



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



# Arquitectura de interoperabilidad para mejorar las capacidades de Análisis de Información y Toma de Decisiones

Departamento de Comunicaciones  
*Universitat Politècnica de València*

Tesis presentada para la obtención del grado de  
*Doctor por la Universitat Politècnica de  
València*

Valencia, Marzo de 2024

Autor:  
Víctor Javier Garrido Peñalver

Director:  
Dr. Manuel Esteve Domingo  
Codirector:  
Dr. Francisco José Pérez Carrasco



*A mis padres y a mis hermanos*



# Resumen

Esta tesis presenta un análisis profundo y soluciones innovadoras para los retos abordados en la Investigación Criminal (IC) y la Gestión de Emergencias (GE), con un enfoque particular en la colaboración interagencial y el manejo de datos en entornos complejos. La investigación comienza estableciendo la relevancia de una colaboración eficaz entre diversas agencias para el manejo efectivo de la información en la era digital, especialmente en el contexto de la IC y la GE. Se destaca cómo la proliferación del contenido digital y la generación masiva de datos han transformado estos campos, presentando tanto oportunidades como desafíos significativos.

La tesis revisa exhaustivamente el estado del arte en estas áreas, identificando las principales limitaciones y posibilidades de desarrollo. Se analizan aspectos críticos como la gestión de la información, las tecnologías de Big Data (BD), la respuesta rápida en emergencias, la interoperabilidad y la colaboración entre agencias, y los desafíos tecnológicos en sistemas complejos. Asimismo, se exploran cuestiones como la gestión de datos heterogéneos, la escasez de recursos y formación y los desafíos asociados al volumen y complejidad de los datos.

Respondiendo a estos desafíos, se propone una arquitectura innovadora que aborda la eficiencia e interoperabilidad de los sistemas actuales en la prevención y resolución de crímenes y en la GE. Esta arquitectura se adapta específicamente a las necesidades de los usuarios finales de los proyectos MAGNETO y ASSISTANCE, incorporando de manera eficiente diferentes componentes de software y empleando tecnologías como RMI, SOAP, REST, y JMS. Se enfatiza la transición hacia arquitecturas basadas en microservicios, utilizando un API Gateway para mejorar la modularidad y la escalabilidad.

La aplicabilidad de esta arquitectura se demuestra en los proyectos MAGNETO y ASSISTANCE, donde se abordan retos específicos. MAGNETO, enfocado en la lucha contra el crimen, integra y analiza datos de diversas fuentes, mientras que ASSISTANCE se centra en la mejora de la Situational Awareness (SA) de los First Responders (FR) mediante la integración de tecnologías avan-

## RESUMEN

---

zadas como UAVs, robots, y sistemas de realidad virtual y aumentada. Ambos proyectos demuestran una mejora significativa en la colaboración interagencial y la efectividad en situaciones de emergencia y lucha contra el crimen.

Finalmente, la tesis concluye con una reflexión sobre los logros obtenidos y plantea posibles áreas de investigación para el futuro. Se sugiere expandir la aplicación de la arquitectura a otros contextos, abordando barreras como la del idioma en la interoperabilidad y explorando la integración de tecnologías emergentes como la realidad aumentada y el IoT. Se pone el énfasis en la necesidad de continuar mejorando las capacidades de respuesta ante emergencias y la lucha contra el crimen en la era digital. La tesis representa un avance significativo en estos campos, proporcionando soluciones tecnológicas avanzadas y abriendo caminos para futuras investigaciones y desarrollos.

# Resum

Aquesta tesi presenta una anàlisi profunda i solucions innovadores per als reptes abordats en la Investigació Criminal (IC) i la Gestió d'Emergències (GE), amb un enfocament particular en la col·laboració interagencial i la gestió de dades en entorns complexos. La investigació comença establint la rellevància d'una col·laboració eficaç entre diverses agències per al maneig efectiu de la informació en l'era digital, especialment en el context de la IC i la GE. Es destaca com la proliferació del contingut digital i la generació massiva de dades han transformat aquests camps, presentant tant oportunitats com desafiaments significatius.

La tesi revisa exhaustivament l'estat de l'art en aquests camps, identificant les principals limitacions i oportunitats per a millores. S'analitzen aspectes crítics com la gestió de la informació, les tecnologies de Big Data (BD), la resposta ràpida en emergències, la interoperabilitat i la col·laboració entre agències, i els desafiaments tecnològics en sistemes complexos. També s'examinen problemes com la gestió de dades heterogènies, l'escassetat de recursos i capacitat, i els desafiaments associats amb el volum i complexitat de les dades.

Responent a aquests desafiaments, es proposa una arquitectura innovadora que aborda l'eficiència i interoperabilitat dels sistemes actuals en la prevenció i resolució de crims i en la GE. Aquesta arquitectura s'adapta específicament a les necessitats dels usuaris finals dels projectes MAGNETO i ASSISTANCE, integrant eficaçment components de software diversos i utilitzant tecnologies com RMI, SOAP, REST, i JMS. S'emfatitza la transició cap a arquitectures basades en microserveis, utilitzant un API Gateway per a millorar la modularitat i l'escalabilitat.

L'aplicabilitat d'aquesta arquitectura es demostra en els projectes MAGNETO i ASSISTANCE, on s'aborden reptes específics. MAGNETO, enfocat en la lluita contra el crim, integra i analitza dades de diverses fonts, mentre que ASSISTANCE es centra en la millora de la Situational Awareness (SA) dels First Responders (FR) mitjançant la integració de tecnologies avançades com UAVs,

## RESUM

---

robots, i sistemes de realitat virtual i augmentada. Ambdós projectes demostren una millora significativa en la col·laboració interagencial i l'efectivitat en situacions d'emergència i lluita contra el crim.

Finalment, la tesi conclou amb una reflexió sobre els assoliments obtinguts i proposa futures línies d'investigació. Es suggereix expandir l'aplicació de l'arquitectura a altres contextos, abordant barreres com la de l'idioma en la interoperabilitat i explorant la integració de tecnologies emergents com la realitat augmentada i l'IoT. S'emfatitza la necessitat de continuar millorant les capacitats de resposta davant emergències i la lluita contra el crim en l'era digital. La tesi representa un avanç significatiu en aquests camps, proporcionant solucions tecnològiques avançades i obrint camins per a futures investigacions i desenvolupaments.



# Abstract

This thesis presents an in-depth analysis and innovative solutions to the challenges faced in Criminal Investigation (CI) and Emergency Management (EM), with a particular focus on interagency collaboration and data management in complex environments. The research begins by establishing the importance of effective collaboration between various agencies for efficient information management in the digital age, especially in the context of CI and EM. It highlights how the proliferation of digital content and massive data generation have transformed these fields, presenting both opportunities and significant challenges.

The thesis thoroughly reviews the state of the art in these fields, identifying major limitations and opportunities for improvements. Critical aspects such as information management, Big Data (BD) technologies, rapid response in emergencies, interoperability, and collaboration between agencies, and technological challenges in complex systems are analyzed. Issues such as the management of heterogeneous data, resource scarcity and training, and challenges associated with data volume and complexity are also examined.

In response to these challenges, an innovative architecture is proposed that addresses the efficiency and interoperability of current systems in crime prevention and resolution and in EM. This architecture is specifically tailored to the end-user needs of the MAGNETO and ASSISTANCE projects, efficiently integrating various software components and utilizing technologies such as RMI, SOAP, REST, and JMS. The transition to architectures based on microservices is emphasized, using an API Gateway to improve modularity and scalability.

The applicability of this architecture is demonstrated in the MAGNETO and ASSISTANCE projects, where specific challenges are addressed. MAGNETO, focused on combating crime, integrates and analyzes data from various sources, while ASSISTANCE focuses on improving the Situational Awareness (SA) of First Responders (FR) through the integration of advanced technologies such as UAVs, robots, and virtual and augmented reality systems. Both projects demonstrate significant improvements in interagency collaboration and effectiveness in emergencies and crime fighting.

## ABSTRACT

---

Finally, the thesis concludes with a reflection on the achievements obtained and proposes future lines of research. It suggests expanding the application of the architecture to other contexts, addressing barriers such as language in interoperability, and exploring the integration of emerging technologies like augmented reality and IoT. The need to continue improving response capabilities in emergencies and combating crime in the digital age is emphasized. The thesis represents a significant advancement in these fields, providing advanced technological solutions and paving the way for future research and developments.

# Agradecimientos

En primer lugar, quiero expresar mi más profundo agradecimiento al Prof. D. Manuel Esteve Domingo, por haberme brindado esta valiosa oportunidad. Por acogerme en el grupo SATRD y brindarme la oportunidad de formar parte de él. Estoy muy agradecido por su confianza y permitirme conocer a personas maravillosas.

También quiero agradecer enormemente a mi codirector, Francisco José Pérez Carrasco, por su constante respaldo, sus sabios consejos y dedicación inagotable para revisar y mejorar mi trabajo, demostrando un compromiso excepcional en cada etapa del proceso.

A mi compañero de FAVIT, Alberto, por haber estado a mi lado durante todo este trayecto. Me llena de alegría haber podido comenzar esta aventura juntos y por haberme brindado esos momentos de distracción y diversión que me permitieron desconectar y recargar energías.

Asimismo, agradecer a cada uno de mis compañeros del grupo de investigación de SATRD, quienes han contribuido a hacer que mi experiencia laboral sea más placentera y enriquecedora, día tras día.

Agradezco a mi familia, quienes siempre han estado a mi lado, brindándome su incondicional apoyo en cada decisión importante. Han celebrado conmigo cada logro y me han respaldado en cada tropiezo, siendo un pilar fundamental en mi camino.

Muchas gracias a todos.

