monolítica es compatible con Linux y simplifica la integración del *networking* (visto como una interfaz Ethernet) con el Nodo Fog.

3.5.3 Modelo y Volumen de Datos

La selección de tecnologías realizadas anteriormente define los modelos de datos y los formatos de comunicación.

3.5.3.1 Modelo de Datos Relacional

El modelo relacional (Persistencia Operacional) actúa como el sistema de registro central para los metadatos y la información estructural. Se centra en definir *qué* dispositivos existen, *dónde* se encuentran y *cómo* se gestionan los eventos de alerta.Las entidades clave de este modelo son:

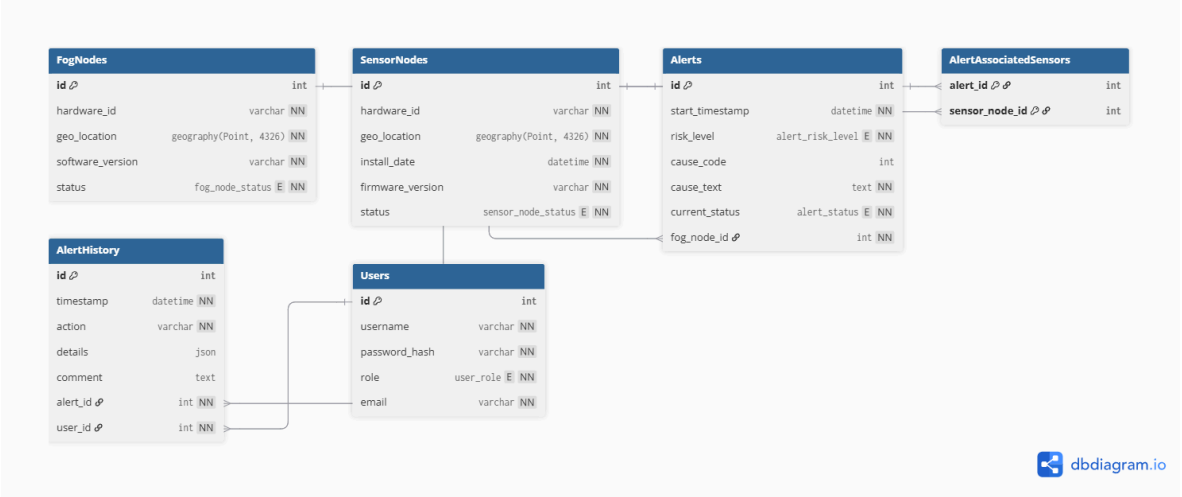


Figura 6: Modelo Entidad-Relación

- ***Entidades de Dispositivos (FogNodes, SensorNodes):***
  Almacenan los metadatos de los dispositivos físicos. Se utiliza una **clave primaria sustituta** (***id***) para optimizar el rendimiento de las uniones (***joins***) y una **clave natural única** (***hardware_id)*** para identificar al dispositivo físico. Este enfoque dual es fundamental para la **Mantenibilidad (RNF-08)**, ya que permite el reemplazo de hardware sin perder la continuidad de los datos históricos. El campo ***geo_location*** se implementa utilizando el tipo de dato nativo ***geography(Point, 4326)*** **de PostGIS**. (The PostGIS Development Group, s. f.).

- **Uso de Tipos Enumerados (ENUM)**: Para garantizar la integridad y consistencia de los datos utiliza **tipos enumerados** para restringir los valores posibles a un conjunto predefinido, eliminando errores de tipeo y simplificando la lógica de la aplicación. Se aplica en los campos ***status*** (***FogNodes***, ***SensorNodes***), ***risk_level*** y ***current_status*** (***Alerts***), y ***role*** (***Users***).

- **Subsistema de Alertas (*Alerts, AlertHistory, AlertAssociatedSensors*):**
  Se implementa un modelo de gestión de incidentes.

  - ***Alerts*** registra el estado actual del evento.
  - ***AlertHistory*** funciona como un log inmutable que audita cada cambio de estado, cumpliendo con RNF-12 (Auditabilidad).
  - ***AlertAssociatedSensors*** vincula una alerta con el clúster de sensores que contribuyeron a su generación.

3.4.6 Modelo de Datos para Series de Tiempo

La Persistencia Temporal utiliza un modelo jerárquico optimizado para el almacenamiento y consulta eficiente de datos de series temporales (The Apache Software Foundation, 2025). La estructura se define mediante rutas, similar a un sistema de archivos:

root.{storage_group}.{device_type}.{device_id}.{measurement}:

La clave para la integración de la persistencia políglota es que el *id* del dispositivo en PostgreSQL se utiliza para construir la ruta en la TSDB, sirviendo de puente entre los metadatos y los datos de series de tiempo.

Rutas de Ejemplo:

- **root.wildfire_system.sensor.101.temperature**
- **root.wildfire_system.sensor.101.co**
- **root.wildfire_system.sensortelemetry.101.battery_voltage**
- **root.wildfire_system.fogtelemetry.22.cpu_usage_percent**

Este diseño permite que las consultas de series de tiempo se realicen directamente en IoTDB con un rendimiento óptimo, mientras que PostgreSQL se encarga de las consultas complejas que involucran metadatos, relaciones y datos geoespaciales.

3.4.7 Volumen de Datos y Formato de Serialización

Para validar la escalabilidad (RNF-07), es esencial optimizar el tamaño de la carga útil (payload). La elección de un formato de serialización binario sobre JSON es una decisión deliberada para minimizar el Tiempo en el Aire (ToA) y el consumo de energía (RNF-02) (Popić et al., 2016; Viotti & Kinderkhedia, 2022).

Se selecciona **Protocol Buffers (Protobuf)** sobre alternativas como CBOR. Protobuf impone un esquema riguroso, lo que garantiza la robustez de los datos (RNF-11) y la compatibilidad de versiones (RNF-08), y produce una carga útil binaria más compacta al reemplazar las claves de texto con etiquetas numéricas (Google, 2025).

- **Estimación de Carga Útil:** Para un paquete de datos de sensor típico (ID, timestamp, 3-4 lecturas de sensor), el tamaño de la carga útil se estima en **~25 bytes**.
- **Estimación de Volumen:**
    - ***Parámetros:*** 20 nodos sensores; 1 medición cada 15 minutos (96 mediciones/nodo/día).

- ***Cálculo por Nodo:*** 25 bytes/medición × 96 mediciones/día = 2,400 bytes/día/nodo (2.4 KB)
- ***Cálculo Total (Día):*** 2.4 KB/nodo × 20 nodos = 48 KB/día
- ***Cálculo Total (Mes):*** 48 KB/día × 30 días = ~1.44 MB/mes

Este volumen de datos extremadamente bajo válida la eficiencia de la arquitectura de comunicación y confirma que los costos de ingesta y almacenamiento de datos en la nube serán mínimos.

3.4.8 Estrategia de Despliegue Físico

La estrategia de despliegue físico (RNF-08) se deriva del rango de detección efectiva de los sensores (Sooriarachchi & Jayakody, 2024). El observable más relevante para la detección temprana a distancia es el humo. Estudios sobre la optimización de WSN para monitoreo de incendios indican que las distancias de detección típicas para sensores de humo varían entre 10 y 100 metros (Gómez-González et al., 2025). Favoreciendo una estrategia de colocación en rejilla hexagonal para maximizar la cobertura (Shi et al., 2020), se definen tres escenarios de despliegue basados en la densidad:

- **Alta densidad (ej. ZIUF críticas):** 4-5 nodos/hectárea.
- **Media Densidad (ej. Zonas de amortiguamiento):** 2-3 nodos/hectárea.
- **Baja Densidad (ej. Vigilancia forestal amplia):** 1 nodo/hectárea.

3.7 ALGORITMO DE DETECCIÓN

La decisión de ubicar la lógica de detección principal en el **Nodo Fog** es fundamental y se basa en los principios del Fog Computing (Bonomi et al., 2012; Yi et al., 2015). Los beneficios son determinantes:

- **Reducción Crítica de la Latencia**: El procesamiento en el borde elimina el retardo de red inaceptable de enviar datos brutos a la nube (Shi et al., 2016).
- **Ahorro de Ancho de Banda**: El Nodo Fog actúa como un filtro inteligente, enviando solo información relevante y consolidada a la nube (Yi et al., 2015; Moussa et al., 2022).
- **Aumento de la Resiliencia y Operación Autónoma**: El sistema puede seguir operando de forma autónoma incluso si se pierde la conexión con la nube, garantizando la continuidad del servicio (Yi et al., 2015).

3.7.1 Análisis Comparativo

A continuación, se presentan y analizan cuatro estrategias alternativas para la implementación del algoritmo de detección en el Nodo Fog: un enfoque basado en reglas heurísticas, uno basado en fusión probabilística, uno basado en lógica difusa y, finalmente, uno basado en aprendizaje automático.

3.7.1.1 Reglas Heurísticas

El enfoque basado en reglas heurísticas es la estrategia más directa para la detección de incendios en un sistema multisensorial. Este método se basa en la definición de un conjunto de reglas lógicas y umbrales predefinidos que, al cumplirse, activan una alarma. Estos sistemas pueden variar en complejidad, desde reglas de umbral simple hasta modelos físico-matemáticos más elaborados.

La forma más básica consiste en definir condiciones explícitas, generalmente en formato **SI-ENTONCES (IF-THEN)**, que combinan las lecturas de los sensores. La lógica fundamental reside en la fusión de datos de múltiples sensores para crear una **"multi-firma"** del evento, lo que permite una detección más robusta y una reducción significativa de las falsas alarmas en comparación con los sistemas que dependen de un único sensor (Gottuk et al., 2002). Por ejemplo, una regla simple podría ser: *SI la [temperatura > 50°C] Y la [concentración de CO > 30 ppm] ENTONCES activar_alarma*. Esta combinación de firmas es mucho más fiable que basarse únicamente en un umbral de temperatura, ya que muchas fuentes de falsas alarmas (como el calor ambiental) no producen monóxido de carbono (Gottuk et al., 2002).

Una implementación más sofisticada de este enfoque son los **sistemas de índices de riesgo de incendio**, que utilizan un conjunto de ecuaciones matemáticas predefinidas para combinar múltiples variables ambientales y producir un único valor de riesgo. Un ejemplo prominente es el **Fire Weather Index (FWI) System** de Canadá, un modelo meteorológico que calcula el riesgo de incendio a partir de mediciones de temperatura, humedad relativa, velocidad del viento y precipitación (Hefeeda & Bagheri, 2007). Este tipo de sistema heurístico, respaldado por décadas de investigación forestal, ofrece una evaluación del peligro de incendio más completa y contextualizada que los umbrales simples (Hefeeda & Bagheri, 2007; Bouabdellah et al., 2013).

Ventajas:

- **Simplicidad y Bajo Costo Computacional**: Los algoritmos basados en reglas son fáciles de implementar y requieren muy pocos recursos de CPU y memoria. Esto los hace ideales para ser ejecutados en dispositivos de borde con capacidades limitadas, como el Nodo Fog de esta arquitectura (Kizilkaya et al., 2022).
- **Interpretabilidad**: Las reglas y ecuaciones son explícitas y fáciles de entender por un operador humano, lo que facilita su ajuste, depuración y validación.

- **Rapidez**: La evaluación de reglas lógicas y ecuaciones matemáticas es extremadamente rápida, lo que garantiza una latencia de detección mínima, cumpliendo con el requisito de una alerta temprana.

Desventajas:

- **Rigidez y Calibración Manual**: Las reglas, umbrales y ecuaciones son estáticos y deben ser definidos manualmente por expertos. Un conjunto de parámetros que funciona bien en un entorno puede no ser adecuado para otro, lo que requiere una calibración cuidadosa para cada despliegue (Liang et al., 2024).
- **Sensibilidad a Falsas Alarmas**: Aunque la fusión de datos reduce las falsas alarmas, el sistema sigue siendo vulnerable si los umbrales no están bien ajustados. Fenómenos no previstos que imitan la firma de un incendio pueden seguir activando alertas incorrectas.
- **Incapacidad de Aprender**: Este enfoque no puede adaptarse a nuevas condiciones o a patrones de eventos no contemplados en las reglas iniciales. No tiene capacidad de aprendizaje a partir de datos históricos.