Víctor Javier Garrido Peñalver  
Valencia, Diciembre de 2023

## AGRADECIMIENTOS

---

# Índice

Índice de figuras	XIII
Índice de tablas	XIX
Acrónimos	XXI
<b>1. Introducción</b>	<b>1</b>
1.1. Introducción . . . . .	1
1.2. Motivación de la tesis . . . . .	4
1.3. Objetivos de la tesis . . . . .	5
1.4. Principales aportaciones . . . . .	6
1.4.1. Artículos . . . . .	6
1.4.2. Congresos y Jornadas . . . . .	6
1.4.3. Proyectos de investigación . . . . .	7
1.4.4. Desarrollo software . . . . .	8
1.5. Estructura de la memoria . . . . .	8
<b>2. Estado del arte</b>	<b>11</b>
2.1. Introducción . . . . .	11
2.2. Capacidades de las organizaciones de emergencias y seguridad .	12
2.2.1. Recolección y gestión de datos . . . . .	14
2.2.2. Análisis de datos . . . . .	15
2.2.3. Colaboración y comunicación interagencial . . . . .	16
2.3. Problemáticas y desafíos . . . . .	19
2.3.1. Problemáticas en la Investigación Criminal . . . . .	19
2.3.2. Problemáticas en la Gestión de Emergencias . . . . .	20
2.3.3. Silos de datos y falta de integración . . . . .	21
2.3.4. Volumen y complejidad de los datos . . . . .	22
2.3.5. Limitaciones tecnológicas y de recursos . . . . .	24
2.4. Big data en la operativa interagencial . . . . .	25

## ÍNDICE

---

2.4.1.	Big Data y Seguridad Pública: definición y características clave . . . . .	26
2.4.2.	Revolucionando la investigación forense: El potencial del Big Data . . . . .	28
2.4.3.	Innovando en la respuesta y Gestión de Emergencias: El Big Data marcando diferencias . . . . .	29
2.5.	Interoperabilidad entre agencias . . . . .	30
2.5.1.	La Interoperabilidad como pilar en la resolución de operativas conjuntas . . . . .	31
2.5.2.	Comunicación y colaboración entre agencias . . . . .	32
2.5.3.	Modelos de datos para la interoperabilidad . . . . .	36
2.5.4.	Ecosistemas de datos ( <i>DataLakes</i> Interoperables) . . . . .	38
2.6.	Herramientas de análisis, visualización y toma de decisiones . . . . .	41
2.6.1.	Tecnologías y herramientas para el análisis . . . . .	41
2.6.2.	Visualización de datos en la investigación y toma de decisiones . . . . .	42
2.7.	Otras herramientas de apoyo y optimización de recursos . . . . .	43
2.7.1.	Despliegue y automatización . . . . .	43
2.7.2.	Comunicación y orquestación . . . . .	44
<b>3.</b>	<b>Especificación de la Arquitectura</b> . . . . .	<b>45</b>
3.1.	Introducción . . . . .	45
3.2.	Visión general de la arquitectura . . . . .	46
3.3.	Adquisición de datos . . . . .	52
3.3.1.	Entorno de Prevención e investigación . . . . .	52
3.3.2.	Entorno de intervención rápida . . . . .	53
3.3.3.	DB-MANAGER . . . . .	55
3.4.	Fusión de datos . . . . .	57
3.4.1.	Modelo de Representación Común . . . . .	57
3.5.	Análisis de datos . . . . .	58
3.5.1.	Postprocess-Manager . . . . .	59
3.5.2.	Módulos de análisis . . . . .	62
3.6.	Representación de los datos . . . . .	64
<b>4.</b>	<b>Caso 1: MAGNETO</b> . . . . .	<b>67</b>
4.1.	Introducción . . . . .	67
4.2.	Objetivos de MAGNETO . . . . .	68
4.2.1.	Objetivos Científicos-Técnicos . . . . .	68
4.2.2.	Objetivos Operacionales . . . . .	69
4.3.	Arquitectura de MAGNETO . . . . .	70
4.3.1.	Servicios Big Data . . . . .	76

4.3.2.	Servicios de Traducción Automática . . . . .	80
4.3.3.	Servicios de Indexado y Filtrado Multimedia . . . . .	82
4.3.4.	Servicios de Procesamiento Semántico . . . . .	84
4.3.5.	Servicios de minería de Texto y Datos . . . . .	85
4.3.6.	Inteligencia Aumentada . . . . .	87
4.3.7.	Herramientas de Administración . . . . .	90
4.4.	Logros de MAGNETO . . . . .	92
<b>5.</b>	<b>Caso 2: ASSISTANCE</b>	<b>105</b>
5.1.	Introducción . . . . .	105
5.2.	Objetivos de ASSISTANCE . . . . .	107
5.3.	Arquitectura de ASSISTANCE . . . . .	108
5.3.1.	Módulo SAP . . . . .	112
5.3.2.	Sensores . . . . .	120
5.3.3.	Capa de red . . . . .	129
5.3.4.	Módulo SAS . . . . .	133
5.3.5.	Intercambio de información entre diferentes módulos . .	134
5.4.	Logros de ASSISTANCE . . . . .	138
<b>6.</b>	<b>Evaluación</b>	<b>147</b>
6.1.	MAGNETO . . . . .	148
6.1.1.	Escenario de pruebas . . . . .	148
6.1.2.	Caso de uso: Investigación en el ataque de una Infraestructura Crítica . . . . .	154
6.1.3.	Demostraciones . . . . .	158
6.2.	Valoración de los usuarios finales . . . . .	160
6.3.	ASSISTANCE . . . . .	160
6.3.1.	Escenario de pruebas . . . . .	160
6.3.2.	Caso de uso 1: Terremoto en Izmir . . . . .	168
6.3.3.	Caso de uso 2: Incendio en una petroquímica de Rotterdam	174
6.3.4.	Caso de uso 3: Ataque terrorista en Sevilla . . . . .	176
6.3.5.	Demostraciones . . . . .	181
6.4.	Valoración de los usuarios finales . . . . .	189
<b>7.</b>	<b>Conclusiones y líneas de trabajo futuras</b>	<b>191</b>
7.1.	Conclusiones finales . . . . .	191
7.1.1.	Conclusiones generales . . . . .	191
7.1.2.	MAGNETO . . . . .	194
7.1.3.	ASSISTANCE . . . . .	196
7.2.	Líneas futuras . . . . .	198

## ÍNDICE

---

Referencias

201



# Índice de figuras

1.1. Ataques terroristas por causa en Europa 2006-2022 [1] . . . . .	1
1.2. Perdidas mundiales por catástrofes naturales, 1980-2018 . . . . .	2
2.1. Fases en la Gestión de Emergencias . . . . .	12
2.2. Fases en una acción conjunta . . . . .	13
2.3. Las 3 Vs del Big Data . . . . .	26
2.4. Arquitecturas de intercambio de mensajes más utilizadas . . . . .	33
2.5. Ecosistema Big Data actual . . . . .	43
3.1. Arquitectura Monolítica . . . . .	49
3.2. Arquitectura de Microservicios . . . . .	49
3.3. Arquitectura REST + AMQP . . . . .	50
3.4. Arquitectura Propuesta . . . . .	51
3.5. Fuentes de Datos Prevención / Investigación . . . . .	54
3.6. DB Manager . . . . .	56
3.7. Postprocess Manager . . . . .	59
3.8. Módulo de Análisis . . . . .	63
3.9. Arquitectura HMI . . . . .	66
4.1. Concepto MAGNETO . . . . .	68
4.2. Arquitectura Plataforma MAGNETO . . . . .	71
4.3. Arquitectura MAGNETO basada en microservicios . . . . .	75
4.4. Orquestación Bases de datos . . . . .	77
4.5. Arquitectura módulo Traducción Automática . . . . .	81
4.6. Extracción Características Vídeo . . . . .	83
4.7. Esquema Speech-to-Text . . . . .	83
4.8. Ejemplo de Text Mining - Interrogatorio Sospechoso . . . . .	86
4.9. Ejemplo salida Text Mining - Registro viviendas . . . . .	87
4.10. Esquema Inteligencia Aumentada MAGNETO . . . . .	87

## ÍNDICE DE FIGURAS

---

4.11. Esquema Módulo de VR . . . . .	88
4.12. Esquema Módulo Web-GIS . . . . .	89
4.13. Esquema Integración Servicios WEB HMI . . . . .	90
4.14. Flujo Autorización y Autenticación . . . . .	92
4.15. Creación Caso de uso . . . . .	94
4.16. Ejemplo Dataset Cifrado . . . . .	95
4.17. Dataset Policía Sabadell . . . . .	95
4.18. JSON Dataset . . . . .	96
4.19. Prueba Visualización VR . . . . .	97
4.20. Dataset en Gafas VR . . . . .	97
4.21. Dataset en GIS HMI . . . . .	97
4.22. Prototipo Leap Motion . . . . .	98
4.23. Trajectory Fusion . . . . .	99
4.24. Ejemplo DROP Component . . . . .	99
4.25. Face Detection & Recognition . . . . .	100
4.26. Resultados Sentiment Analysis . . . . .	101
4.27. Resultados Keyword Extraction . . . . .	102
4.28. Resultado Semantic Reasoning . . . . .	103
4.29. Semantic Reasoning - Knowledge Base . . . . .	103
5.1. Concepto ASSISTANCE . . . . .	106
5.2. Arquitectura ASSISTANCE alto nivel . . . . .	108
5.3. Arquitectura Sistema ASSISTANCE . . . . .	109
5.4. Modelo de Datos Sensores . . . . .	111
5.5. UAV Matrice DJI . . . . .	113
5.6. Video Fusion SAP . . . . .	114
5.7. Flujo datos CBRN . . . . .	115
5.8. Visualización Pluma Tóxica . . . . .	115
5.9. Arquitectura módulo DALR . . . . .	116
5.10. Ejemplo Ruta Evacuación . . . . .	117
5.11. Intercambio Información SAP . . . . .	118
5.12. Mensajes . . . . .	118
5.13. Definición de Áreas . . . . .	119
5.14. Medida de Distancia . . . . .	119
5.15. Vista 3D . . . . .	119
5.16. Video UAV . . . . .	121
5.17. Señales Vitales FR . . . . .	121
5.18. Medidas Sensores Gas . . . . .	121
5.19. Flujo dato UAV . . . . .	123
5.20. Plataforma Robot . . . . .	124
5.21. PIAP GRYF . . . . .	124

## ÍNDICE DE FIGURAS

---

5.22. GCS Robot . . . . .	125
5.23. Dispositivo Cosinuss Two . . . . .	127
5.24. Flujo Datos Cosinuss . . . . .	127
5.25. Cámaras AXIS . . . . .	128
5.26. Aplicación Traccar . . . . .	129
5.27. Flujo datos Traccar . . . . .	129
5.28. Arquitectura de Red ASSISTANCE . . . . .	130
5.29. Terminales radio . . . . .	131
5.30. Esquema Red ASSISTANCE . . . . .	132
5.31. C2 móvil . . . . .	133
5.32. Flujo datos SAS . . . . .	135
5.33. Comunicación SAS . . . . .	135
5.34. Comunicación SAP . . . . .	136
5.35. Comunicación CHT . . . . .	137
5.36. Comunicación MMM . . . . .	138
5.37. Puntos Acceso wifi integrado en <i>Unmanned Aerial Vehicle</i> (UAV)s	139
5.38. Operativa Enjambre UAVs . . . . .	140
5.39. Captura UAV en Ejercicio Real . . . . .	140
5.40. Operativa Robots . . . . .	141
5.41. Operativa Tablet en Campo . . . . .	142
5.42. Pluma tóxica . . . . .	143
5.43. Sensores de gas . . . . .	143
5.44. Posicionamiento Unidades . . . . .	144
5.45. Frecuencia Cardíaca Unidad . . . . .	144
5.46. Rutas de Evacuación . . . . .	144
6.1. Entorno de virtualización VMware . . . . .	148
6.2. Detalle de las máquinas virtuales en los servidores . . . . .	149
6.3. Caso de uso propuesto por el Departamento de Policía de Múnich	154
6.4. Ejemplo de informes policiales introducidos en el módulo de <i>TextMining</i> . . . . .	155
6.5. Resultados generados por el módulo <i>TextMining-Result</i> . . . . .	155
6.6. Ejemplo de detección por medio del módulo <i>FaceRecognition</i> . . . . .	156
6.7. Resultados del módulo de extracción de datos de <i>Smartphones</i> . . . . .	156
6.8. Resultados del módulo de análisis semántico . . . . .	157
6.9. Eventos en los que se demostró la plataforma MAGNETO . . . . .	158
6.10. Pantalla de acceso a la plataforma . . . . .	159
6.11. Lista de análisis a ejecutar . . . . .	159
6.12. Análisis de reconocimiento de matrículas . . . . .	159
6.13. Análisis de detección de personas . . . . .	159
6.14. Análisis de fusión de trayectorias . . . . .	159

## ÍNDICE DE FIGURAS

---

6.15. Representación de resultados de <i>hotspots</i> . . . . .	159
6.16. Entorno híbrido CLOUD-EDGE VMware . . . . .	161
6.17. Detalle de las máquinas virtuales en los servidores . . . . .	162
6.18. Estado inicial del ejercicio . . . . .	168
6.19. Primera misión a los UAVs . . . . .	170
6.20. Los FRs y los comandantes comienzan los rescates . . . . .	170
6.21. Evolución de la situación debido al uso de las herramientas AS- SISTANCE . . . . .	171
6.22. Segunda misión a los UAVs . . . . .	173
6.23. Fin del ejercicio . . . . .	173
6.24. Primera misión de UAVs y robots . . . . .	174
6.25. Localización de fuegos y víctimas . . . . .	175
6.26. Definición de perímetros de peligro y zonas seguras . . . . .	175
6.27. Localización de los FRs en el terreno . . . . .	176
6.28. Estado inicial del escenario . . . . .	177
6.29. Primera misión de los UAVs . . . . .	178
6.30. El enjambre de robots y UAVs trabajan en el escenario . . . . .	179
6.31. UAV hostil y piloto terrorista neutralizados . . . . .	180
6.32. Explosivo desactivado y víctimas rescatadas . . . . .	181
6.33. Envío de mensajes y operativas desde el puesto de mando y control	182
6.34. Recepción de mensajes en el terreno . . . . .	182
6.35. Preparación de los UAVs y las cámaras . . . . .	182
6.36. Vídeos en la SAP . . . . .	182
6.37. Vídeos en las tablets . . . . .	182
6.38. Rescates de víctimas . . . . .	183
6.39. Equipo implicado en la demostración . . . . .	183
6.40. Envío de mensajes y operativas desde la SAP . . . . .	184
6.41. Recepción de mensajes en el terreno . . . . .	184
6.42. Preparación de los UAVs y las cámaras . . . . .	185
6.43. Vídeos y sensores en las tablets . . . . .	185
6.44. Flujos de vídeo y sensores en la SAP . . . . .	185
6.45. Rescates de víctimas . . . . .	185
6.46. Equipo implicado en la demostración . . . . .	186
6.47. Envío de mensajes pre-generados desde el terreno . . . . .	187
6.48. Recepción de mensajes en la SAP . . . . .	187
6.49. Enjambre de UAVs para mejora de cobertura . . . . .	187
6.50. UAV captor con la red de captura instalada . . . . .	187
6.51. Captura de UAV hostil en vuelo por el UAV captor . . . . .	187
6.52. Robot de los TEDAX acercándose al objeto sospechoso . . . . .	188
6.53. Robot acercándose al objetivo . . . . .	188
6.54. Inspección del objetivo . . . . .	188

## ÍNDICE DE FIGURAS

---

6.55. Rescates de víctimas . . . . .	188
6.56. Equipo implicado en la demostración . . . . .	189

## ÍNDICE DE FIGURAS

---

# Índice de tablas

4.1. Componentes del MBDF y sus Implementaciones . . . . .	76
4.2. Operaciones HTTP y sus Acciones . . . . .	78
4.3. Operaciones HTTP y sus Formatos . . . . .	79
4.4. Operaciones API y sus Formatos . . . . .	80
4.5. Operaciones y Formatos en Elasticsearch . . . . .	81
4.6. Colores y Tipos de Incidentes . . . . .	96
6.1. Actores Involucrados en la investigación . . . . .	153
6.2. Datasets Utilizados en la investigación . . . . .	153
6.3. Tabla de valoración de los usuarios finales . . . . .	160
6.4. Actores Involucrados en el Terremoto de Izmir . . . . .	165
6.5. Datasets y Fuentes de Datos del Escenario del Terremoto . . .	165
6.6. Actores Involucrados en el Incidente Petroquímico de Rotterdam	165
6.7. Datasets y Fuentes de Datos del Escenario Petroquímico . . . .	166
6.8. Actores Involucrados del Ataque Terrorista en Sevilla . . . . .	166
6.9. Datasets y fuentes de datos del Ataque Terrorista en Sevilla . .	166
6.10. Resumen de Comentarios y Puntuaciones de las Pruebas Piloto	190

## ÍNDICE DE TABLAS

---



# Acrónimos

<b>AA</b>	<i>Autenticación y Autorización</i>
<b>AAHD</b>	<i>Acil Afet Ambulans Hekimleri Derneği</i>
<b>ACRIMAS</b>	<i>Aftermath Crisis Management System-of-systems Demonstration</i>
<b>ADN</b>	<i>Ácido Desoxirribonucleico</i>
<b>AMQP</b>	<i>Advanced Message Queuing Protocol</i>
<b>API</b>	<i>Application Programming Interface</i>
<b>AR</b>	<i>Augmented Reality</i>
<b>ASSISTANCE</b>	<i>Adapted situation awareness tools and tailored training scenarios for increasing capabilities and enhancing the protection of first responders</i>
<b>AWS</b>	<i>Amazon Web Services</i>
<b>BD</b>	<i>Big Data</i>
<b>BLE</b>	<i>Bluetooth Low Energy</i>
<b>C2</b>	<i>Command &amp; Control</i>
<b>CAN</b>	<i>Controller Area Network</i>
<b>CAP</b>	<i>Common Alerting Protocol</i>
<b>CBRN</b>	<i>Chemical, Biological, Radiological and Nuclear</i>
<b>CCTV</b>	<i>Closed Circuit Television</i>
<b>CHT</b>	<i>Chemical Hazard Tool</i>
<b>CNBOP</b>	<i>Scientific and Research Centre for Fire Protection</i>
<b>CO</b>	<i>Monóxido de Carbono</i>
<b>CO2</b>	<i>Dióxido de Carbono</i>
<b>CRM</b>	<i>Common Representational Model</i>

## ACRÓNIMOS

---

<b>CRUD</b>	<i>Create, Read, Update, Delete</i>
<b>DALR</b>	<i>Damaged Assets Location Routing</i>
<b>DCS</b>	<i>Data Collection System</i>
<b>DDP</b>	<i>Datagram Delivery Protocol</i>
<b>DDS</b>	<i>Data Distribution System</i>
<b>DHCP</b>	<i>Dynamic Host Configuration Protocol</i>
<b>DISASTER</b>	<i>Data Interoperability Solution At Stakeholders</i> <i>Data Interoperability Solution At Stakeholders Emergency</i> <i>Reaction</i>
<b>DL</b>	<i>Deep Learning</i>
<b>DNN</b>	<i>Deep Neural Network</i>
<b>DNS</b>	<i>Domain Name System</i>
<b>DRIVER</b>	<i>Driving Innovation in Crisis Management for European</i> <i>Resilience</i>
<b>DROP</b>	<i>Distinctive Region or Pattern</i>
<b>DRS</b>	<i>Disaster Resilient Society</i>
<b>ECS</b>	<i>Elastic Container Service</i>
<b>EDXL</b>	<i>Emergency Data Exchange Language</i>
<b>EM</b>	<i>Evacuation Management</i>
<b>EMA</b>	<i>Emergency Management Agencies</i>
<b>EMERGEL</b>	<i>EMERGENCY Elements</i>
<b>EPOC</b>	<i>European Pool against Organised Crime</i>
<b>ESB</b>	<i>Enterprise Service Bus</i>
<b>ESO</b>	<i>Event and Situation Ontology</i>
<b>FCT</b>	<i>Fighting Crime and Terrorism</i>
<b>FR</b>	<i>First Responder</i>
<b>GB</b>	<i>Gezamenlijke Brandweer</i>
<b>GCC</b>	<i>Gestión Colaborativa de Crisis</i>
<b>GCS</b>	<i>Ground Control Station</i>
<b>GDACS</b>	<i>Global Disaster Alert and Coordination System</i>
<b>GE</b>	<i>Gestión de Emergencias</i>
<b>GIS</b>	<i>Geographic Information System</i>

<b>GML</b>	<i>Geography Markup Language</i>
<b>GPS</b>	<i>Global Positioning System</i>
<b>GPU</b>	<i>Graphics Processing Unit</i>
<b>GUI</b>	<i>Graphical User Interface</i>
<b>HD</b>	<i>High Definition</i>
<b>HDFS</b>	<i>Hadoop Distributed File System</i>
<b>HL7</b>	<i>Health Level Seven International</i>
<b>H2020</b>	<i>Horizon 2020</i>
<b>HE</b>	<i>Horizon Europe</i>
<b>HMI</b>	<i>Human Machine Interface</i>
<b>HTML</b>	<i>HyperText Markup Language</i>
<b>HTTP</b>	<i>Hypertext Transfer Protocol</i>
<b>IA</b>	<i>Inteligencia Artificial</i>
<b>IAM</b>	<i>Identity and access management</i>
<b>IC</b>	<i>Investigación Criminal</i>
<b>IMU</b>	<i>Inertial Measuring Unit</i>
<b>IoT</b>	<i>Internet of Things</i>
<b>ITS</b>	<i>Intelligent Transport Systems</i>
<b>JAUS</b>	<i>Joint Architecture for Unmanned Systems</i>
<b>JC3IEDM</b>	<i>Joint Command, Control and Communications Information Exchange Data Model</i>
<b>JMS</b>	<i>Java Message Service</i>
<b>JSON</b>	<i>JavaScript Object Notation</i>
<b>KB</b>	<i>Knowledge Base</i>
<b>LEA</b>	<i>Law Enforcement Agencie</i>
<b>LTE</b>	<i>Long Term Evolution</i>
<b>MAGNETO</b>	<i>Multimedia Analysis and correlation enGine for orgaNised crimE prevenTion and investigatiOn</i>
<b>MANET</b>	<i>Mobile Ad Hoc Network</i>
<b>MBDF</b>	<i>MAGNETO Big Data Framework</i>
<b>MEP</b>	<i>Message Exchange Pattern</i>
<b>MIC</b>	<i>Multinational Interoperability Council</i>