3.7.1.2 Fusión Probabilística

Este método utiliza modelos estadísticos para estimar la probabilidad de que ocurra un incendio basándose en las lecturas de los sensores. En lugar de depender de umbrales fijos, cada medición de un sensor contribuye a una función de probabilidad que evalúa el riesgo. Este enfoque, eminentemente centrado en los datos (*data-centric*), permite una gestión más dinámica de la información (Ramachandran et al., 2008).

Un sistema de este tipo puede dividir la red de sensores en "zonas" y asignar probabilidades de ocurrencia de incendio a cada una. Luego, estas probabilidades pueden agregarse para obtener una estimación global del riesgo. Metodologías específicas como la Teoría de Dempster-Shafer han sido propuestas para este fin, permitiendo fusionar la "evidencia" proveniente de múltiples sensores (ej. temperatura y humedad) para calcular una creencia combinada sobre la hipótesis de un incendio (Díaz-Ramírez et al., 2012). Al modelar la detección como un problema probabilístico, se puede manejar de forma inherente la incertidumbre y el ruido de los datos (Ramachandran et al., 2008).

Ventajas:

- **Manejo robusto de la incertidumbre:** Es su principal fortaleza, ya que está diseñado matemáticamente para trabajar con datos ruidosos e inciertos.
- **Fundamento estadístico:** Las decisiones se basan en un modelo estadístico riguroso, lo que puede proporcionar una mayor confianza en las alertas generadas.

Desventajas:

- **Complejidad del modelo:** Definir y validar un modelo probabilístico preciso puede ser más complejo que establecer reglas simples.
  No es un sistema de aprendizaje: Al igual que los métodos heurísticos, los modelos probabilísticos son estáticos y no se adaptan automáticamente a nuevos patrones de datos.

3.7.1.3 Lógica Difusa

Este enfoque traduce las mediciones numéricas continuas de los sensores (ej. 45°C) a conceptos lingüísticos cualitativos (ej. "temperatura alta") con ciertos **grados de pertenencia**. Esto permite modelar la imprecisión y la gradualidad del mundo real, donde las transiciones entre estados no son abruptas (Bolourchi & Uysal, 2013; Khalid et al., 2019). Un sistema de inferencia difuso (*Fuzzy Inference System*) opera en tres etapas:

- **Fuzzificación:** Las entradas numéricas de los sensores (ej. temperatura, humo) se convierten en valores difusos utilizando **funciones de membresía** (ej. una temperatura de 45°C puede ser 70% "Alta" y 30% "Media").

- **Inferencia basada en reglas:** Se aplica un conjunto de reglas lingüísticas, similares a las del enfoque heurístico, pero que operan sobre los valores difusos. Por ejemplo: *SI la [Temperatura es Alta] Y el [Humo es Denso] ENTONCES la [Probabilidad de Fuego es Muy Alta]* (Bolourchi & Uysal, 2013). El sistema evalúa todas las reglas en paralelo para determinar un resultado difuso.

- **Defuzificación:** El resultado difuso agregado se convierte de nuevo en un valor numérico preciso (ej. una probabilidad de incendio del 95%) para la toma de decisiones (Khalid et al., 2019).

Para manejar niveles aún mayores de incertidumbre, se han propuesto sistemas de **Lógica Difusa de Tipo-2**, que utilizan funciones de membresía que son ellas mismas difusas, permitiendo modelar la incertidumbre sobre la definición exacta de conceptos como "temperatura alta" (Singh & Singh, 2012).

Ventajas:

- **Flexibilidad y Suavidad en la Decisión**: Evita las decisiones abruptas de los umbrales fijos, proporcionando una respuesta más gradual y estable, lo que puede reducir falsas alarmas por fluctuaciones momentáneas.

- **Basado en el Conocimiento Experto**: Las reglas se basan en el conocimiento humano de cómo se comporta un incendio, lo que hace que el sistema sea interpretable.

Desventajas:

- **Complejidad en el Diseño**: La definición de las funciones de membresía y el conjunto de reglas puede ser compleja y subjetiva, requiriendo un ajuste fino para un rendimiento óptimo (Bolourchi & Uysal, 2013).
- **Costo Computacional Moderado:** Aunque es viable para dispositivos de borde, es computacionalmente más intensivo que un simple conjunto de reglas heurísticas.

3.7.1.4 Aprendizaje Automático

Un enfoque alternativo para la detección de incendios consiste en el uso de **Aprendizaje Automático (*Machine Learning* - *ML*)**. A diferencia de los sistemas basados en reglas predefinidas, un modelo de ML tiene la capacidad de "aprender" los patrones complejos y no lineales que caracterizan a un incendio directamente desde los datos de los sensores. Esto permite una detección más precisa y adaptable, superando la rigidez de los enfoques heurísticos y de lógica difusa.

El proceso típicamente se divide en dos fases. Primero, un modelo —como una **Red Neuronal Artificial (ANN)**, una **Máquina de Vectores de Soporte (SVM)** o modelos más complejos de **Deep Learning** como las redes neuronales recurrentes (LSTM)— se entrena fuera de línea utilizando un gran conjunto de datos históricos que contiene ejemplos tanto de condiciones normales como de incendios reales (Chauhan et al., 2013; Dampage et al., 2022; Almasoud, 2022). Durante este entrenamiento, el modelo ajusta sus parámetros internos para minimizar el error de predicción. Una vez entrenado, el modelo optimizado se despliega en el Nodo Fog para la **inferencia**, donde procesa los datos de los sensores en tiempo real para clasificarlos como "fuego" o "no fuego" (Dampage et al., 2022).

La evolución de los sistemas de ML (*MLSys*) ha permitido que estos modelos, antes confinados a potentes servidores, puedan ejecutarse de manera eficiente en el borde de la red (Alistarh et al., 2019). Más aún, el emergente campo de **TinyML** demuestra la viabilidad de ejecutar modelos de *deep learning* en microcontroladores de ultra bajo consumo, con tamaños de modelo de apenas unos pocos kilobytes. Esto se logra mediante herramientas como *TensorFlow Lite for Microcontrollers*, que optimizan las redes neuronales para operar con recursos mínimos (Warden & Situnayake, 2019). Esta tendencia no sólo valida la estrategia de ejecutar la inferencia en el Nodo Fog, sino que también ofrece beneficios adicionales como una mayor eficiencia energética y una mejor privacidad, al procesar los datos localmente sin necesidad de transmitirlos a la nube (Yadav et al., 2024).

Ventajas:

- **Alta Precisión y Adaptabilidad**: Los modelos de ML pueden capturar relaciones sutiles y complejas entre las diferentes variables de los sensores, lo que conduce a una mayor precisión y a una menor tasa de falsas alarmas (Chauhan et al., 2013).

- **Capacidad de Generalización**: Un modelo bien entrenado puede generalizar su conocimiento a nuevas situaciones y entornos que no estaban presentes en los datos de entrenamiento, ofreciendo una detección más robusta.
- **Automatización del Diseño de Lógica**: El modelo aprende las "reglas" de detección por sí mismo, eliminando la necesidad de que un experto las diseñe y calibre manualmente.

Desventajas:

- **Dependencia de los Datos**: El rendimiento del modelo depende críticamente de la calidad y cantidad de los datos de entrenamiento. Se requiere un conjunto de datos grande, diverso y correctamente etiquetado, lo cual puede ser difícil de obtener.
- **Costo Computacional**: El entrenamiento de modelos de ML es computacionalmente muy intensivo y debe realizarse en la nube o en servidores potentes. Aunque la inferencia es más ligera, sigue requiriendo más recursos en el Nodo Fog que los enfoques basados en reglas.
- **Naturaleza de "Caja Negra":** Especialmente en el caso de las redes neuronales profundas, puede ser difícil interpretar por qué el modelo ha tomado una decisión específica, lo que complica la depuración y la validación de su comportamiento.

3.7.3 Selección de Lógica de Detección

Tras el análisis comparativo de las estrategias de detección, se concluye que un enfoque basado en **reglas heurísticas** representa la opción más pragmática y robusta para la fase inicial del sistema. Esta decisión se fundamenta en el **costo computacional de orden de magnitud** que prioriza la viabilidad, la interpretabilidad y la rapidez de ejecución en el hardware del Nodo Fog.

Un algoritmo heurístico, como el que se propone en este diseño, se basa en un conjunto de ecuaciones matemáticas y reglas lógicas. La carga computacional para una ejecución de este tipo es del orden de **10^3 a 10^4 operaciones de punto flotante (FLOPs)** y su huella de memoria es inferior a **1 MB**[6]. En contraste, un enfoque basado en *Machine Learning*, incluso uno optimizado para el borde de la red, presenta una demanda de recursos varios órdenes de magnitud superior. Por ejemplo:

- **Modelos para Microcontroladores (TinyML):** Un modelo de detección de palabras clave optimizado con TensorFlow Lite, diseñado para dispositivos de muy baja

[6] Estimación de orden de magnitud derivada del análisis de la complejidad inherente al algoritmo propuesto, que se compone de un número finito de operaciones algebraicas y comparaciones lógicas.

potencia, puede requerir una memoria de trabajo de **25 KB** y ejecutar decenas de miles de operaciones por cada inferencia (Warden & Situnayake, 2019).

- **Modelos de Visión por Computador Ligeros:** Un modelo como YOLOX, adaptado para la detección de incendios en imágenes, puede tener más de **9 millones de parámetros** y requerir **2.5 GigaFLOPs** (2.5×10^9 operaciones) por cada inferencia (Luan et al., 2024).

Esta diferencia de **3 a 5 órdenes de magnitud** en la carga computacional válida la elección del enfoque heurístico como la solución más eficiente para garantizar una operación de baja latencia y bajo consumo en un dispositivo de borde.

Si bien los enfoques de Aprendizaje Automático (ML) demuestran un mayor potencial de precisión en estudios comparativos (Hadisuwito & Hassan, 2020; Shmuel & Heifetz, 2023), su implementación se descarta para la fase inicial debido a su inviabilidad computacional y a la alta dependencia de grandes volúmenes de datos de entrenamiento. De manera similar, los métodos de fusión probabilística y lógica difusa, aunque robustos, requieren un diseño subjetivo y un ajuste fino considerable.

El enfoque heurístico, en cambio, permite una implementación directa basada en modelos físico-matemáticos ya validados. El **Sistema Canadiense de Índice Meteorológico de Incendios (FWI System)** se identifica como un modelo robusto y pertinente, cuya idoneidad se ve reforzada por investigaciones locales que lo han adaptado a las condiciones de Viña del Mar (Castillo, 2019). No obstante, es crucial entender que el FWI es un indicador de peligro (qué tan propenso está el combustible para arder), no un detector de ignición. Por lo tanto, se propone un **algoritmo heurístico híbrido de dos etapas**:

1. **Etapa 1: Análisis de Riesgo Contextual:** El Nodo Fog calculará en tiempo real el FWI utilizando los datos de sus sensores. Esto transforma al FWI de una herramienta regional a un indicador de riesgo hiperlocal, estableciendo el contexto de peligro para la zona inmediata.
2. **Etapa 2: Confirmación de Ignición:** El sistema utilizará el nivel de riesgo del FWI para ajustar su sensibilidad. Se implementará una regla de "multi-firma", que corresponde a la implementación del modelo de fusión a nivel de decisión, para la detección del evento, basada en la fusión de datos de humo (PM2.5), gases (CO) y la confirmación visual del sensor de llama IR, una metodología cuya eficacia ha sido validada en sistemas de WSN jerárquicos (Molina-Pico et al., 2016) y en estudios de campo que correlacionan picos de contaminantes con incendios reales (Lertsinsrubtavee et al., 2023).

CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN

Este capítulo detalla la estrategia y el plan para validar la arquitectura propuesta, con el objetivo de demostrar que el diseño cumple con los Requerimientos No Funcionales (RNF) más críticos definidos en el Capítulo 4. La validación se enfoca en verificar la funcionalidad, resiliencia, seguridad y precisión del sistema.

4.1 ESTRATEGIA DE VALIDACIÓN

Dado que un despliegue a gran escala está fuera del alcance de esta memoria, la estrategia de validación se basa en un enfoque mixto que combina pruebas empíricas en un entorno controlado con análisis teóricos basados en el diseño:

- **Pruebas de Concepto (PoC):** Se propone la construcción de un prototipo a escala reducida, compuesto por dos Nodos Sensores y un Nodo Fog. Este prototipo permitirá realizar pruebas funcionales de los componentes clave de la arquitectura en un entorno de laboratorio.
- **Validación por Diseño y Análisis:** Para requerimientos difíciles de medir empíricamente en un corto período (como la autonomía a largo plazo), la validación se basará en los cálculos de ingeniería y las especificaciones técnicas detalladas en el diseño.
- **Verificación de Cumplimiento de Estándares:** Se demostrará que los formatos de datos y protocolos de comunicación propuestos se adhieren a los estándares abiertos definidos, garantizando la interoperabilidad.