## ACRÓNIMOS

---

<b>MIR-PN</b>	<i>Ministerio del Interior – Policía Nacional</i>
<b>ML</b>	<i>Machine Learning</i>
<b>MLN</b>	<i>Markov Logic Network</i>
<b>MMM</b>	<i>Mission Management Module</i>
<b>MQTT</b>	<i>Message Queuing Telemetry Transport</i>
<b>NATS</b>	<i>Neural Autonomic Transport System</i>
<b>NIEM</b>	<i>National Information Exchange Model</i>
<b>NLTK</b>	<i>Natural Language Toolkit</i>
<b>NLP</b>	<i>Natural Language Processing</i>
<b>NoSQL</b>	<i>Not only SQL</i>
<b>OASIS</b>	<i>Organization for the Advancement of Structured Information Standards</i>
<b>OGC</b>	<i>Open Geospatial Consortium</i>
<b>OSPOM</b>	<i>Ochotnicza Straż Pożarna w Ożarowie Mazowieckim</i>
<b>OWL</b>	<i>Ontology Web Language</i>
<b>RDF</b>	<i>Resource Description Framework</i>
<b>REST</b>	<i>REpresentational State Transfer</i>
<b>RMI</b>	<i>Java Remote Method Invocation</i>
<b>RTSP</b>	<i>Real Time Streaming Protocol</i>
<b>S3</b>	<i>Simple Storage Service</i>
<b>SA</b>	<i>Situational Awareness</i>
<b>SAP</b>	<i>Situational Awareness Platform</i>
<b>SAS</b>	<i>Sensors Abstraction Service</i>
<b>SBFF</b>	<i>Södertörns Branförsvarsförbund Fire Brigade</i>
<b>SI</b>	<i>Sistemas de Información</i>
<b>SIG</b>	<i>Sistemas de Información Geográfica</i>
<b>SOAP</b>	<i>Simple Object Access Protocol</i>
<b>SOS</b>	<i>Sensor Observation Service</i>
<b>SUMO</b>	<i>Suggested Upper Merged Ontology</i>
<b>SUV</b>	<i>Sports Utility Vehicle</i>
<b>TEDAX</b>	<i>Técnico Especialista en Desactivación de Artefactos Explosivos</i>

<b>UAV</b>	<i>Unmanned Aerial Vehicle</i>
<b>UDDI</b>	<i>Universal Description, Discovery, and Integration</i>
<b>UE</b>	<i>Unión Europea</i>
<b>UPV</b>	<i>Universitat Politècnica de València</i>
<b>URI</b>	<i>Uniform Resource Identifier</i>
<b>URL</b>	<i>Uniform Resource Locator</i>
<b>UxV</b>	<i>Unmanned eXpeditory Vehicle</i>
<b>VPC</b>	<i>Virtual Private Cloud</i>
<b>VPN</b>	<i>Virtual Private Network</i>
<b>VR</b>	<i>Virtual Reality</i>
<b>VOSOC</b>	<i>Virtual On Site Operations Coordination Center</i>
<b>W3C</b>	<i>World Wide Web Consortium</i>
<b>WebRTC</b>	<i>Web Real-Time Communications</i>
<b>WS</b>	<i>Web Services</i>
<b>WSDL</b>	<i>Web Services Description Language</i>
<b>XML</b>	<i>eXtensible Markup Language</i>

## ACRÓNIMOS

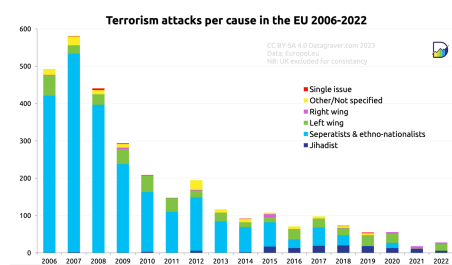
---

# Capítulo 1

## Introducción

### 1.1. Introducción

En las últimas convocatorias de la Comisión Europea en el marco de los programas *Horizon 2020* (H2020) y *Horizon Europe* (HE), más concretamente, en los *TOPIS Fighting Crime and Terrorism* (FCT) y *Disaster Resilient Society* (DRS) la investigación e innovación en seguridad y respuesta, se ha destacado como una prioridad transversal. Se han enfocado esfuerzos y recursos en estudios que avanzan en la mejora de los procesos de investigación contra el terrorismo, el crimen organizado, el cibercrimen y la gestión de desastres naturales, áreas críticas donde la evolución continua de las amenazas requiere de respuestas igualmente dinámicas y efectivas [2].



**Figura 1.1:** Ataques terroristas por causa en Europa 2006-2022 [1]

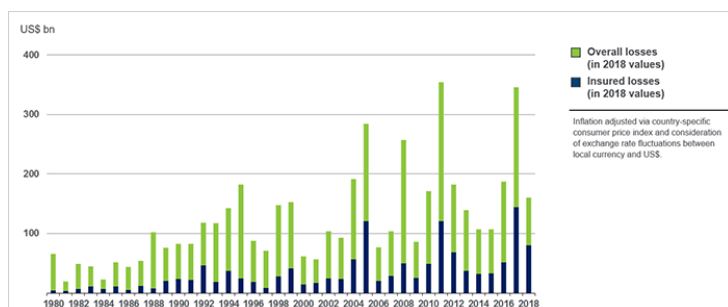
El año 2017 señaló un punto de inflexión en la *Unión Europea* (UE), registrando 205 atentados terroristas frustrados, fallidos y consumados, marcando un aumento del 45% respecto al año anterior. Este incremento pone en

## CAPÍTULO 1. INTRODUCCIÓN

---

evidencia la necesidad de una vigilancia más efectiva y sistemas de respuesta mejorados, especialmente considerando que los ataques yihadistas, aunque constituyen solo una fracción de los incidentes totales, resultaron ser desproporcionadamente letales [3].

Simultáneamente, el creciente número y la magnitud de los desastres naturales han llevado a pérdidas humanas y económicas sin precedentes, impulsando la necesidad de innovar en la *Gestión de Emergencias* (GE) [4].



**Figura 1.2:** Pérdidas mundiales por catástrofes naturales, 1980-2018

El crecimiento poblacional y la urbanización en áreas de alto riesgo han complicado la gestión de catástrofes, haciendo que las operaciones de reconstrucción sean cada vez más duraderas y costosas. La *Gestión Colaborativa de Crisis* (GCC) juega un papel vital en este contexto, aunque la falta de interoperabilidad entre los sistemas de información utilizados durante las emergencias sigue siendo un desafío significativo [5].

Existen iniciativas que buscan mejorar la interoperabilidad y la GCC, como el *Multinational Interoperability Council* (MIC) [6], el *Global Disaster Alert and Coordination System* (GDACS)[7] y el *Virtual On Site Operations Coordination Center* (VOSOC) [8]. Sin embargo, aún se necesita un enfoque común que permita gestionar las emergencias de manera integral y transfronteriza, desde la prevención hasta la respuesta, y que integre las diferentes fases de la GE tanto en el caso de incidentes naturales como en actos generados por el ser humano.

Además, la Comisión Europea ha subrayado la importancia de desarrollar sistemas y soluciones innovadoras que fortalezcan la protección de los espacios públicos [9]. Este enfoque se centra en una comprensión integral de las amenazas para identificar y priorizar medidas de protección y reacción ante cualquier tipo de situación de emergencia.

En conjunto con la aparición de la era del *Big Data* (BD), los desafíos en la *Investigación Criminal* (IC) y en la gestión de eventos se han intensifica-



do debido a la gran cantidad y diversidad de los formatos de datos. Esto ha llevado a la necesidad de herramientas analíticas capaces de procesar, analizar y extraer información relevante de enormes flujos de datos. La «vigilancia predictiva» [10] se ha convertido en un campo de interés creciente, donde el análisis de datos heterogéneos puede ayudar a predecir y prevenir actividades delictivas.

Este trabajo doctoral se desarrolla en el contexto de dos proyectos clave:

- *Multimedia Analysis and correlation enGine for orgaNised crime prevenTion and investigatiOn* (MAGNETO) [11]
- *Adapted situation awareneSS tools and taiIlored training scenarios for increaSing capabiliTies and enhANcing the proteCtion of first respondErs* (ASSISTANCE) [12]

MAGNETO se centra en el desarrollo de una arquitectura que permita el análisis y la representación avanzada de grandes volúmenes de datos para mejorar la eficiencia en ICs. Paralelamente, ASSISTANCE se dedica a aumentar las capacidades y reforzar la protección de los servicios de emergencias ante situaciones críticas, a través del desarrollo de herramientas de conciencia situacional adaptadas y escenarios de entrenamiento personalizados.

El proyecto MAGNETO desempeña un papel fundamental en la respuesta a la delincuencia organizada y el terrorismo. MAGNETO se centra en el desarrollo de una plataforma integral que integra tecnologías punteras para el análisis de datos masivos, destinadas a la prevención y la investigación de actos delictivos. A través de una arquitectura de sistemas distribuidos, MAGNETO facilita la colaboración entre diferentes organismos y entidades, proporcionando herramientas que permiten el procesamiento avanzado de datos, el análisis de correlaciones y la representación de información compleja. Esto permite a los investigadores descubrir patrones ocultos y obtener perspectivas que son críticas en la lucha contra amenazas emergentes.

El proyecto ASSISTANCE, reconociendo el papel vital que juegan los servicios de emergencias en situaciones de crisis, busca mejorar su seguridad y eficacia mediante el uso de nuevas tecnologías y formación específica. Se abordan retos como la coordinación en eventos con múltiples agencias, la comunicación efectiva en condiciones adversas, y la toma de decisiones en entornos de alto riesgo. ASSISTANCE no solo proporciona soluciones técnicas, sino que también resalta la importancia de la preparación y capacidad de adaptación de los equipos, integrando simulaciones realistas y protocolos de entrenamiento para garantizar que los equipos de emergencia puedan actuar de manera informada y coordinada.

La integración de los resultados de MAGNETO y ASSISTANCE en esta tesis doctoral pretende proporcionar un marco comprensivo que permita a las

agencias de seguridad y emergencias actuar de manera más informada, ágil y coordinada, mejorando así las estrategias de prevención, detección y respuesta ante las amenazas de seguridad modernas.