4.2 PLAN DE PRUEBAS Y CRITERIOS DE ÉXITO

El siguiente plan de pruebas establece una trazabilidad directa entre cada Requerimiento No Funcional crítico y un método de validación específico, junto con su criterio de éxito medible.

4.2.1 Validación de Precisión de Detección (RNF-05)

El objetivo de esta prueba es validar que el algoritmo de "multi-firma" implementado en el Nodo Fog puede distinguir eficazmente un evento de incendio simulado de una falsa alarma.

- **Método de Validación:** La prueba se realizará mediante una Prueba de Concepto (PoC) en el prototipo. Se simularon dos escenarios distintos en un entorno controlado:

1. **Escenario de Incendio Simulado:** Se utilizará una fuente de calor y un generador de humo para activar simultáneamente los sensores de temperatura, material particulado (PM2.5) y monóxido de carbono (CO).
2. **Escenario de Falsa Alarma Simulada:** Se utilizará únicamente la fuente de calor para provocar un aumento anómalo solo en el sensor de temperatura, sin activar los sensores de humo y gases.

- **Criterio de Éxito:** El sistema superará la prueba si el Nodo Fog genera y registra una alerta formal únicamente en el Escenario 1. En el Escenario 2, el sistema debe registrar las lecturas anómalas de temperatura pero no debe generar una alerta de incendio, demostrando la eficacia del algoritmo de fusión de datos.

4.2.2 Validación de Resiliencia Operacional (RNF-04)

El objetivo es verificar que el Nodo Fog es capaz de operar de forma autónoma, almacenando datos localmente si pierde la conexión con los servicios en la nube para prevenir la pérdida de información.

- **Método de Validación:** Se utilizará el prototipo en funcionamiento normal, transmitiendo datos de los sensores al backend. Se procederá a desconectar físicamente el cable de red del Nodo Fog, simulando una caída de la conexión a internet. Se dejará el sistema operando en este estado durante cinco minutos, permitiendo que los Nodos Sensores continúen enviando datos al Nodo Fog. Finalmente, se conectará el cable de red.
- **Criterio de Éxito:** La validación será exitosa si, tras restablecer la conexión, los registros del backend muestran la recepción de todos los datos acumulados durante el período de desconexión. Adicionalmente, se deberá poder consultar la base de datos SQLite del Nodo Fog para verificar que los registros fueron almacenados temporalmente y luego marcados como "enviados".

4.2.3 Validación de Baja Latencia de Alerta (RNF-01)

Esta prueba busca medir la latencia de la red local, es decir, el tiempo transcurrido desde que un sensor detecta un evento hasta que el Nodo Fog genera la alerta local.

- **Método de Validación:** Se requiere una modificación menor en el software del prototipo. Se añadirá la inclusión de marcas de tiempo (timestamps) de alta precisión en dos puntos: el firmware del Nodo Sensor registrará t1 al momento de enviar un paquete de datos anómalo, y la aplicación del Nodo Fog registrará t3 al momento de confirmar una alerta tras procesar dicho paquete. Se ejecutará el "Incendio Simulado" para gatillar el evento.

- **Criterio de Éxito:** La prueba se considerará superada si la diferencia (t3 - t1) es consistentemente inferior a 30 segundos[7], lo que demostraría la alta eficiencia de la red LoRa Mesh y la capacidad de procesamiento en tiempo real en el borde.

4.2.4 Validación de Seguridad Integral (RNF-11)

El propósito de esta prueba es confirmar empíricamente que la comunicación entre el Nodo Fog y el backend en la nube está debidamente cifrada, protegiendo la confidencialidad e integridad de los datos.

- **Método de Validación:** Se utilizará la herramienta de análisis de redes Wireshark para capturar el tráfico de red saliente desde el Nodo Fog hacia la API del backend mientras se transmiten datos de los sensores.
- **Criterio de Éxito:** La validación es exitosa si la inspección de los paquetes capturados en Wireshark muestra que el protocolo utilizado para la comunicación es TLSv1.3 y que el payload de los mensajes es ilegible. Esto validará el uso correcto de MQTTS y una comunicación segura.

4.2.5 Validación de Interoperabilidad (RNF-09)

Esta prueba tiene como objetivo demostrar que el sistema puede generar alertas en formatos estandarizados y abiertos, facilitando su integración con sistemas externos.

- **Método de Validación:** La validación se realizará en dos partes:
    1. **Protocolo de Alerta Común (CAP):** Se generará un archivo XML de ejemplo que siga rigurosamente la estructura de una alerta CAP (basado en la sección 2.5.2.1). Este archivo será subido a un validador de CAP en línea reconocido, como el proporcionado por Google Public Alerts.
    2. **RSS (Really Simple Syndication):** Se implementará el *endpoint* del *feed* RSS en la API del backend. Se utilizará un lector de RSS estándar (ej. Feedly, o un plugin de navegador) para suscribirse a dicho *endpoint* y visualizar las alertas generadas por el sistema.
- **Criterio de Éxito:** La prueba será exitosa si el validador en línea confirma que el archivo XML es un mensaje CAP 1.2 sintácticamente válido, y si el lector de RSS es capaz de suscribirse y mostrar correctamente el título, descripción y fecha de las alertas publicadas.

[7] Basado en tiempos teóricos de la cadena de comunicación LoRa (13s). Detección y Procesamiento (2s), Transmisión LoRa (3s), Procesamiento (1s), Backhaul (5s), Procesamiento Final (2s)

4.2.6 Validación de Autonomía Energética (RNF-02)

El objetivo de esta prueba es validar el **modelo de consumo energético** teórico presentado en el diseño, el cual proyecta una autonomía de batería superior a los 90 días.

- **Método de Validación:** Dado que una prueba empírica de 90 días está fuera del alcance de esta memoria, la validación se realizará mediante una combinación de **análisis por diseño y una prueba empírica del modelo de consumo**.

    a. **Análisis por Diseño:** La validación se apoya en el presupuesto energético detallado en el diseño, que sirve como hipótesis teórica a verificar.

    b. **Prueba Empírica del Modelo de Consumo:** Para comprobar si los valores teóricos del modelo son precisos en la práctica, se realizará una prueba de corta duración en el prototipo del Nodo Sensor. Con la batería completamente cargada, se medirá con un multímetro de precisión el consumo de corriente (en µA y mA) durante las dos fases críticas del ciclo de operación: la fase de **sueño profundo (*deep sleep*)** y la fase **activa**.

- **Criterio de Éxito:** La validación se considerará exitosa si los valores de consumo de corriente medidos empíricamente se encuentran dentro de un margen de tolerancia razonable (ej. ±15%) respecto a los valores especificados en las hojas de datos y utilizados en el presupuesto teórico. Confirmar que el consumo real en ambas fases es consistente con el modelo teórico otorgaría un alto grado de confianza a la proyección de autonomía a largo plazo de más de 90 días.

4.3 RESULTADOS ESPERADOS

Se espera que la ejecución de este plan de pruebas valide exitosamente los aspectos más innovadores y críticos de la arquitectura propuesta. La confirmación de la precisión en la detección mediante la "multi-firma" demostrará la robustez del enfoque de fusión de datos. La prueba de resiliencia validará el pilar fundamental de la arquitectura de *Fog Computing*: la capacidad de operación autónoma. Finalmente, la verificación de los estándares de seguridad e interoperabilidad confirmará que el diseño no solo es funcional, sino que también se alinea con las mejores prácticas de la industria para sistemas de misión crítica.

4.4 LIMITACIONES DE LA VALIDACIÓN

Es fundamental reconocer las limitaciones de este plan de validación para contextualizar los resultados:

- **Entorno Controlado:** Las pruebas se realizan en un entorno de laboratorio, que no replica la complejidad de las condiciones ambientales reales de una ZIUF (viento, humedad variable, interferencias de radio).
- **Escala Reducida:** El prototipo no permite validar el comportamiento de la red Mesh a gran escala (escalabilidad a cientos de nodos, enrutamiento dinámico bajo fallos masivos).
- **Duración Limitada:** Las pruebas se ejecutan en un período corto y no validan la degradación de los componentes o la fiabilidad del sistema a lo largo de varios meses de operación continua.

CAPÍTULO 5: CONCLUSIONES

El presente trabajo abordó el desafío crítico de la detección temprana de incendios forestales en las ZIUF del AMV, donde la latencia de los sistemas tradicionales representa una barrera fundamental para la respuesta eficaz. A través de esta memoria, se ha cumplido el objetivo de diseñar una arquitectura de sistema novedosa, fundamentada en la integración de tecnologías de IoT, Fog Computing y Redes Mesh, especificando sus componentes y comportamiento para responder de manera directa a esta problemática.

A continuación, se presentan las principales conclusiones derivadas de este trabajo de diseño arquitectónico.

5.1 CONTRIBUCIÓN

La principal contribución de esta memoria es el diseño de una arquitectura de sistema distribuida, resiliente y adaptada al complejo contexto de las ZIUF. Se ha especificado una solución técnica que, a nivel de diseño, es capaz de superar la brecha fundamental de los sistemas actuales: el tiempo de detección.

El diseño se basa en un enfoque de **detección hiperlocal y de baja latencia**, donde el procesamiento de datos se realiza en el borde de la red. Esta decisión arquitectónica permite reducir significativamente el tiempo de alerta a minutos, en contraste con las horas que pueden requerir los sistemas satelitales. Esta capacidad representa una oportunidad crucial para mejorar la respuesta inicial y mitigar los devastadores impactos socioambientales y económicos que enfrenta la región, abordando las vulnerabilidades específicas identificadas en el AMV.

5.2 VIABILIDAD E IMPACTO

Más allá de la contribución técnica, se concluye que el sistema diseñado posee un fuerte alineamiento estratégico con las políticas nacionales y, fundamentalmente, una viabilidad económica clara.

5.2.1 VIABILIDAD ECONÓMICA

El análisis económico se centró en la inversión inicial en hardware (*CAPEX*) y los costos operacionales recurrentes (*OPEX*) para un despliegue de referencia de 100 hectáreas (1 km^2).

5.2.1.1 COSTOS DE INVERSIÓN (CAPEX)

Los costos unitarios se basan en la selección de hardware para **Producción** detallada anteriormente, optimizada para fiabilidad y TCO a largo plazo. El costo proyectado es de **$79.48 USD** por Nodo Sensor y **$363.00 USD** por Nodo Fog. Para cuantificar el costo de

implementación, se utiliza un **Área de Cobertura de Referencia de 100 hectáreas (1 km²)** y la **Relación de Redundancia de 10:1**[8]. Aplicando las densidades de despliegue detalladas en el diseño de la solución, el costo total de hardware estimado es:

Densidad	N° Nodos Sensor	N° Nodos Fog	Costo Total Estimado de Hardware (USD)
1.0 nodos/ha	90	10	$10,783.20
2.0 nodos/ha	180	20	$21,566.40
4.5 nodos/ha	405	45	$48,524.40

Tabla 8: Costos de Inversión

5.2.1.2 COSTOS OPERACIONES (OPEX)

Basado en el escenario de media densidad (200 nodos totales: 180 sensores, 20 fogs), el volumen de datos mensual se estima en 12.96 MB[9]. Considerando la conectividad de datos, la infraestructura en la nube y una provisión para mantenimiento, el costo operacional total anual se proyecta en:

Componente de Costo	Detalle	Costo Operacional Total Anual (USD)
Conectividad de Datos	Planes IoT/M2M para 20 Nodos Fog.[10]	$720
Infraestructura Cloud	Estimación de precios de AWS.[11]	$264
Mantenimiento y Reposición	Provisión para reemplazo de baterías y una tasa de falla de componentes del 2%[12].	$250
Costo Operacional Total Anual (OPEX)		$1,234

Tabla 9: Costos Operacionales

5.2.2 ANÁLISIS COSTO - BENEFICIO

El análisis de costo-beneficio demuestra que la inversión en el sistema es marginal en comparación con los costos económicos documentados de un solo evento de megaincendio. Utilizando como referencia la catástrofe de febrero de 2024 en la Región de Valparaíso, cuyo Plan de Reconstrucción se estima en **1.1 mil millones de dólares**, la conclusión es contundente.

[8] Relación conservadora que prioriza la **máxima fiabilidad y baja latencia**.
[9] Basado en el tamaño del payload (calculado anteriormente) para 200 nodos.
[10] $36/año por SIM basado en planes IoT/M2M ofrecidos en Chile.
[11] Basado en el uso de 200 nodos con un ciclo de reporte cada 5 minutos.
[12] Estimación estándar en la planificación de costos operativos (OPEX) en electrónica desplegada en exteriores considerando el estrés ambiental (Pecht, 2009)

El beneficio principal del sistema es el **costo evitado** de daños a la propiedad e infraestructura, operaciones de combate, impacto económico y productivo, y costos ambientales y de salud. El beneficio cualitativo más importante es la **protección de vidas humanas**, un valor invaluable.

Se concluye con un alto grado de confianza que la inversión requerida para implementar el sistema en su escenario de más alta densidad (cubriendo 100 hectáreas) es de aproximadamente **$48,524.40 USD**. Al comparar esta cifra con el costo de reconstrucción del evento de 2024, la inversión proyectada representa aproximadamente el **0.0044%** del costo del desastre. Esta relación costo-beneficio abrumadoramente favorable posiciona a la arquitectura propuesta como una estrategia de inversión excepcionalmente eficiente para la mitigación de riesgos de incendios forestales.

5.3 LIMITACIONES

Es fundamental reconocer que este trabajo presenta limitaciones inherentes a su alcance. La presente memoria se ha enfocado en el diseño arquitectónico y la especificación del sistema, no en su implementación y validación empírica. Por lo tanto, las conclusiones sobre el rendimiento, la precisión y la fiabilidad del sistema son teóricas, basadas en las capacidades conocidas de las tecnologías seleccionadas y en el plan de validación propuesto. La efectividad real del sistema sólo podrá ser cuantificada a través de la ejecución de una prueba piloto en un entorno real.

5.4 REFLEXIÓN

El drástico aumento en la frecuencia e intensidad de los incendios forestales en Chile exige un cambio de paradigma, transitando desde un enfoque predominantemente reactivo hacia uno proactivo y basado en la tecnología. La arquitectura especificada en esta memoria representa un paso concreto en esa dirección, ofreciendo un plano detallado para la construcción de una herramienta que puede salvar vidas, proteger ecosistemas y fortalecer la resiliencia de las comunidades más vulnerables. El camino a seguir, detallado en el capítulo de recomendaciones, se enfoca ahora en llevar este diseño del plano a la realidad.

CAPÍTULO 6: RECOMENDACIONES

Habiendo especificado la arquitectura del sistema de detección temprana, este capítulo presenta un conjunto de recomendaciones para guiar los pasos subsecuentes. Estas recomendaciones se centran en la validación empírica del diseño propuesto, su validación operacional con los actores clave y las futuras líneas de investigación y desarrollo que pueden potenciar significativamente sus capacidades.

6.1 VERIFICACIÓN

Tras el diseño, es crucial implementar el plan de verificación del Capítulo 5. La principal recomendación es la implementación física de la arquitectura en una **zona piloto representativa.** Aunque el diseño es teóricamente sólido, solo una prueba en un entorno real confirmará empíricamente los criterios de aceptación y evaluará el rendimiento del sistema en condiciones operativas.

6.1.1 Zona Piloto

Se recomienda seleccionar una zona dentro del AMV que cumpla con criterios clave derivados del análisis del problema, como una clara ZIUF, una topografía compleja, un historial de vulnerabilidad reconocida y la colaboración de la comunidad local (Alegría Tardón, 2020). Considerando estos criterios, se ha identificado como zona piloto ideal un sector específico dentro del Jardín Botánico Nacional (Viña del Mar), en el área adyacente al Canal Chacao y el sector El Olivar. Esta zona es particularmente relevante por su representatividad crítica de ZIUF, sus desafiantes características geográficas y el trágico historial de riesgo evidenciado en la catástrofe de febrero de 2024 (Martínez et al., 2024; Alegría Tardón, 2020).

Figura 7: Mapa Zona Piloto Recomendada

6.1.2 Validación con Stakeholders

Paralelamente a la verificación técnica, es crucial realizar una validación con los stakeholders finales. Se recomienda organizar sesiones de demostración del sistema operando en la zona piloto con representantes de CONAF, Cuerpos de Bomberos y SENAPRED para recolectar retroalimentación cualitativa sobre la usabilidad de la interfaz (RNF-10), la claridad de las alertas y su potencial integración en los flujos de trabajo operativos. Esta validación es un paso indispensable para asegurar que la solución tecnológica responda a las necesidades operacionales reales y para abordar la brecha en la investigación sobre la Interacción Humano-Máquina (HMI) en sistemas de emergencia (Almeida et al., 2023; Özel et al., 2024)."

6.2 OPTIMIZACIÓN DE WSN

La arquitectura actual se basa en una red mesh auto-configurable, pero su eficiencia energética y escalabilidad a largo plazo pueden ser mejoradas. Una línea de investigación futura debería enfocarse en la **optimización de la topología, enrutamiento de la red y ubicación física óptima de los sensores.**

6.3 EDGE AI

Una línea de trabajo futura relevante es la evolución del algoritmo de detección desde un modelo heurístico hacia uno basado en **Inteligencia Artificial en el Borde (*Edge AI*)**. Las recomendaciones son:

- **Nodo Sensor:** Se recomienda la adopción del paradigma Tiny Machine Learning (TinyML), que consiste en la ejecución de modelos de *machine learning* directamente en microcontroladores de bajo consumo, como el **ESP32 especificado en esta memoria** (Warden & Situnayake, 2019). Este campo emergente permite que los propios dispositivos sensores procesen datos y extraigan conclusiones localmente (Yadav et al., 2024). Un modelo de clasificación entrenado con *TensorFlow Lite for Microcontrollers* podría reconocer patrones complejos en los datos de los sensores, ofreciendo una detección ultra-rápida, mayor precisión y una mejor eficiencia energética al reducir las transmisiones innecesarias (Warden & Situnayake, 2019; Yadav et al., 2024) .

- **Nodo Fog:** Se recomienda investigar el uso de modelos como **Máquinas de Vectores de Soporte (SVM),** que han demostrado una alta precisión en la clasificación de niveles de riesgo (Zhang & Pan, 2024), o modelos de series de tiempo como ***LSTM (Long Short-Term Memory)*** para analizar las secuencias de datos de múltiples sensores.

La incorporación de estas técnicas transformaría el sistema de uno reactivo a uno proactivo y cognitivo, representando la siguiente evolución natural de la arquitectura propuesta (Alistarh et al., 2019).

6.4 FIABILIDAD Y SEGURIDAD

Una línea de investigación fundamental debe centrarse en la **fiabilidad a largo plazo de la red.** Futuros trabajos deberían explorar la implementación de algoritmos para la **detección de nodos defectuosos** en tiempo real. Enfoques como el de selección negativa o el análisis de datos con lógica difusa han demostrado ser efectivos para identificar y aislar sensores que entregan lecturas anómalas, evitando así falsas alarmas o fallos en la detección (Mohapatra & Shrimali, 2023;).

Para un sistema aún más robusto, se recomienda investigar la implementación de modelos de **Inteligencia Artificial para la detección de anomalías e intrusiones**. Modelos como los *Transformers* pueden aprender el comportamiento normal de la red y detectar desviaciones sutiles que indican no solo un fallo de hardware, sino también un posible ciberataque, asegurando así la integridad y seguridad del sistema (Haque & Soliman, 2025). Complementariamente, se podrían desarrollar **modelos de confianza** que evalúen dinámicamente la fiabilidad de los datos de cada sensor antes de ser procesados por el algoritmo de detección (Khan et al., 2025).

6.5 MAPAS DE RIESGO

Una vez que el sistema esté operativo y recopilando datos de múltiples nodos, una línea de investigación futura sería la implementación de técnicas de interpolación geoestadística, como el **Kriging**, para **generar mapas de riesgo de alta resolución y en tiempo real.**

En el sistema propuesto por esta memoria, cada Nodo Fog calcula un índice FWI hiperlocal para su área inmediata. Al combinar los datos de toda la red, el sistema central podría utilizar Kriging para estimar el **valor del FWI en las zonas entre los sensores**, creando una **superficie continua de riesgo** para toda el área protegida. Esta técnica es ideal para el monitoreo ambiental con flujos de datos de sensores en tiempo real (Lorkowski & Brinkhoff, 2015). La idoneidad del Kriging para este propósito ha sido validada en estudios que lo comparan con otros métodos de interpolación para variables climáticas de incendios, demostrando que generalmente ofrece la mayor precisión, especialmente cuando se combina con variables auxiliares como la elevación (Jain & Flannigan, 2017; Cheng, 2020).

6.6 SISTEMA HÍBRIDO VISUAL

La arquitectura propuesta, basada en sensores físicos, destaca por su inmunidad a las condiciones de visibilidad. Sin embargo, su máximo potencial se alcanzaría al **integrar con sistemas de vigilancia visual,** creando un **sistema de detección híbrido y sinérgico**

Se recomienda diseñar y **desarrollar una plataforma que utilice las alertas de la red de sensores como un "disparador inteligente"** (*smart trigger*) para los activos de vigilancia visual. Una alerta generada por el Nodo Fog, con su coordenada geográfica precisa, podría comandar automáticamente el despegue de un UAV de confirmación equipado con una cámara y un modelo de detección en tiempo real como YOLOv9 (Bakirci & Bayraktar, 2024). Este UAV proporciona evidencia visual inmediata, permitiendo a los equipos de emergencia evaluar la magnitud del incendio y mejorar la conciencia situacional antes de llegar al lugar. Este enfoque combina la fiabilidad 24/7 de los sensores físicos con la riqueza contextual de la evidencia visual, creando un sistema de confirmación dual que maximiza la confianza en la alerta y acelera la toma de decisiones.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre, P., León, J., González-Mathiesen, C., Román, R., Penas, M., & Ogueda, A. (2024). Modelling the vulnerability of urban settings to wildland–urban interface fires in Chile. *Natural Hazards and Earth System Sciences*, 24(4), 1521-1537. https://doi.org/10.5194/nhess-24-1521-2024

Al Enany, M. O., Harb, H. M., & Attiya, G. (2021). A comparative analysis of MQTT and IoT application protocols. En *International Conference on Electronic Engineering* (pp. 1-6). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/iceem52022.2021.9480384

Alam, S. (2024, 1 de noviembre). Single page applications (SPAs) vs. multi-page applications (MPAs): Advantages and challenges. Medium. https://medium.com/@sehban.alam/single-page-applications-spas-vs-multi-page-applications-mpas-advantages-and-challenges-df06bee3fed1

Alegría Tardón, R. E. (2020). *Estudio y evaluación del riesgo de incendios forestales en la interfaz urbano-forestal de las comunas que componen el Área Metropolitana de Valparaíso : periodo 2000 - 2017* [Tesis de Pregrado, Universidad de Chile]. https://repositorio.uchile.cl/handle/2250/178619

Alkhafajee, A. R., Al-Muqarm, A. M. A., Alwan, A. H., & Mohammed, Z. R. (2021). Security and performance analysis of MQTT protocol with TLS in IoT networks. En *International Iraqi Conference on Engineering Technology and Their Applications (IICETA)* (4.ª ed., pp. 206-211). https://doi.org/10.1109/iiceta51758.2021.9717495

Almasoud, A. S. (2022). Intelligent deep learning enabled wild Forest fire detection system. *Computer Systems Science and Engineering*, 44(2), 1485-1498. https://doi.org/10.32604/csse.2023.025190

Almeida, J. S., Jagatheesaperumal, S. K., Nogueira, F. G., & De Albuquerque, V. H. C. (2023). EdgeFireSmoke++: A novel lightweight algorithm for real-time forest fire detection and visualization using internet of things-human machine interface. *Expert Systems with Applications*, 221, 119747. https://doi.org/10.1016/j.eswa.2023.119747

Amazon Web Services (AWS). (2025). *Applying C4 model concepts to AWS solution architecture design*.