### 1.2. Motivación de la tesis

El trabajo realizado durante la presente tesis doctoral se ancla en la investigación aplicada, dirigida específicamente hacia la optimización de procesos en la investigación, la resolución de actividades delictivas y el entrenamiento y coordinación de las diferentes agencias involucradas en la GE. Inspirada por los avances en los proyectos europeos MAGNETO y ASSISTANCE, se ha desarrollado una plataforma distribuida que sincroniza diferentes herramientas para resolver escenarios de prueba y situaciones reales en ICs, así como en situaciones posteriores de emergencia derivadas de actividades delictivas tales como ataques terroristas. Las motivaciones que han impulsado la realización de esta tesis son las siguientes:

**Interoperabilidad:** Con un enorme ecosistema de herramientas para varios ámbitos, surge la necesidad de la interoperabilidad. El diseño de una plataforma que permite la combinación de diferentes herramientas y el intercambio de información entre módulos puede optimizar los tiempos y costes en la resolución de un caso.

**Arquitectura distribuida y escalable:** Ante la diversidad de plataformas en *CLOUD* y entornos privados, es fundamental que las soluciones actuales sean diseñadas considerando su potencial despliegue distribuido y escalable. Esto implica la capacidad de adaptarse a distintos entornos y escenarios, así como la incorporación de posibles herramientas futuras.

**Usabilidad:** Se debe de priorizar el diseño de una interfaz de usuario que permita utilizar las funcionalidades de la plataforma de manera centralizada, sencilla e intuitiva, adaptada a usuarios con diversos perfiles y conocimientos.

**Diseño de mensajes para el intercambio de información:** Se debe de tener en cuenta el diseño y desarrollo de un conjunto de mensajes que facilitan la comunicación entre los diferentes módulos y herramientas, esencial para la operatividad de entornos distribuidos e interoperables.

**Optimización de tiempos en la Investigación Criminal y en la respuesta en el terreno:** La plataforma debe buscar, mejorar y optimizar tareas repetitivas y el procesamiento de datos a través de herramientas BD, reduciendo así el tiempo y los recursos necesarios en ICs y en actividades de campo.

El trabajo en MAGNETO y ASSISTANCE no solo proporciona una base técnica y operativa para esta tesis, sino que también establece un marco teórico y metodológico que resalta la importancia de la innovación tecnológica en

seguridad pública. La integración de los resultados de ambos proyectos busca proporcionar soluciones avanzadas que permitan a las agencias de seguridad y emergencias actuar de manera más informada, ágil y coordinada, mejorando así las estrategias de prevención, detección y respuesta ante las amenazas de seguridad modernas.

### 1.3. Objetivos de la tesis

Tras los requisitos y necesidades dentro del campo de la IC así como en la optimización y agilización de actividades de campo dentro de la GE, se ha diseñado una serie de objetivos alineados con la motivación de la tesis que permitirán avanzar significativamente en los campos de la IC y en la GE, aprovechando las capacidades del BD y las tecnologías de la información para mejorar la interoperabilidad, la usabilidad y la eficiencia de las respuestas ante crisis.

#### 1. Análisis del Estado del Arte:

- Describir y analizar los procesos actuales y las herramientas utilizadas en la IC y la GE.
- Identificar y evaluar las herramientas de BD existentes que podrían mejorar y optimizar estos procesos.

#### 2. Interoperabilidad y Comunicación:

- Definir los mecanismos de interoperabilidad entre las herramientas analizadas, incluyendo la definición de mensajes y colas que permitan el intercambio eficaz de información y notificaciones entre las plataformas y sistemas implicados.

#### 3. Diseño y Desarrollo de la Plataforma:

- Diseñar y especificar una arquitectura distribuida que permita la interoperabilidad y la escalabilidad, basada en las necesidades identificadas en la investigación y en los casos de uso específicos.
- Desarrollar y poner en marcha sistemas de ingestión de datos que faciliten la incorporación de información a la plataforma, asegurando su adecuación a los estándares relevantes como *Common Alerting Protocol* (CAP), *Sensor Observation Service* (SOS) y *Open Geospatial Consortium* (OGC).

#### 4. Optimización de la Investigación Criminal:

- Implementar una plataforma basada en soluciones BD con el propósito de agilizar y automatizar las labores tediosas y repetitivas en el campo de la IC.
- Aplicar el modelo y la arquitectura propuesta en un caso de uso real, con el fin de verificar las mejoras en la resolución de ICs y la GE.

### 5. Validación y Evaluación:

- Utilizar los proyectos MAGNETO y ASSISTANCE como casos de estudio para aplicar y validar la arquitectura propuesta, demostrando su efectividad en la mejora de la gestión de la información y la toma de decisiones en situaciones de emergencia.
- Evaluar las mejoras conseguidas mediante la implementación del modelo y la arquitectura propuesta, tanto en términos de eficiencia operativa como en la calidad de la respuesta a emergencias y la IC.

De esta manera, abordando los objetivos de esta sección, la tesis se enfoca en proporcionar soluciones prácticas y teóricas que puedan ser adoptadas por los organismos de seguridad y emergencias, mejorando así su capacidad de operar de manera más informada, ágil y coordinada.

## 1.4. Principales aportaciones

### 1.4.1. Artículos

- Pérez, F.J., **Garrido, V.J.**, García, A. et al. *Multimedia analysis platform for crime prevention and investigation*. *Multimed Tools Appl* 80, 23681–23700 (2021). <https://doi.org/10.1007/s11042-020-10206-y>
- Pérez, F., García, A, **Garrido, V.** , Esteve, M., Zambrano, M. (2021). *C2 Advanced Multi-domain Environment and Live Observation Technologies*. *International journal of computers communications and control*. 16. 10.15837/ijccc.2021.6.4251.

### 1.4.2. Congresos y Jornadas

- Behmer, E., Chandramouli, K., **Garrido, V.**, Mühlenberg, D., Müller, D., Müller, W., Pallmer, D., Pérez, F., Piatrik, T., Vargas, C.. (2019). *Ontology Population Framework of MAGNETO for Instantiating Heterogeneous Forensic Data Modalities*. In *15th Conference on Artificial Intelligence Applications and Innovations (AIAI 2019)* 10.1007/978-3-030-19823-7\_44.

- **Garrido, V.** *Proyectos Europeos H2020: MAGNETO* in *Día Nacional de las Telecomunicaciones 2021* Universidad Técnica del Norte, Ibarra, Ecuador
- Pérez, F.J., **Garrido, V.J.**, García, A. et al. *Multimedia analysis platform for crime prevention and investigation*. *Multimedia Tools in 1st International Conference on Applied Technologies (ICAT 2019)* Universidad Técnica del Norte, Ibarra, Ecuador. <https://doi.org/10.1007/s11042-020-10206-y>
- Pérez, F.J., **Garrido, V.J.**, García, A. et al. *C2 Advanced Multi-domain Environment and Live Observation Technologies* in *1st International Conference on Applied Technologies (ICAT 2019)* Universidad Técnica del Norte, Ibarra, Ecuador.

### 1.4.3. Proyectos de investigación

- Proyecto MAGNETO:
  - WP.2 Requirements and architecture
  - WP.3 Heterogeneous Data Mining and Evidence Collection
  - WP.5 Augmented Intelligence
  - WP.6 Integration and Verification
  - WP.7 Training
  - WP.8 Demonstrations
- Proyecto ASSISTANCE:
  - WP.2 User Requirements, scenarios, and system architecture
  - WP.3 Sensor abstraction service
  - WP.4 Unmanned platforms and wearables sensors
  - WP.5 Adapted situation awareness capabilities and communications
  - WP.6 Advanced training network based on virtual and augmented reality
  - WP.7 System demonstration and validation

### 1.4.4. Desarrollo software

Durante las actividades de desarrollo en los proyectos MAGNETO y ASSISTANCE, se han logrado avances notables en la creación de componentes de software a través de las diversas capas de la arquitectura propuesta. Se ha definido un modelo de contenedores Docker genérico que se integra en el bus de comunicaciones para recibir y publicar datos esenciales. Además, se ha diseñado y desarrollado un orquestador que permite el despliegue eficiente de múltiples contenedores según sea necesario, utilizando la *Application Programming Interface* (API) que Docker ofrece.

En el contexto del proyecto MAGNETO, para facilitar la interacción con grandes conjuntos de datos, se ha implementado una API específica para el sistema de archivos distribuido HDFS. Este desarrollo clave proporciona un acceso simplificado y seguro al almacenamiento de datos masivos, esencial en el contexto del análisis de BD en las ICs.

En el marco del proyecto ASSISTANCE, se han generado resultados adicionales, incluyendo el desarrollo de sistemas de detección y respuesta para emergencias, que utilizan tecnologías avanzadas. Esto abarca desde soluciones de *Inteligencia Artificial* (IA) para la evaluación de riesgos en tiempo real hasta herramientas de simulación para entrenamientos de los servicios de emergencia, todos integrados a través de un marco cohesivo que mejora la coordinación y efectividad.

Como complemento a estas herramientas técnicas, se ha creado una serie de interfaces de usuario *Human Machine Interface* (HMI)s intuitivos que brinda acceso simplificado a los servicios integrados de la plataforma, ofreciendo una solución consolidada para el análisis complejo de datos y la presentación visual de información procesada, así como la coordinación de unidades y operativa en el terreno.

Estos avances en MAGNETO y ASSISTANCE representan un salto cualitativo en la tecnología aplicada a la seguridad pública y la GE, alineados con la estrategia general de mejorar la capacidad de respuesta y la toma de decisiones ante situaciones críticas. Los desarrollos de software obtenidos no solo incrementan la eficiencia operativa, sino que también promueven un nuevo estándar en las prácticas de seguridad mediante la innovación tecnológica.

## 1.5. Estructura de la memoria

La estructura de la memoria de la tesis se presenta de la siguiente manera, reflejando el flujo lógico y la profundidad de la investigación realizada en el marco de los proyectos MAGNETO y ASSISTANCE:

1. **Introducción:** Se presenta el contexto, motivación, objetivos y principales aportaciones del estudio. Se finaliza con una descripción de la estructura de la memoria.
2. **Estado del Arte:** Se examina el panorama actual en la GE y seguridad, con un enfoque en la necesidad de soluciones colaborativas y el uso de BD, así como los desafíos y herramientas existentes para la interoperabilidad.
3. **Especificación de la Arquitectura:** Se detalla la arquitectura propuesta, describiendo cada módulo y las posibles configuraciones, así como la adquisición, fusión, análisis y representación de datos.
4. **Caso 1: MAGNETO:** Se describe la aplicación de la arquitectura al proyecto MAGNETO, sus objetivos, desarrollo y logros, con énfasis en la mejora de la IC.
5. **Caso 2: ASSISTANCE:** Se expone la aplicación de la arquitectura al proyecto ASSISTANCE, detallando sus objetivos, arquitectura y logros, destacando las mejoras en la protección y eficiencia de los servicios de emergencia.
6. **Evaluación:** Se evalúan los sistemas diseñados en ambos casos, se presentan los escenarios de prueba y se analizan los resultados obtenidos.
7. **Conclusiones y Líneas de Trabajo Futuras:** Se presentan las conclusiones finales y se proponen futuras líneas de investigación basadas en los hallazgos de la tesis.
8. **Referencias:** Se incluye una lista de todas las fuentes y referencias citadas a lo largo del trabajo.