Amazon Web Services Inc. [AWS]. (s. f.). *¿Qué son los microservicios?* https://aws.amazon.com/es/microservices/

Amazon Web Services Inc. [AWS]. (s. f.-a). *PostgreSQL y MySQL: diferencia entre los sistemas de administración de bases de datos relacionales (RDBMS)*. AWS. https://aws.amazon.com/es/compare/the-difference-between-mysql-vs-postgresql

Aufranc, J. (2022, 6 diciembre). $200 Swarm M138 kit enables two-way satellite connectivity for IoT projects. *CNX Software - Embedded Systems News* https://www.cnx-software.com/2022/12/06/swarm-m138-kit-two-way-satellite-connectivity-iot-projects/

Bakirci, M., & Bayraktar, I. (2024). Harnessing UAV technology and YOLOv9 algorithm for real-time forest fire detection. En *International Russian Automation Conference (RusAutoCon)* (pp. 95-100). https://doi.org/10.1109/rusautocon61949.2024.10694663

Bender, M., Kirdan, E., Pahl, M.-O., & Carle, G. (2021). Open-source MQTT evaluation. En *Annual Consumer Communications & Networking Conference (CCNC)* (18.ª ed., pp. 1-4). https://doi.org/10.1109/ccnc49032.2021.9369499

Bolourchi, P., & Uysal, S. (2013). Forest fire detection in wireless sensor network using fuzzy logic. En *International Conference on Computational Intelligence, Communication Systems and Networks* (5.ª ed., pp. 83-87). https://doi.org/10.1109/cicsyn.2013.32

Bormann, C., & Hoffman, P. (2020). Concise Binary Object Representation (CBOR). https://doi.org/10.17487/rfc8949

Bouabdellah, K., Noureddine, H., & Larbi, S. (2013). Using wireless sensor networks for reliable forest fires detection. *Procedia Computer Science*, 19, 794-801. https://doi.org/10.1016/j.procs.2013.06.104

Brito, T., Zorawski, M., Mendes, J., Azevedo, B. F., Pereira, A. I., Lima, J., & Costa, P. (2021). Optimizing data transmission in a wireless sensor network based on LoRaWAN protocol. En Communications in computer and information science (pp. 281-293). https://doi.org/10.1007/978-3-030-91885-9_20

Brown, S. (s. f.). *C4 Model*. https://c4model.com/

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, *25*(6), 599-616. https://doi.org/10.1016/j.future.2008.12.001

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. En *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing* (pp. 13-16). Association for Computing Machinery.

Castillo, R. (2019). *Cálculo de índice de riesgo de incendios utilizando variables meteorológicas* [Tesis de Pregrado, Universidad Técnica Federico Santa María]. https://doi.org/10.71700/dspace-memorias/1394

Certini, G., Moya, D., Lucas-Borja, M. E., & Mastrolonardo, G. (2021). The impact of fire on soil-dwelling biota: A review. *Forest Ecology and Management*, 488, 119008. https://doi.org/10.1016/j.foreco.2021.119008

Chan, C. C., Alvi, S. A., Zhou, X., Durrani, S., Wilson, N., & Yebra, M. (2024). A survey on IoT ground sensing systems for early wildfire detection: Technologies, challenges and opportunities. IEEE Access, 1. https://doi.org/10.1109/access.2024.3501336

Chauhan, A., Semwal, S., & Chawhan, R. (2013). Artificial neural network-based forest fire detection system using wireless sensor network. En *Annual IEEE India Conference (INDICON)* (pp. 1-6). https://doi.org/10.1109/indcon.2013.6725913

Cheng, Y. (2020). *A study of methods for spatial interpolation of fire weather in the Canadian Prairies* [Tesís de Magister, Universidad de Guelph]. https://atrium.lib.uoguelph.ca/xmlui/handle/10214/17899

China, C. R. (2025, 22 julio). GraphQL vs REST API. IBM Think. https://www.ibm.com/think/topics/graphql-vs-rest-api

Choi, W., & Jung, I. Y. (2024). Multi-Sensor Photoelectric Fire Alarm Device Implementation for Early Fire Detection in Campsites. Applied Sciences, 14(21), 9965. https://doi.org/10.3390/app14219965

Centro de Ciencia del Clima y la Resiliencia (CR2). (2015). La megasequía 2010-2015: una lección para el futuro. https://www.cr2.cl/informe-a-la-nacion-la-megasequia-2010-2015-una-leccion-para-el-f uturo/

Chávez, R., Pérez, M., Fuentes, S., Castro, G., Álvarez, L., & Castillo, M. (2024). Mega-Incendio Valparaíso febrero 2024. Primeras imágenes satelitales revelan la magnitud y severidad del evento. Laboratorio de Geo-información y Percepción Remota, Instituto de Geografía, Pontificia Universidad Católica de Valparaíso & Laboratorio de Ingeniería de Incendios Forestales, Universidad de Chile. https://www.pucv.cl/uuaa/site/docs/20240209/20240209151003/incendio_valpo_2024_v01.pdf

Cordero, R. R., Feron, S., Damiani, A., Carrasco, J., Karas, C., Wang, C., Kraamwinkel, C. T., & Beaulieu, A. (2024). Extreme fire weather in Chile driven by climate change and El Niño–Southern Oscillation (ENSO). Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-52481-x

Dampage, U., Bandaranayake, L., Wanasinghe, R., Kottahachchi, K., & Jayasanka, B. (2022). Forest fire detection system using wireless sensor networks and machine learning. Scientific Reports, 12(1). https://doi.org/10.1038/s41598-021-03882-9

Díaz-Ramírez, A., Tafoya, L. A., Atempa, J. A., & Mejía-Alvarez, P. (2012). Wireless Sensor Networks and Fusion Information Methods for Forest Fire Detection. Procedia Technology, 3, 69-79. https://doi.org/10.1016/j.protcy.2012.03.008

EATON. (2024). Technical Data ELX1087: TVA supercapacitors Automotive Grade cylindrical cells. https://www.eaton.com/content/dam/eaton/products/electronic-components/resources/data-sheet/eaton-tva-automotive-supercapacitor-cylindrical-cell-data-sheet-elx1087-en.pdf

Espressif Systems. (2025). ESP32-S3 Series datasheet. https://documentation.espressif.com/esp32-s3_datasheet_en.pdf

Eugster, P. T., Felber, P. A., Guerraoui, R., & Kermarrec, A. (2003). The many faces of publish/subscribe. ACM Computing Surveys, 35(2), 114-131. https://doi.org/10.1145/857076.857078

Gil, M., & Cruz Florencia. (2024). Gestión del riesgo de incendios forestales en Chile: aprendizajes y temas emergentes. Temas de la Agenda Pública, 19(170), 1-20. https://politicaspublicas.uc.cl/publicacion/temas-de-la-agenda-publica/gestion-del-riesgo-de-incendios-forestales-en-chile-aprendizajes-y-temas-emergentes/

Gobierno de Chile. (2024). Plan de reconstrucción: incendios Viña del Mar, Quilpué, Villa Alemana, región de Valparaíso (Ministerio de Desarrollo Social y Familia, Ed.). Ministerio de Desarrollo Social y Familia. https://www.desarrollosocialyfamilia.gob.cl/storage/docs/Plan_reconstruccion.pdf

Gonzales, L., & Lara, I. (2024). Incendios forestales 2024: perspectivas (Centro Latinoamericano de Políticas Económicas y Sociales de la Pontificia Universidad Católica de Chile [CLAPES UC], Ed.). https://assets.clapesuc.cl/070224_Incendios_Forestales_e64b4a481b.pdf

González, M., Sapiains, R., Gómez-González, S., Garreaud, R., Miranda, A., Galleguillos, M., Jacques-Coper, M., Pauchard, A., Hoyos-Santillan, J., Vega, L., Lavín, F., Lara, A., Aldunce, P., Schneider, V., Arriagada, R., Ugarte, A., Farias, L., García, R., Castillo, I., & Centro de Ciencia del Clima y la Resiliencia [CR2] (Eds.). (2020). Incendios forestales en Chile: causas, impactos y resiliencia. https://www.cr2.cl/incendios/

González, P. (2017). Impacto de los incendios forestales en suelos, agua y vegetación. Biblioteca del Congreso Nacional de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/23945/2/Impacto%20Incendio%20Forestal.pdf

Google. (2025). Protocol buffers documentation. https://protobuf.dev/

Gottuk, D. T., Peatross, M. J., Roby, R. J., & Beyler, C. L. (2002). Advanced fire detection using multi-signature alarm algorithms. Fire Safety Journal, 37(4), 381-394. https://doi.org/10.1016/s0379-7112(01)00057-1

Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). Cyber-physical systems and internet of things. https://doi.org/10.6028/nist.sp.1900-202

Gräßler, I., Wiechel, D., Roesmann, D., & Thiele, H. (2021). V-model based development of cyber-physical systems and cyber-physical production systems. Procedia CIRP, 100, 253-258. https://doi.org/10.1016/j.procir.2021.05.119

Gupta, P., Follette Cook, M., & Prados, A. (s. f.). Monitoreo de incendios, humo y aerosoles desde el espacio (National Aeronautics and Space Administration [NASA], Ed.) [Diapositivas].

Gómez-González, J. L., Marcoulaki, E., Cantizano, A., Konstantinidou, M., Caro, R., & Castro, M. (2025). Simulated fire observables as indicators for optimizing wireless sensor networks in wildfire risk monitoring. Ecological Indicators, 175, 113509. https://doi.org/10.1016/j.ecolind.2025.113509

González Saggia, V. (2023). *Plan de innovación en detección temprana de incendios forestales en la Isla Yacyretá* [Tesis de Magister, Universitat de Barcelona]. https://diposit.ub.edu/dspace/handle/2445/201470

Godoy Anfossi, E. (2022). Propuesta de detección de incendios utilizando procesamiento de imagen, en sistemas de control aéreo [Tesis de técnico universitario, Universidad Técnica Federico Santa María]. Repositorio USM. https://repositorio.usm.cl/entities/tesis/2d538401-48d3-41e3-a9ff-257bfc20a158

Goffin, B. D., Aryal, A., & Deppert, Q. (2023, 7 agosto). Chile Wildland Fires: Augmenting wildfire risk assessment efforts with satellite-based measurements of soil moisture and vegetation health in Central and South-Central Chile [Diapositivas]. NASA DEVELOP, Estados Unidos. NASA Technical Reports Server (NTRS). https://ntrs.nasa.gov/citations/20230011079

Hadisuwito, A. S., & Hassan, F. H. (2020). A Comparative Study of the Forest Fire Danger Index Calculation Methods Using Backpropagation. Journal of Physics: Conference Series, 1529(5), 052051.

Haque, A., & Soliman, H. (2025). A Transformer-Based Autoencoder with Isolation Forest and XGBoost for Malfunction and Intrusion Detection in Wireless Sensor Networks for Forest Fire Prediction. Future Internet, 17(4), 164. https://doi.org/10.3390/fi17040164

Hasura. (2025). GraphQL subscriptions for realtime data. https://hasura.io/learn/graphql/intro-graphql/graphql-subscriptions/

Hefeeda, M., & Bagheri, M. (2007). Wireless sensor networks for early detection of forest fires. En IEEE International Conference on Mobile Adhoc and Sensor Systems (pp. 1-6). https://doi.org/10.1109/mobhoc.2007.4428702

Industry IoT Consortium [IIC]. (2022). The Industrial Internet Reference Architecture. https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf

Internet of things: Principles and paradigms. (2016). [PDF]. En R. Buyya & A. V. Dastjerdi (Eds.), Morgan Kaufmann Publishers Inc. eBooks. Morgan Kaufmann. https://doi.org/10.1016/C2015-0-04135-1

Jain, P., & Flannigan, M. (2017). Comparison of methods for spatial interpolation of fire weather in Alberta, Canada. Canadian Journal Of Forest Research, 47(12), 1646-1658. https://doi.org/10.1139/cjfr-2017-0101

Jonsson, F. (2016). Component-based software design of embedded real-time systems. DiVA portal.

Joy, M. J. R., & Branch, P. (2024). Flooding in LORA mesh networks. En International Telecommunication Networks and Applications Conference (ITNAC) (34.a ed., pp. 1-4). https://doi.org/10.1109/itnac62915.2024.10815298

Kadir, E. A., Alomainy, A., Daud, H., Maharani, W., Muhammad, N., & Syafitri, N. (2023). Multi Sensor Network System for Early Detection and Prediction of Forest Fires in Southeast Asia. En International Telecommunication Networks and Applications Conference (33.a ed., pp. 190-195). https://doi.org/10.1109/itnac59571.2023.10368547

Khalid, W., Sattar, A., Qureshi, M. A., Amin, A., Malik, M. A., & Hussain, K. (2019). A smart wireless sensor network node for fire detection. Turkish Journal of Electrical Engineering and Computer Sciences, 27(4), 2541-2556.