## CAPÍTULO 1. INTRODUCCIÓN

---



# Capítulo 2

## Estado del arte

### 2.1. Introducción

En la era actual, caracterizada por una proliferación y generación de contenido digital sin precedentes, la gestión de la información se ha transformado radicalmente [13]. Los organismos encargados de la aplicación de la ley se ven inundados por un volumen abrumador de datos, emergiendo la necesidad de estrategias innovadoras para su procesamiento eficiente y efectivo. La adopción de tecnologías de BD se perfila como un enfoque prometedor, posibilitando el análisis exhaustivo de fuentes de información heterogéneas para agilizar las ICs y potenciar la conciencia situacional [14].

En paralelo, las emergencias, definidas por incidentes repentinos que ponen en riesgo vidas y bienes, requieren una respuesta ágil y coordinada por parte de las múltiples entidades de protección y seguridad pública. La eficacia en la GE se apoya en la integración de una gama de habilidades y conocimientos especializados, lo que a menudo representa un desafío significativo para la colaboración efectiva entre las agencias involucradas y el acceso a grandes volúmenes de información [15]. La clave para superar estos obstáculos radica en un intercambio de información constante y fluido, que permita una coordinación y colaboración sin fisuras.

Esta tesis doctoral busca abordar estos desafíos multifacéticos a través de soluciones tecnológicas avanzadas que facilitan tanto la IC como la GE. La innovación tecnológica y la interoperabilidad se convierten en pilares fundamentales, permitiendo a las entidades pertinentes responder con mayor eficacia y eficiencia en un entorno cada vez más complejo y conectado.

### 2.2. Capacidades de las organizaciones de emergencias y seguridad

La eficiencia en la Gestión de Emergencias y la investigación de actividades delictivas depende críticamente de una coordinación impecable, integrando recursos y habilidades de una amplia gama de agencias a nivel internacional, nacional, regional y local. Estas entidades, encargadas tanto de la GE como de la aplicación de la ley, se enfrentan a una urgente necesidad de plataformas y herramientas que posibiliten respuestas rápidas y eficaces a situaciones críticas.

Dentro del ámbito de la GE, es fundamental un ciclo continuo de gestión que abarca mitigación, preparación, respuesta y recuperación. Cada una de estas etapas es esencial y requiere estrategias y acciones específicas: desde la mitigación de impactos hasta la preparación para situaciones inminentes, pasando por respuestas efectivas en momentos de crisis y, finalmente, una recuperación que restablece la normalidad y fortalece la resiliencia ante futuros incidentes. La naturaleza cíclica de este proceso se refleja en un modelo ampliamente aceptado por expertos y académicos, subrayando la importancia de la preparación proactiva y la reconstrucción post-emergencia, además de la respuesta inmediata a desastres.



**Figura 2.1:** Fases en la Gestión de Emergencias

La naturaleza cíclica de este proceso se refleja en un modelo ampliamente aceptado por expertos y académicos, subrayando la importancia de la preparación proactiva y la reconstrucción post-emergencia, además de la respuesta inmediata a desastres. [16].

Para apoyar estas fases críticas, es esencial un flujo constante y efectivo de información entre todas las agencias involucradas. Esto posibilita no solo la coordinación operativa sino también la colaboración estratégica, crucial para

## 2.2 Capacidades de las organizaciones de emergencias y seguridad

una gestión integral y efectiva de las crisis. Aquí, las tecnologías emergentes y las plataformas de datos integradas juegan un papel fundamental, proporcionando los recursos necesarios para almacenar, procesar y analizar grandes volúmenes de datos, lo que a su vez facilita el intercambio de información y la toma de decisiones basadas en datos.

En el contexto de la seguridad pública, la creciente dependencia de tecnologías digitales ha generado una producción masiva de datos, originados en fuentes diversas como cámaras *Closed Circuit TeleVision* (CCTV), redes sociales y comunicaciones móviles. Las entidades encargadas de hacer cumplir la ley requieren de herramientas avanzadas para procesar y analizar estos datos de manera eficaz, lo que es crucial para llevar a cabo ICs competentes [17]. Esto implica el desarrollo de repositorios centralizados de datos, sistemas avanzados de análisis y correlación de información, y herramientas de búsqueda y visualización multimodal.

Además, la interoperabilidad entre agencias y la colaboración efectiva son esenciales para la gestión integral de emergencias y la IC. Las soluciones tecnológicas emergentes y las plataformas de datos integradas son cruciales para proporcionar los medios para un intercambio de información eficiente y una toma de decisiones informada.

Las investigaciones del crimen organizado y delitos económicos, así como los delitos relacionados con la suplantación de identidad, requieren el manejo de volúmenes de datos extremadamente grandes y heterogéneos. Estos desafíos subrayan la necesidad de soluciones que permitan el almacenamiento y procesamiento centralizado de datos, la automatización y programación de tareas analíticas, y la generación de notificaciones en tiempo real para mejorar la respuesta a las actividades delictivas y las amenazas a la seguridad.



**Figura 2.2:** Fases en una acción conjunta

## CAPÍTULO 2. ESTADO DEL ARTE

---

En resumen y en consonancia con la Figura 2.2, la ejecución y coordinación de actuaciones en las organizaciones de emergencias y seguridad deben ser multifacéticas y estar enfocadas en la mejora continua. Esto no solo incluye la adopción de tecnologías avanzadas y prácticas operativas, sino también la formación y el desarrollo del personal, y la integración de procesos interagenciales. La combinación de estos elementos asegura una respuesta eficiente y eficaz en la protección de la vida, la propiedad y el medioambiente ante eventos adversos y desastres. Por ello se han identificado las siguientes capacidades relativas a la recolección, gestión y análisis de datos, así como el uso de ellos dentro de operativas colaborativas entre agencias.

### 2.2.1. Recolección y gestión de datos

La recolección y gestión de datos es un pilar fundamental tanto en la GE como en la IC. En este apartado, se examina el estado del arte de las prácticas y tecnologías utilizadas para recopilar, almacenar y gestionar datos críticos en estos campos.

#### Gestión de Emergencias

En el campo de la GE moderna, la eficiencia en la recopilación y manejo de datos es clave. La constante innovación en tecnologías de la información ha transformado radicalmente la capacidad de las *Emergency Management Agencies* (EMA) para obtener datos precisos y en tiempo real, redefiniendo su respuesta ante las crisis. La ubicación y el estado de los operativos en el terreno, junto con la integración de datos provenientes de *Unmanned Aerial Vehicle* (UAV)s, satélites y sensores de *Internet of Things* (IoT), son fundamentales para una toma de decisiones eficaz y una coordinación efectiva.

Asimismo, las redes sociales se han establecido como herramientas cruciales en la GE, proporcionando información actualizada y facilitando a las agencias de emergencias la recolección de datos relevantes sobre las experiencias y necesidades de las personas afectadas. El uso de herramientas analíticas avanzadas permite analizar esta información para identificar patrones, localizar personas en riesgo y mejorar la distribución de recursos.

Además, el análisis de BD ha sido un avance significativo para las EMA, permitiéndoles desarrollar modelos predictivos más precisos, optimizar la asignación de recursos y acelerar la toma de decisiones. El uso de plataformas de datos integradas, que aprovechan las tecnologías de computación en *CLOUD* y en *EDGE*, brinda a los administradores de emergencias un acceso inmediato a información crucial, vital para garantizar una respuesta rápida y eficiente [18].

## 2.2 Capacidades de las organizaciones de emergencias y seguridad

### Investigación Criminal

En la IC, la recolección y gestión de datos se ha vuelto igualmente sofisticada. Los *Law Enforcement Agencies* (LEA)s necesitan herramientas capaces de manejar y analizar datos de diversas fuentes, incluyendo registros de CCTV, bases de datos de inteligencia, interceptaciones de comunicaciones y evidencia digital recuperada en el lugar del delito.

Afrontan un desafío doble: por un lado, se debe garantizar la integridad y seguridad de los datos recopilados; y por otro, la capacidad de procesar y analizar estos datos de manera rápida y eficiente para descubrir patrones, correlaciones y evidencias clave. El uso de algoritmos de aprendizaje automático y técnicas de minería de datos ha permitido a los investigadores filtrar información relevante de los vastos repositorios de datos y obtener conocimientos que antes eran inaccesibles [19].

Otro factor crucial es la interoperabilidad entre distintos sistemas y organizaciones, lo cual es esencial para una colaboración y un intercambio de información efectivos. Los estándares abiertos y los protocolos de intercambio de datos facilitan este proceso, permitiendo que las agencias compartan información de manera segura y eficiente.

El estado del arte continúa evolucionando a medida que nuevas tecnologías y prácticas emergen. La IA, el *Deep Learning* (DL) y la computación cuántica prometen llevar la recolección y gestión de datos a niveles sin precedentes, ofreciendo oportunidades para mejorar aún más las capacidades en GE y en la IC.

#### 2.2.2. Análisis de datos

La evolución de la IC moderna ha subrayado la importancia de herramientas analíticas avanzadas capaces de lidiar con la diversidad, el volumen y la complejidad de los datos. Técnicas como el text mining, la minería de datos, el reconocimiento de patrones y el aprendizaje automático son fundamentales para descubrir patrones que permitan realizar predicciones significativas sobre nuevos datos [19]. Estos procesos deben abordar la complejidad inherente al lenguaje natural y la gestión de datos tanto estructurados como no estructurados. La habilidad de procesar y analizar datos de manera eficiente y variada es vital en la IC para responder a las dinámicas y demandas actuales.

En el ámbito de la GE, el procesamiento y análisis oportuno de grandes volúmenes de datos provenientes de múltiples fuentes es esencial para la toma de decisiones informada y la coordinación eficiente de respuestas. La fusión semántica de información apoya las decisiones y acciones al proporcionar in-

formación contextualizada, aprovechando la sinergia en los datos adquiridos de múltiples fuentes, como sensores, bases de datos y conocimiento humano [20].

Ambos campos se benefician de las tecnologías de análisis multimedia, incluyendo la extracción de metadatos, indexación de datos, fusión de datos y búsqueda y recuperación eficiente. Estas herramientas permiten el manejo efectivo de la información durante situaciones críticas y la resolución de crímenes complejos. Las ontologías ajustadas y las técnicas de razonamiento permiten el enriquecimiento de la información existente y el descubrimiento de nuevos conocimientos, proporcionando así una visión completa de los dominios de interés.