Khan, T., Singh, K., Bhati, B. S., Ahmad, K., Al-Rasheed, A., Getahun, M., & Soufiene, B. O. (2025). Trust-driven approach to enhance early forest fire detection using machine learning. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-99032-6

Kizilkaya, B., Ever, E., Yatbaz, H. Y., & Yazici, A. (2022). An effective forest fire detection framework using heterogeneous wireless multimedia sensor networks. ACM Transactions On Multimedia Computing Communications And Applications, 18(2), 1-21. https://doi.org/10.1145/3473037

KYOCERA AVX. (2025). SCC Series – SuperCapacitors | KYOCERA AVX. https://www.kyocera-avx.com/products/supercapacitors/scc-series/

Laribee, D. (2009). Best Practice - An Introduction to Domain-Driven design. MSDN Magazine Issues, 24(2).

https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/february/best-practice-an-introduction-to-domain-driven-design

Lazidis, A., Tsakos, K., & Petrakis, E. G. (2022). Publish–Subscribe Approaches for the IoT and the Cloud: Functional and performance evaluation of open-source systems. Internet Of Things, 19, 100538. https://doi.org/10.1016/j.iot.2022.100538

Lertsinsrubtavee, A., Kanabkaew, T., & Raksakietisak, S. (2023). Detection of forest fires and pollutant plume dispersion using IoT air quality sensors. Environmental Pollution, 338, 122701. https://doi.org/10.1016/j.envpol.2023.122701

Liu, R., Yuan, J., & Huang, X. (2024). Benchmarking Time Series databases with IoTDB-Benchmark for IoT scenarios. arXiv. https://doi.org/10.48550/arxiv.1901.08304

Liu, W., Shen, Z., & Xu, S. (2024). CF-YOLO: a capable forest fire identification algorithm founded on YOLOv7 improvement. Signal Image And Video Processing, 18(8-9), 6007-6017. https://doi.org/10.1007/s11760-024-03288-w

Lorkowski, P., & Brinkhoff, T. (2015). Environmental monitoring of continuous phenomena by sensor data streams: A system approach based on Kriging. *Advances In Computer Science Research*. https://doi.org/10.2991/ict4s-env-15.2015.4

Luan, T., Zhou, S., Zhang, G., Song, Z., Wu, J., & Pan, W. (2024). Enhanced Lightweight YOLOX for Small Object Wildfire Detection in UAV Imagery. Sensors, 24(9), 2710. https://doi.org/10.3390/s24092710

Luong, T. (2022, 1 octubre). FastAPI vs. Fastify vs. Spring Boot vs. Gin Benchmark. https://www.travisluong.com/fastapi-vs-fastify-vs-spring-boot-vs-gin-benchmark/

Martínez, C., León, J., Bonet, M., Inzunza, S., Guerrero, N., Román, R., Acevedo, R., Araya, E., & Centro de Investigación para la Gestión Integrada del Riesgo de Desastres [CIGIDEN]. (2024). Incendios 02 y 03 de febrero de 2024, Viña del Mar (Región de Valparaíso): Informe de daños - fase de emergencia. https://wildfirex.cl/wp-content/uploads/2024/02/Reporte-incendios-Vina-del-Mar-2024_version-1_14.02.2024_compressed.pdf

McBride, B., & Reynolds, D. (2020). Survey of Time Series Database Technology. Epimorphics Ltd. https://nora.nerc.ac.uk/id/eprint/527832

Meshtastic. (s. f.). Mesh Broadcast Algorithm. https://meshtastic.org/docs/overview/mesh-algo/

Messina, F., Santoro, C., & Santoro, F. F. (2024). Enhancing Security and Trust in Internet of Things through Meshtastic Protocol Utilising Low-Range Technology. Electronics, 13(6), 1055. https://doi.org/10.3390/electronics13061055

De la Torre, C., Wagner, B., & Rousos, M. (2022, 4 de diciembre). Designing a DDD-oriented microservice. En .NET Microservices: Architecture for Containerized .NET Applications. Microsoft. https://learn.microsoft.com/en-us/dotnet/architecture/microservices/microservice-ddd-cqrs-patterns/ddd-oriented-microservice

Microsoft. (s. f.). Identify microservice boundaries. Microsoft Learn. https://learn.microsoft.com/en-us/azure/architecture/microservices/model/microservice-boundaries

Mohapatra, S., & Shrimali, B. (2023). Fault detection in forest fire monitoring using negative selection approach. En IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC) (pp. 732-736). https://doi.org/10.1109/r10-htc57504.2023.10461878

Molina-Pico, A., Cuesta-Frau, D., Araujo, A., Alejandre, J., & Rozas, A. (2016). Forest Monitoring and Wildland Early Fire Detection by a Hierarchical Wireless Sensor Network. Journal Of Sensors, 2016, 1-8. https://doi.org/10.1155/2016/8325845

Moussa, N., Khemiri-Kallel, S., & Alaoui, A. E. B. E. (2022). Fog-assisted hierarchical data routing strategy for IoT-enabled WSN: Forest fire detection. Peer-to-Peer Networking And Applications, 15(5), 2307-2325. https://doi.org/10.1007/s12083-022-01347-y

Nakamura, E. F., Loureiro, A. A. F., & Frery, A. C. (2007). Information fusion for wireless sensor networks. ACM Computing Surveys, 39(3), 9. https://doi.org/10.1145/1267070.1267073

Naumann, M., Schimpe, M., Keil, P., Hesse, H. C., & Jossen, A. (2018). Analysis and modeling of calendar aging of a commercial LiFePO4/graphite cell. Journal Of Energy Storage, 17, 153-169. https://doi.org/10.1016/j.est.2018.01.019

Newman, S. (2015). Building microservices. Oreilly & Associates Incorporated. https://book.northwind.ir/bookfiles/building-microservices/Building.Microservices.pdf

Nguyen, L. T. T., Ha, S. X., Le, T. H., Luong, H. H., Vo, K. H., Nguyen, K. H. T., Nguyen, A., Dao, T. A., & Nguyen, H. V. K. (2022). BMDD: a novel approach for IoT platform

(broker-less and microservice architecture, decentralized identity, and dynamic transmission messages). PeerJ Computer Science, 8, e950. https://doi.org/10.7717/peerj-cs.950

nperf. (s. f.). Mapa de cobertura 3G / 4G / 5G. nPerf.com. https://www.nperf.com/es/map/CL/-/-/signal

OASIS. (2010). Common Alerting Protocol Version 1.2: OASIS Standar. https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf

Organización Panamericana de la Salud [OPS] & Organización Mundial de la Salud [OMS]. (2025). Análisis de la situación de salud pública de los incendios forestales en Sudamérica. https://www.paho.org/sites/default/files/2025-02/incendios-forestales-suramerica-febrero-2025-es.pdf

Pang, Y., Wu, Y., & Yuan, Y. (2023). FuF-Det: An Early Forest Fire Detection Method under Fog. Remote Sensing, 15(23), 5435. https://doi.org/10.3390/rs15235435

Parvin, J. R. (2019). An Overview of Wireless Mesh Networks. En *IntechOpen eBooks*. https://doi.org/10.5772/intechopen.83414

Poljak, R., Poscic, P., & Jaksic, D. (2017). Comparative analysis of the selected relational database management systems. En International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (40.a ed., pp. 1496-1500). https://doi.org/10.23919/mipro.2017.7973658

Popić, S., Pezer, D., Mrazovac, B., & Teslic, N. (2016). Performance evaluation of using Protocol Buffers in the Internet of Things communication. 2022 International

Conference On Smart Systems And Technologies (SST). https://doi.org/10.1109/sst.2016.7765670

The PostGIS Development Group. (s. f.). *PostGIS 3.3.9Dev Manual*. https://postgis.net/docs/manual-3.3/

The PostgreSQL Global Development Group. (2025, 25 de septiembre). *PostgreSQL 18.0 documentation*. https://www.postgresql.org/docs/current/index.html

Poblete, S. (2024). Uso de teledetección satelital para la detección de focos de incendios forestales [Tesis de Pregrado, Universidad Técnica Federico Santa María]. https://doi.org/10.71700/dspace-memorias/2781

Ramachandran, C., Misra, S., & Obaidat, M. S. (2008). A probabilistic zonal approach for swarm-inspired wildfire detection using sensor networks. International Journal of Communication Systems, 21(10), 1047-1073.

Ratner, A., Alistarh, D., Alonso, G., Andersen, D. G., Bailis, P., Bird, S., Carlini, N., Catanzaro, B., Chayes, J., Chung, E., Dally, B., Dean, J., Dhillon, I. S., Dimakis, A., Dubey, P., Elkan, C., Fursin, G., Ganger, G. R., Getoor, L., . . . Talwalkar, A. (2019). MLSYS: the new frontier of machine learning systems. *arXiv*. https://doi.org/10.48550/arxiv.1904.03257

Rodríguez y Silva, F., Molina Martínez, J. R., & Castillo Soto, M. (2012). Aproximación metodológica para la evaluación del impacto económico de los incendios forestales, mediante el uso de teledetección espacial, aplicación mediante el uso de imágenes Modis. En Memorias del Cuarto Simposio Internacional Sobre Políticas, Planificación y Economía de los Incendios Forestales: Cambio Climático e

Incendios Forestales. U.S. Department of Agriculture, Forest Service, Pacific Southwest Research Station. https://www.fs.usda.gov/psw/publications/documents/psw_gtr245/es/psw_gtr245_305.pdf

Sairi, A., Labed, S., Miles, B., & Kout, A. (2023, 6 marzo). A review on early forest fire detection using IoT-enabled WSN. En International Conference On Advances In Electronics, Control And Communication Systems (ICAECCS. https://doi.org/10.1109/icaeccs56710.2023.10104887

Salaria, A., & Singh, A. (2025). A guide for selection of wireless communication technology for effective and robust early forest fire detection system. Bulletin Of Electrical Engineering And Informatics, 14(2), 1026-1035. https://doi.org/10.11591/eei.v14i2.8613

Shevchenko, N. (2020, 21 diciembre). An Introduction to Model-Based Systems Engineering (MBSE). SEI Blog. https://www.sei.cmu.edu/blog/introduction-model-based-systems-engineering-mbse/

Shi, J., Wang, W., Gao, Y., & Yu, N. (2020). Optimal Placement and Intelligent Smoke Detection Algorithm for Wildfire-Monitoring Cameras. IEEE Access, 8, 72326-72339. https://doi.org/10.1109/access.2020.2987991

Shmuel, A., & Heifetz, E. (2023). Developing novel machine-learning-based fire weather indices. Machine Learning Science And Technology, 4(1), 015029. https://doi.org/10.1088/2632-2153/acc008

Sichevskyi, O. (2025, 5 septiembre). Build Large-Scale Apps with Go: Best Practices and Case Studies. MobiDev. https://mobidev.biz/blog/golang-app-development-best-practices-case-studies

Singh, A. K., & Singh, H. (2012). Forest Fire Detection through Wireless Sensor Network using Type-2 Fuzzy System. International Journal Of Computer Applications, 52(9), 19-23. https://doi.org/10.5120/8230-1315

SMARTsemi. (2023, 19 septiembre). Embedded MultiMediaCards (eMMCs) vs. Secure Digital (SD) Cards. SmartSemi. https://smartsemi.com/embedded-multimediacards-emmcs-vs-secure-digital-sd-cards/

Smith, C. (2025, 7 marzo). V-Model and Functional safety: ensuring process adherence in engineering. Critical Systems Analysis. https://www.criticalsystemsanalysis.com/articles/v-model-and-functional-safety-ensuring-process-adherence-in-engineering/

Sooriarachchi, V. P., & Jayakody, D. N. K. (2024). Model for Advanced Sensor Placement in Wildfire Detection Systems. 2022 IEEE Wireless Communications And Networking Conference (WCNC), 1-6. https://doi.org/10.1109/wcnc57260.2024.10570764

Suryadevara, N. K., & Dutta, A. (2022). Meshtastic Infrastructure-less Networks for Reliable Data Transmission to Augment Internet of Things Applications. En Springer eBooks (pp. 622-640). https://doi.org/10.1007/978-3-030-93398-2_55

Saldamli, G., Deshpande, S., Jawalekar, K., Gholap, P., Tawalbeh, L., & Ertaul, L. (2019). Wildfire detection using wireless mesh network. En Institute of Electrical and

Electronics Engineers [IEEE] (Ed.), 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC). https://doi.org/10.1109/fmec.2019.8795316

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: vision and challenges. IEEE Internet Of Things Journal, 3(5), 637-646. https://doi.org/10.1109/jiot.2016.2579198

Subsecretaría de Telecomunicaciones (SUBTEL). (2024, 3 de febrero). Subtel informa: 70 mensajes SAE enviados en la zona central del país y 213 antenas fuera de servicio en la región de Valparaíso por incendios forestales. https://www.subtel.gob.cl/actualizacion-1100-horas-subtel-informa-29-mensajes-sae-enviados-en-la-zona-central-del-pais-y-226-antenas-fuera-de-servicio-en-la-region-de-valparaiso-por-incendios-forestales/

Tan, Y. K., & Panda, S. K. (2011). Self-Autonomous wireless sensor nodes with wind energy harvesting for remote sensing of Wind-Driven wildfire spread. *IEEE Transactions On Instrumentation And Measurement*, *60*(4), 1367-1377. https://doi.org/10.1109/tim.2010.2101311

The Apache Software Foundation. (2025, 26 marzo). IoTDB website. IoTDB Website. https://iotdb.apache.org/

TheBentern, & Guvwaf. (2024, 18 agosto). Why Meshtastic uses managed flood routing. Meshtastic. https://meshtastic.org/blog/why-meshtastic-uses-managed-flood-routing/

Tjukanov, T. (2018, 27 junio). Why should you care about PostGIS?: A gentle introduction to spatial databases. Medium.

https://medium.com/@tjukanov/why-should-you-care-about-postgis-a-gentle-introduction-to-spatial-databases-9eccd26bc42b

Urzúa, N., & Cáceres, F. (2011). Incendios forestales: principales consecuencias económicas y ambientales en Chile. Revista Interamericana de Ambiente y Turismo, 7(1), 18-24. https://riat.utalca.cl/index.php/test/article/view/108/74

Van Wagner, C. E., & Service, C. F. (1987). Development and Structure of the Canadian Forest Fire Weather Index System. https://ostrnrcan-dostrncan.canada.ca/entities/publication/d96e56aa-e836-4394-ba29-3afe91c3aa6c

Veraverbeke, S., Sedano, F., Hook, S. J., Randerson, J. T., Jin, Y., & Rogers, B. M. (2014). Mapping the daily progression of large wildland fires using MODIS active fire data. International Journal Of Wildland Fire, 23(5), 655-667. https://doi.org/10.1071/wf13015

Vidal-Silva, C., Pizarro, R., Castillo-Soto, M., De la Fuente, C., Duarte, V., Sangüesa, C., Ibañez, A., Paredes, R., & Ingram, B. (2025). Wildfire Occurrence and Damage Dataset for Chile (1985–2024): A Real Data Resource for Early Detection and Prevention Systems. Data, 10(7), 93. https://doi.org/10.3390/data10070093

Viotti, J. C., & Kinderkhedia, M. (2022). A benchmark of JSON-compatible binary serialization specifications. arXiv. https://doi.org/10.48550/arxiv.2201.03051

Wang, C., Qiao, J., Huang, X., Song, S., Hou, H., Jiang, T., Rui, L., Wang, J., & Sun, J. (2023). Apache IoTDB: a Time series database for IoT applications. Proceedings Of The ACM On Management Of Data, 1(2), 1-27. https://doi.org/10.1145/3589775

Warden, P., & Situnayake, D. (2019). TinyML: Machine learning with TensorFlow lite on Arduino and Ultra-Low-Power microcontrollers. O'Reilly Media, Inc. https://tinymlbook.com/wp-content/uploads/2020/01/tflite_micro_preview.pdf

Wirepas. (s. f.). Wirepas Mesh IoT connectivity. https://wirepas.com/wirepas-mesh/

Wong, A. W., Goh, S. L., Hasan, M. K., & Fattah, S. (2024). Multi-Hop and Mesh for LoRa Networks: Recent Advancements, Issues, and Recommended Applications. ACM Computing Surveys, 56(6), 1-43. https://doi.org/10.1145/3638241

Yadav, P., Ngai, E. C. H., Gupta, M., Shresthamali, S., & Ranjan, A. (2024). Machine Learning on Edge in Sensor Systems (SenSys-ML 2024). En 2024 IEEE 3rd Workshop on Machine Learning on Edge in Sensor Systems (SenSys-ML) (pp. 1-2). https://doi.org/10.1109/sensys-ml62579.2024.00005

Yi, S., Li, C., Li, Q., & Association for Computing Machinery [ACM]. (2015). A survey of Fog Computing: Concepts, applications and issues. En Proceedings of the 2015 Workshop on Mobile Big Data. https://doi.org/10.1145/2757384.2757397

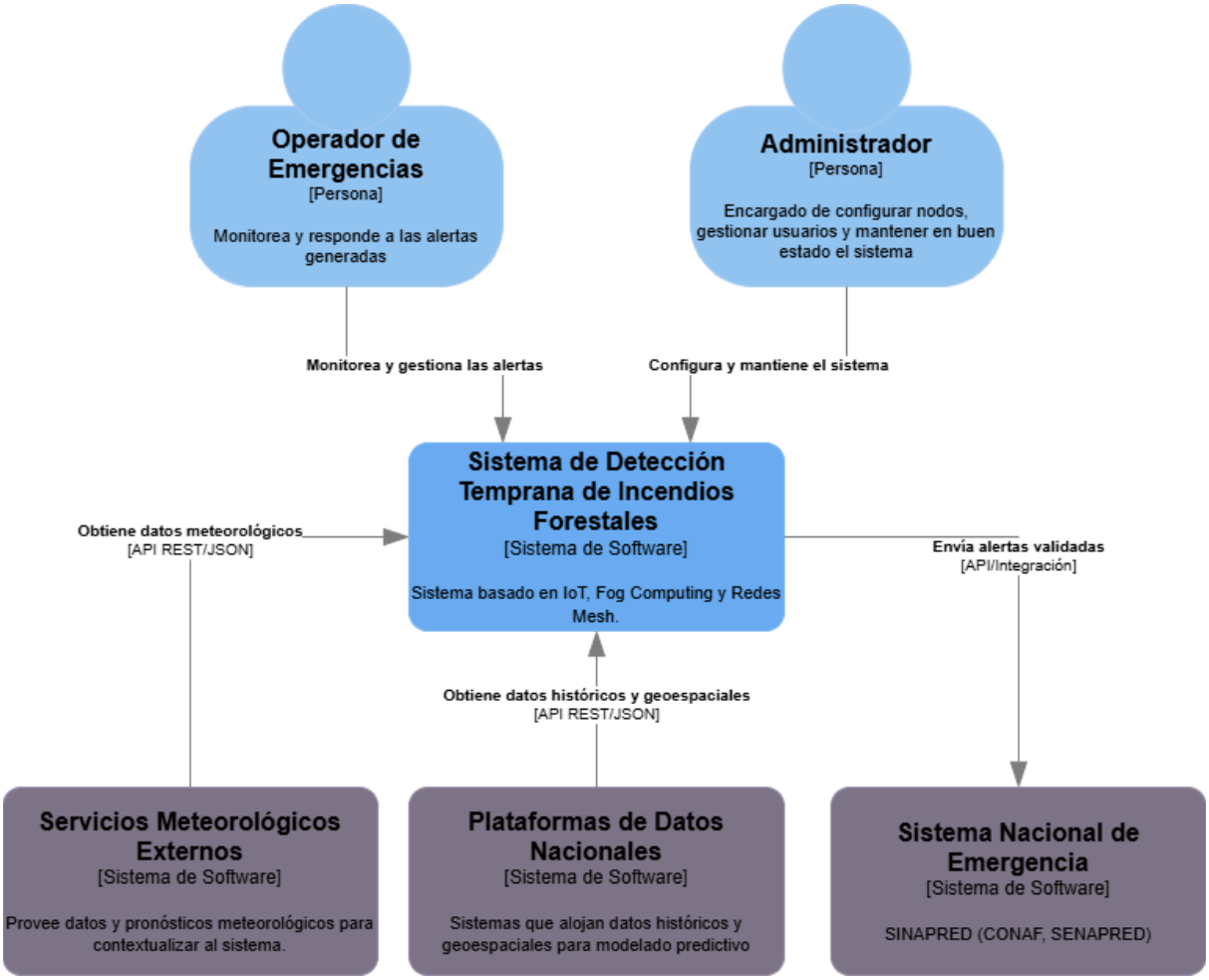
Liang, Y., Rui, X., Wang, Y., Zhang, J., Zhang, Y., Zhang, X., & Song, W. (2025). An early forest fire detection algorithm base on Multi-Sensor data fusion. *SSRN*. https://doi.org/10.2139/ssrn.5136843

Zhang, S., & Pan, M. (2024). Advancing Forest-Fire Management: Exploring Sensor Networks, Data Mining Techniques, and SVM Algorithm for Prediction. Prevention And Treatment Of Natural Disasters, 3(2). https://doi.org/10.54963/ptnd.v3i2.271

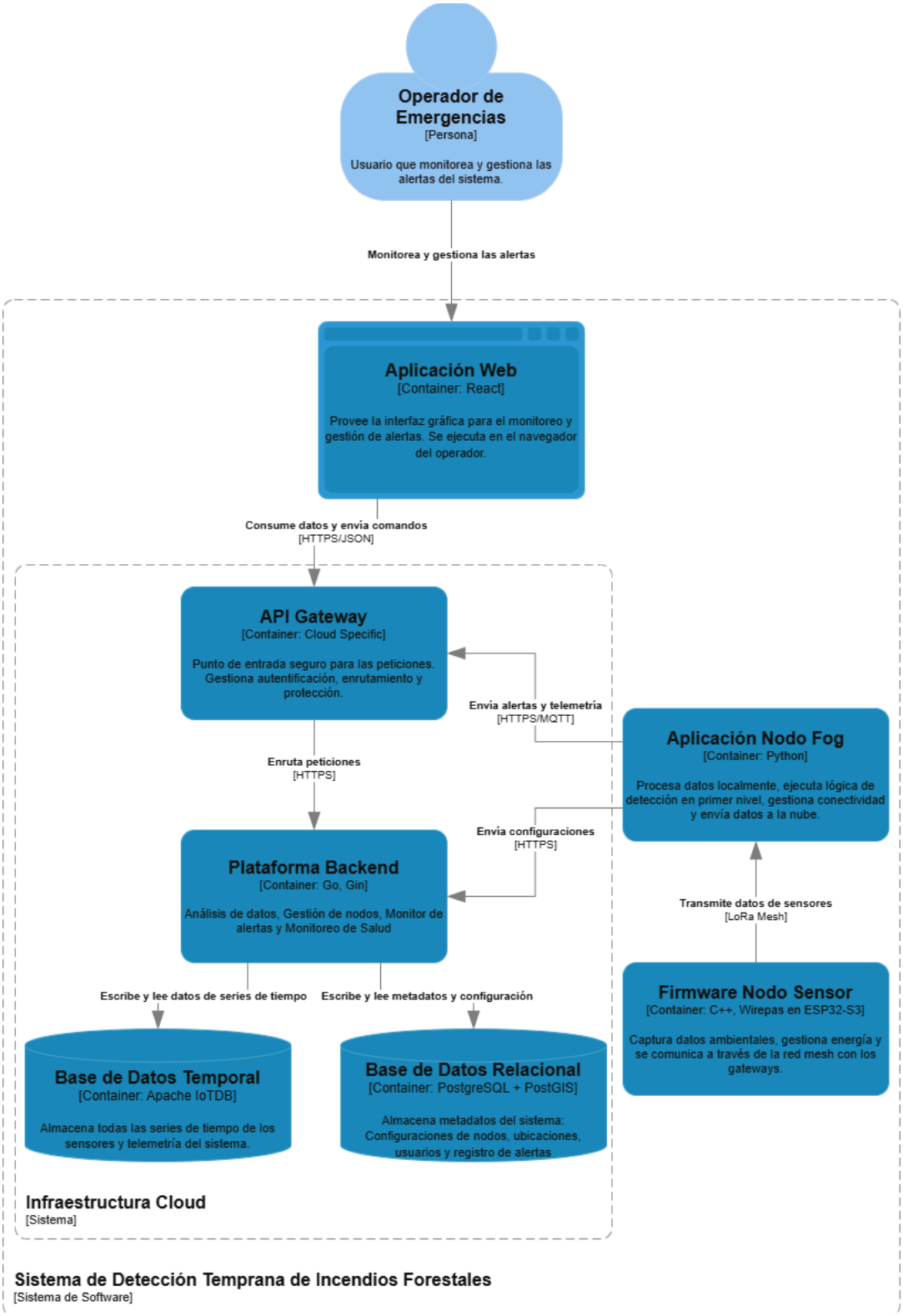
Özel, B., Alam, M. S., & Khan, M. U. (2024). Review of Modern Forest Fire Detection Techniques: Innovations in Image Processing and Deep Learning. Information, 15(9), 538. https://doi.org/10.3390/info15090538