En definitiva, el análisis y gestión de datos actual requiere de una integración de tecnologías avanzadas que faciliten la interoperabilidad en la IC y la capacidad de respuesta frente a emergencias, como se puede apreciar a continuación.

### ■ **Gestión de Emergencias:**

1. Procesamiento y análisis rápido de datos para una toma de decisiones ágil.
2. Fusión semántica de información para una visión contextualizada y completa durante emergencias.
3. Ontologías y razonamiento para el enriquecimiento y descubrimiento de información relevante.

### ■ **Investigación Criminal:**

1. Análisis de datos multimedia para la identificación y seguimiento de patrones en investigaciones.
2. Técnicas avanzadas de text mining y minería de datos para el análisis predictivo y el reconocimiento de patrones.
3. Aprendizaje automático para mejorar la eficiencia y la efectividad de las investigaciones.

### **2.2.3. Colaboración y comunicación interagencial**

La colaboración y comunicación efectivas entre distintas agencias son piezas fundamentales en la gestión de crisis y la IC. La capacidad de compartir información de manera efectiva permite a las agencias cumplir con sus objetivos y facilita una respuesta coordinada y colaborativa ante emergencias complejas.

El uso de material multimedia se ha convertido en un activo fundamental en la recolección de inteligencia, prevención del crimen, manejo de crisis

## 2.2 Capacidades de las organizaciones de emergencias y seguridad

y aplicaciones forenses. Las autoridades deben poder utilizar rápidamente los datos recolectados por diferentes sistemas de CCTV o *streams* de datos para responder de manera eficiente a los eventos de seguridad. Los estándares internacionales, como la norma EN ISO 22311 [21], han sido propuestos para la exportación de archivos de videovigilancia, basándose en un consenso sobre las necesidades mínimas de los investigadores a nivel mundial.

Por otro lado, en la GE, la mayoría de las herramientas existentes se limitan a crisis específicas o a la simulación y visualización de información geográfica. La interoperabilidad, definida como la capacidad de intercambiar y utilizar información, es crucial para la gestión eficiente de recursos y la colaboración en respuestas a emergencias. Además, proporciona a los responsables de la toma de decisiones la información necesaria para definir y gestionar operaciones, documentar procedimientos, mitigar riesgos y suministrar los datos esenciales para las tareas asignadas.

Para que diferentes sistemas intercambien información y sean interoperables, es imprescindible analizar los mecanismos de comunicación, los modelos de datos existentes, los tipos de bases de datos y las herramientas que proporcionan o requieren información de la plataforma.

### Interoperabilidad y estándares

La capacidad de operar de manera interoperable entre agencias es un elemento crítico, particularmente en contextos de crisis donde la eficiencia y la precisión son indispensables. Los estándares internacionales como la norma EN ISO 22311 son vitales, ya que establecen un consenso global que facilita la coordinación y la colaboración interagencial.

El intercambio de documentos multimedia, respaldados por estándares internacionales, se han convertido en herramientas esenciales en la inteligencia y GE. Estos estándares permiten una recopilación y análisis de datos más ágil y efectivo, incrementando así la capacidad de las agencias para actuar de manera proactiva frente a incidentes de seguridad y desastres naturales.

Los siguientes estándares de interoperabilidad son clave para el intercambio eficaz de información:

- **EN ISO 22311:** Estándar internacional para los sistemas de alerta y aviso en situaciones de emergencia.
- **National Information Exchange Model (NIEM):** Modelo de Estados Unidos para el intercambio de información entre agencias gubernamentales y socios del sector privado [22].

## CAPÍTULO 2. ESTADO DEL ARTE

---

- **Emergency Data Exchange Language (EDXL)**: Conjunto de especificaciones para facilitar el intercambio de información en entornos de seguridad y emergencia [23].
- **CAP** : Protocolo desarrollado por la *Organization for the Advancement of Structured Information Standards* (OASIS) [24] para el intercambio de información sobre amenazas y emergencias [25].
- **Geography Markup Language (GML)**: Lenguaje de marcado basado en *eXtensible Markup Language* (XML) para representar información geográfica, utilizado en *Sistemas de Información Geográfica* (SIG) [26].
- **Health Level Seven International (HL7)**: Conjunto de estándares para el intercambio, integración, compartición y recuperación de información electrónica de salud [27].
- **IEEE 1512**: Estándar del Instituto de Ingenieros Eléctricos y Electrónicos para el intercambio de información en incidentes de transporte [28].
- **ISO/IEC 27001**: Estándar internacional para la gestión de la seguridad de la información, crucial para proteger la integridad y la confidencialidad de los datos intercambiados [29].
- **CEN/TS 16157**: Serie de especificaciones técnicas para *Intelligent Transport Systems* (ITS) y su interoperabilidad en Europa [30].
- **World Wide Web Consortium (W3C) Standards**: Normas del W3C para la web, incluyendo lenguajes como *HyperText Markup Language* (HTML) y XML, fundamentales para la interoperabilidad en entornos digitales [31].

Estos estándares desempeñan un papel crucial en asegurar que la información es intercambiada de manera eficiente, segura y efectiva, facilitando una respuesta coordinada en situaciones de emergencia y mejorando la colaboración entre distintas agencias.

### Mecanismos de comunicación y modelos de datos

Establecer una infraestructura de comunicación sólida y adoptar modelos de datos estandarizados es esencial para una interoperabilidad efectiva. Estos elementos son imprescindibles para asegurar un flujo de información coherente y sin obstáculos entre sistemas diferentes, lo que permite una toma de decisiones bien fundamentada y una colaboración fluida entre agencias en situaciones de crisis y en IC.



La elección de un modelo de datos adecuado es crucial para el intercambio de información. Modelos como EDXL ofrecen un enfoque generalizado, mientras que *Joint Command, Control and Communications Information Exchange Data Model* (JC3IEDM) [32] y NIEM proporcionan estructuras ricas y flexibles. *EMERGENCY ELEMENTS* (EMERGEL), aunque limitado, presenta la posibilidad de extensión para proyectos específicos. La capacidad de personalizar estos modelos es fundamental para el éxito en la gestión de información.

### 2.3. Problemáticas y desafíos

La eficiencia en la GE y la seguridad pública enfrenta múltiples desafíos que son fundamentales para la protección de la sociedad y la administración efectiva de la justicia. En el ámbito de la IC, los desafíos incluyen desde la recopilación y procesamiento de grandes volúmenes de datos hasta su análisis forense y uso en la resolución de casos complejos. Las LEAs buscan continuamente mejorar sus metodologías y herramientas para mantenerse al día con las tecnologías emergentes y las tácticas en constante evolución de los delincuentes.

Por otro lado, en la GE, los retos se amplifican al coordinar esfuerzos entre múltiples agencias, optimizar la comunicación en situaciones críticas y tomar decisiones informadas basadas en datos que pueden ser incompletos o aun en desarrollo. La capacidad para responder a desastres naturales o incidentes provocados por humanos, así como la recuperación posterior, depende en gran medida de la interoperabilidad de los sistemas y de la efectividad con la que las agencias pueden compartir y analizar la información.

Esta sección profundiza primero en los obstáculos y problemáticas específicas que enfrentan tanto las LEAs como las agencias de GE en el desempeño de sus funciones críticas a lo largo de diferentes escenarios y después se examinan los desafíos para la gestión, integración y análisis de datos, las dificultades inherentes a la colaboración interagencial, y los retos presentados por recursos limitados y expectativas en constante cambio. Comprender estas problemáticas es esencial para desarrollar soluciones efectivas y para mejorar la preparación y respuesta ante situaciones de crisis.

#### 2.3.1. Problemáticas en la Investigación Criminal

En la lucha contra el crimen, particularmente en la prevención e investigación de ataques terroristas y disturbios, Europa ha sido escenario de numerosos ataques en los últimos años. Los ataques de 2017 en diversas ciudades europeas, incluido el ataque suicida en Manchester [33], los sucesos en el puente de

## CAPÍTULO 2. ESTADO DEL ARTE

---

Westminster [34] y el atentado en Las Ramblas de Barcelona [35], subrayan la gravedad y la amenaza persistente del terrorismo.

La declaración del problema se centra en la necesidad de procesar grandes volúmenes de datos de diferentes modalidades. Las CCTV, las redes sociales y las comunicaciones móviles han desempeñado un papel clave en la investigación de estos crímenes, pero la abrumadora cantidad de datos multimedia y textuales hace que la tarea sea aún más desafiante. [36]

El volumen de datos y el gran número de oficiales de policía involucrados en la clarificación y prevención de ataques adicionales indican la necesidad crítica de plataformas y herramientas que permitan a las agencias de aplicación de la ley actuar y responder rápidamente para llevar a los perpetradores ante la justicia y prevenir nuevos ataques.

En el caso del crimen económico organizado y la detección de la corrupción, las agencias especializadas se enfrentan a la tarea de procesar casos extensos que a menudo involucran redes a nivel regional o internacional. La gran cantidad de datos a procesar complica el análisis coherente y la coordinación manual necesaria debido a soluciones de software descentralizadas, lo que degrada significativamente la eficiencia en el procesamiento de casos [37].

Por último, el crimen de identidad, que ha aumentado exponencialmente, presenta desafíos adicionales debido al uso de datos personales para facilitar crímenes graves y eludir la detección por parte de las fuerzas del orden. Los avances tecnológicos, aunque facilitan la vida, también han creado nuevas formas para que se cometa fraude, lo que representa un problema considerable para las agencias de aplicación de la ley.

Este análisis de casos de uso diferentes identifica las problemáticas y desafíos clave que enfrentan las agencias de aplicación de la ley en la era moderna, destacando la necesidad de enfoques innovadores y colaborativos para mejorar las estrategias de investigación y prevención.

### 2.3.2. Problemáticas en la Gestión de Emergencias

Las operaciones de GE enfrentan desafíos significativos que abarcan desde la coordinación de múltiples organizaciones de primeros auxilios hasta la rápida toma de decisiones en situaciones de crisis. Los escenarios pueden incluir desastres naturales en entornos urbanos, accidentes industriales con liberación de sustancias peligrosas, y ataques terroristas en lugares públicos concurridos.

En los entornos urbanos, un desastre natural como un terremoto puede causar daños generalizados a infraestructuras críticas, colapso de edificaciones y un número elevado de víctimas. La coordinación efectiva de los servicios de emergencia y médicos es vital para la evaluación de daños, rescate y recuperación.

Los accidentes industriales representan otro conjunto de desafíos. La posibilidad de exposición a sustancias tóxicas requiere una identificación rápida y precisa de las fuentes de peligro y la gestión de la información sobre la dispersión de tóxicos para evitar la exposición y realizar evacuaciones si fuera necesario.