ANEXOS

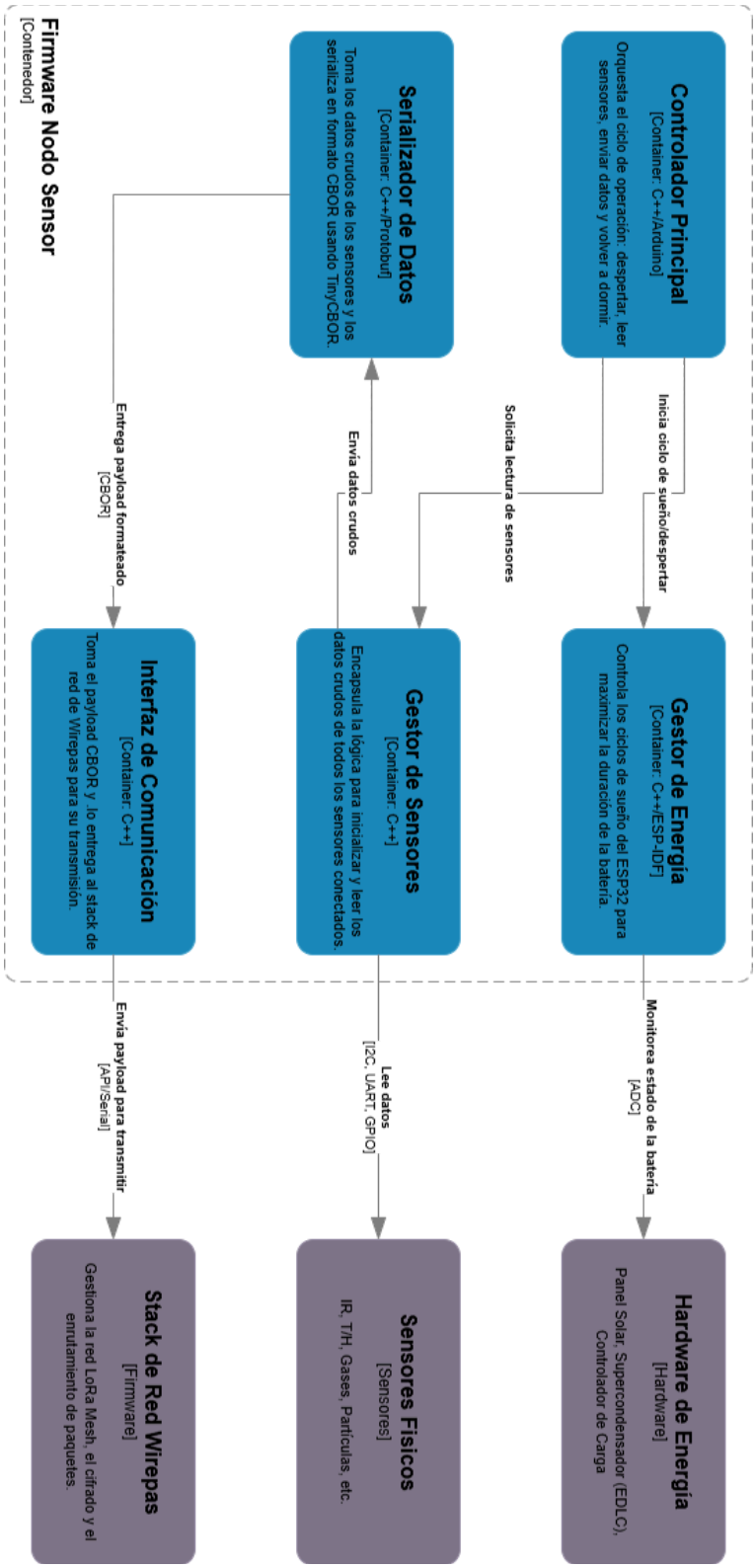
Anexo A: Diagrama C4 Nivel 1 (Contexto)



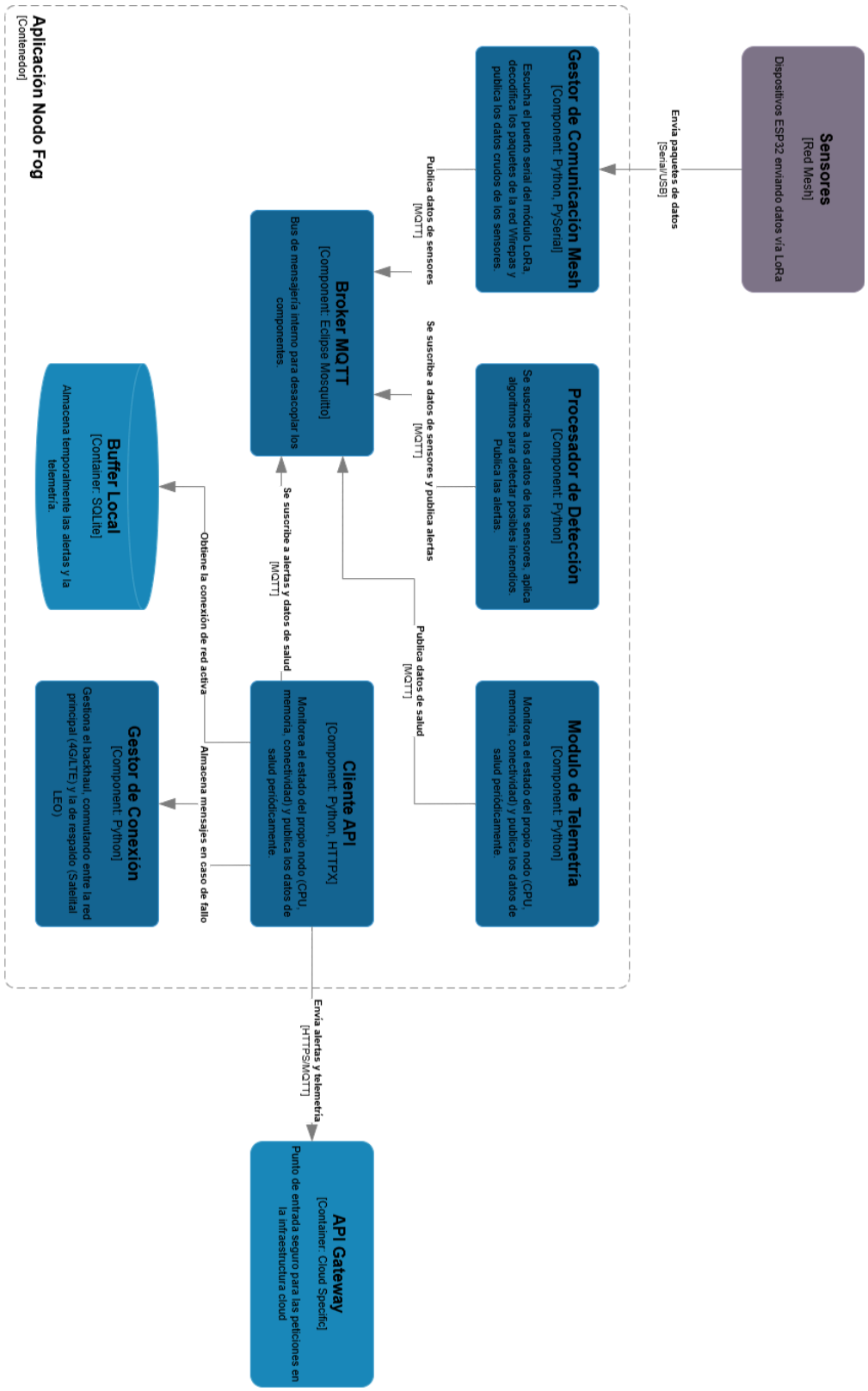
Anexo B: Diagrama C4 Nivel 2 (Contenedores)



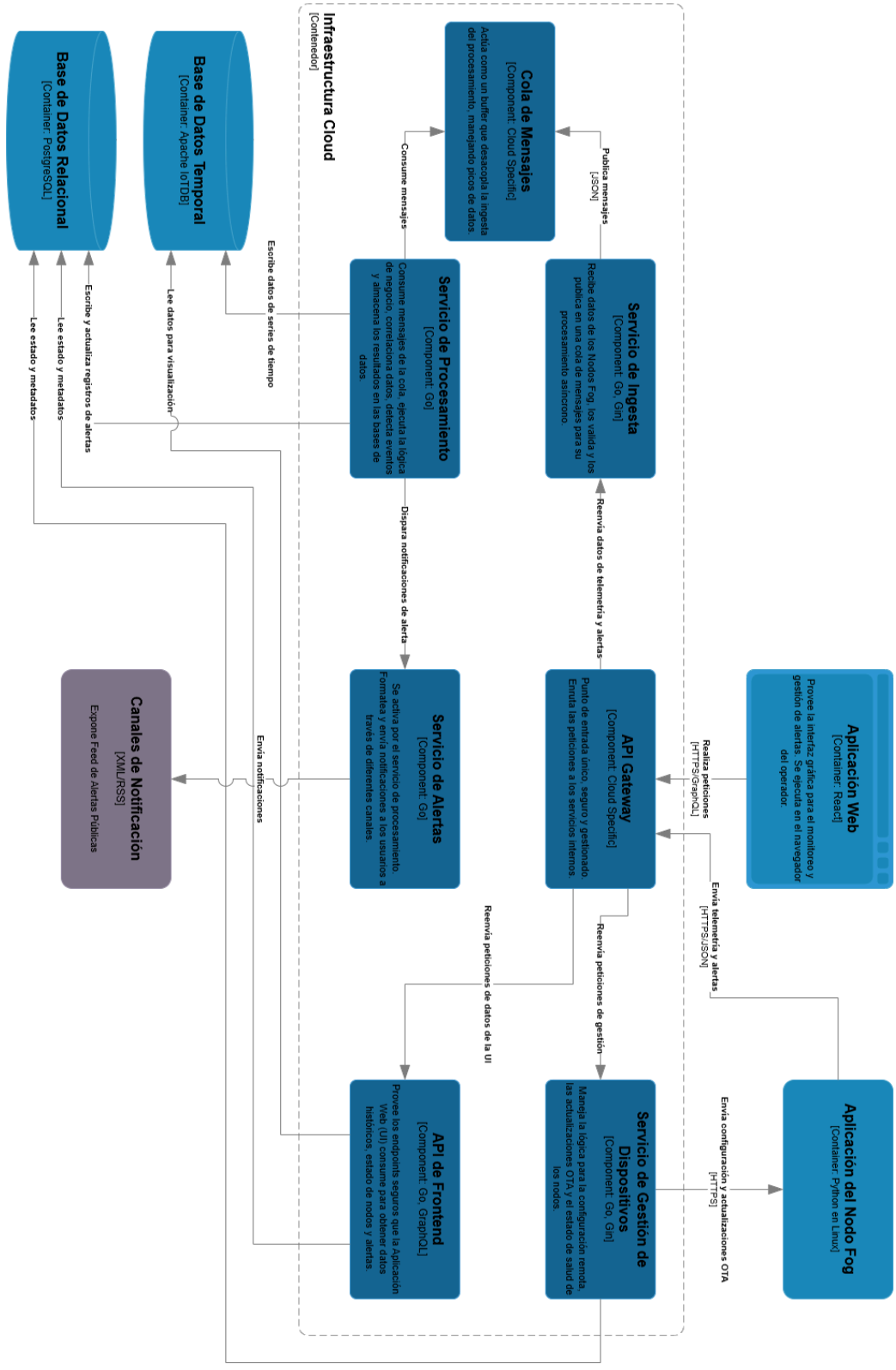
Anexo C: Diagrama C4 Nivel 3 (Firmware Nodo Sensor)



Anexo D: Diagrama C4 Nivel 3 (Aplicación Nodo Fog)



Anexo E: Diagrama C4 Nivel 3 (Infraestructura Cloud)



Anexo F: Modelo Entidad-Relación