Además, los ataques terroristas presentan una problemática única en cuanto a la GE. El uso potencial de agentes químicos o biológicos y la presencia de UAVs requiere de una respuesta rápida y una comunicación efectiva entre todas las agencias involucradas para minimizar el daño y proteger a la población civil.

En todos estos escenarios, la eficiencia en la GE depende de la capacidad para intercambiar información de manera efectiva y realizar acciones coordinadas, que deben ser soportadas por sistemas y protocolos de comunicación adecuados, así como por la integración de tecnologías innovadoras que permitan una respuesta rápida y eficaz ante situaciones adversas.

### 2.3.3. Silos de datos y falta de integración

Un reto notable tanto en la IC como en la GE es la integración eficaz de datos de múltiples fuentes. La existencia de silos de datos, donde la información se encuentra confinada en sistemas aislados sin interconexión, representa un obstáculo importante. Esta separación impide que investigadores y equipos de emergencia accedan a una perspectiva completa y actualizada de los acontecimientos que están manejando.

En el ámbito de la IC, la falta de integración puede dar como resultado una recolección ineficaz de pruebas, retrasos en la identificación de patrones delictivos y una colaboración deficiente entre distintas agencias. La heterogeneidad de los datos, que incluye formatos variados como vídeo, audio y texto, exige herramientas de análisis avanzadas capaces de procesar y correlacionar información de manera eficiente y precisa.

Por otro lado, en la GE, la incapacidad de integrar datos en tiempo real de fuentes como sensores IoT, imágenes satelitales y bases de datos de recursos críticos, puede obstaculizar las operaciones de respuesta y recuperación. La necesidad de tener información actualizada sobre la ubicación y el estado de los equipos de respuesta de emergencias y los recursos en el terreno es vital para una gestión efectiva [38].

Este desafío se intensifica debido a la diversidad de protocolos y estándares existentes, lo que requiere una estrategia de integración que facilite la interoperabilidad entre sistemas dispares. Avanzar hacia la adopción de estándares abiertos y desarrollar interfaces de programación de aplicaciones (APIs) que faciliten un intercambio de datos seguro y uniforme, son medidas esenciales para sortear estos desafíos.

Además, la implementación de plataformas de integración de datos que utilicen tecnologías como el *Natural Language Processing* (NLP) y el aprendizaje automático, puede ofrecer la capacidad de transformar grandes volúmenes de datos no estructurados en información accionable, proporcionando así una ventaja significativa en ambos campos. La meta es lograr un sistema que no solo almacene datos, sino que también los interprete y los haga accesibles y útiles para todos los actores involucrados.

### 2.3.4. Volumen y complejidad de los datos

Debido al creciente volumen y la complejidad de los datos, en la actualidad se presentan desafíos significativos tanto en la IC como en la GE. Estos desafíos abarcan desde la recopilación y el almacenamiento hasta el análisis y la interpretación efectiva de grandes conjuntos de datos.

En el ámbito de la IC, los profesionales se enfrentan a un flujo constante y abrumador de datos provenientes de una variedad de fuentes [39].

- Datos de comunicación: Registros detallados de llamadas y mensajes de texto, incluyendo los primeros registros digitales de operadores telefónicos.
- Datos de redes sociales: Información inicial de plataformas como Facebook y Twitter, antes de la implementación de políticas de privacidad avanzadas.
- Datos de vigilancia: Transición de imágenes y videos analógicos de CCTV a formatos digitales.
- Datos forenses digitales: Uso de software de análisis forense inicial como EnCase o FTK para extraer datos de dispositivos digitales.
- Registros financieros: Primeros registros digitales de transacciones bancarias y tarjetas de crédito.

Del mismo modo, dentro del ámbito de la GE, el volumen y la complejidad de los datos se manifiestan en la necesidad de procesar información en tiempo real para tomar decisiones rápidas y efectivas.

- Datos de sensores: Información de sensores meteorológicos digitales y calidad del aire.
- Datos geográficos: Implementación inicial de sistemas GIS para mapeo y planificación de respuestas.

## 2.3 Problemáticas y desafíos

---

- Comunicaciones de emergencia: Registros digitales de llamadas y comunicaciones por radio mejoradas.
- Datos de redes sociales: Uso de Twitter y Facebook para seguimiento de eventos en tiempo real.
- Imágenes y videos: Uso de UAVs y cámaras digitales para evaluación de daños y reconocimiento del terreno.

Hasta ahora y teniendo en cuenta la transición hacia la era digital, se han utilizado tecnologías y herramientas que de forma semiautomática podían hacer frente a un volumen limitado de datos, algunas de estas soluciones son las siguientes:

- Bases de Datos Relacionales Avanzadas: Como MySQL [40] y Oracle [41], para el manejo de grandes volúmenes de datos estructurados.
- Herramientas de Análisis Forense Digital: Software como EnCase [42] y FTK [43], utilizados en etapas iniciales de la digitalización forense.
- Sistemas de Gestión de Información Geográfica (GIS): Implementaciones tempranas de software GIS como ArcGIS [44].
- Sistemas de Archivo Digital y Catalogación: Uso de sistemas de archivo digitales para almacenar registros y documentos.
- Herramientas de Visualización y Análisis de Datos: Software como Tableau [45] y herramientas de análisis de redes sociales para la interpretación de grandes conjuntos de datos.

Aunque las tecnologías mencionadas anteriormente fueron fundamentales en la transición hacia la era digital, en el contexto actual, su capacidad se ha quedado limitada frente a las crecientes demandas. El manejo efectivo de los enormes volúmenes de datos generados en la actualidad, especialmente en flujos de datos en tiempo real, requiere de soluciones más avanzadas y sofisticadas. Las aplicaciones modernas deben ser capaces de procesar y analizar datos a una velocidad y escala sin precedentes, integrando tecnologías emergentes como el aprendizaje automático, la IA y plataformas de BD. Estas soluciones punteras no solo ofrecen un almacenamiento y procesamiento de datos más eficiente, sino que también proporcionan capacidades analíticas avanzadas, lo que es crucial para responder a situaciones de emergencia y para la IC en el dinámico entorno actual.

### 2.3.5. Limitaciones tecnológicas y de recursos

La rápida evolución de la tecnología y la creciente dependencia de sistemas digitales en la IC y la GE plantean desafíos únicos. A pesar de los avances tecnológicos, muchas organizaciones se enfrentan a limitaciones en términos de infraestructura tecnológica obsoleta, recursos insuficientes y falta de personal capacitado. Estas limitaciones no solo impiden una respuesta eficaz, sino que también pueden comprometer la calidad y la eficiencia del trabajo realizado en estas áreas críticas.

#### Investigación Criminal

La IC moderna se enfrenta a varios desafíos tecnológicos y de recursos [46], que incluyen:

- **Capacidad de procesamiento:** Las unidades forenses digitales a menudo trabajan con hardware limitado, lo que retrasa el análisis de grandes volúmenes de datos de dispositivos electrónicos incautados.
- **Gestión de llamadas y datos financieros:** La integración y análisis de registros de llamadas y transacciones financieras requieren sistemas avanzados y capacitación especializada, algo que no todas las agencias tienen.
- **Escasez de personal experto:** La falta de expertos en ciberseguridad y análisis de datos es un cuello de botella significativo, limitando la capacidad de respuesta a delitos cibernéticos complejos.

#### Gestión de Emergencias

En la GE, las limitaciones [47] incluyen:

- **Comunicaciones en crisis:** Durante eventos de gran escala, los sistemas de comunicación pueden ser insuficientes, como se vio en [referencia a un caso específico de un documento proporcionado].
- **Uso de UAVs y tecnología avanzada:** Aunque los UAVs son herramientas valiosas para la evaluación de desastres, su implementación efectiva es a menudo limitada por restricciones de presupuesto y capacitación del personal involucrado en la operativa.
- **Infraestructura de respuesta:** La falta de infraestructura adecuada para la GE, como centros de comando móviles y sistemas de alerta temprana, es un problema recurrente.

### 2.4. Big data en la operativa interagencial

El uso del BD, el *Machine Learning* (ML) y la IA está transformando significativamente las operativas interagenciales en diversos sectores. Estas tecnologías avanzadas ofrecen soluciones innovadoras a problemas complejos y mejoran la colaboración y la eficiencia en las operaciones [39].

Más en detalle, el impacto y las aplicaciones generales que pueden ofrecer estas tecnologías se pueden identificar claramente como sigue:

- **Análisis y procesamiento de datos a gran escala:** El BD permite la gestión y análisis de grandes volúmenes de información, facilitando la identificación de tendencias, patrones y correlaciones que serían imposibles de descubrir manualmente.
- **Optimización del ML:** El ML utiliza estos grandes conjuntos de datos para entrenar modelos que pueden predecir comportamientos, optimizar procesos y automatizar decisiones basadas en datos.
- **Soluciones basadas en IA:** La IA proporciona herramientas avanzadas para la toma de decisiones, simulación de escenarios y mejora de la eficiencia operativa en diversas aplicaciones.

Además, los beneficios que puede proporcionar soluciones como el BD, como el ML y la IA son los siguientes:

- **Mejora de la comunicación:** Las tecnologías de IA pueden facilitar la comunicación entre diferentes agencias, traduciendo y sintetizando información de múltiples fuentes para una comprensión común.
- **Coordinación de respuestas:** El análisis de datos en tiempo real permite una coordinación más efectiva y una respuesta rápida a situaciones complejas, lo cual es crucial en entornos interagenciales.
- **Predicción y planificación estratégica:** Algoritmos de ML pueden predecir eventos y situaciones futuras, lo que ayuda en la planificación estratégica y la asignación de recursos.

Por lo tanto, el BD, ML y la IA ofrecen soluciones integrales a desafíos comunes en operaciones entre agencia, como la gestión de grandes volúmenes de datos, la integración de sistemas dispares y la optimización de procesos. Estas tecnologías no solo potencian la capacidad analítica, sino que también promueven una colaboración más estrecha y efectiva entre diferentes entidades y sectores [48].

### 2.4.1. Big Data y Seguridad Pública: definición y características clave

El concepto de BD ha cobrado una relevancia significativa en el ámbito de la seguridad pública. Se refiere a la acumulación, procesamiento y análisis de grandes conjuntos de datos para mejorar la eficiencia y efectividad de las operaciones de seguridad y análisis forense [49].

#### Definición de Big Data en Seguridad Pública

El BD en la actualidad se extiende más allá de las tres Vs tradicionales (Volumen, Variedad y Velocidad)



**Figura 2.3:** Las 3 Vs del Big Data

Actualmente, se incluyen otras dimensiones críticas que impactan en la forma en que los datos son utilizados y valorados.

- **Volumen:** El término implica el manejo de cantidades masivas de datos generados por diversas fuentes, incluyendo registros digitales, sistemas de vigilancia, y plataformas de comunicación.
- **Velocidad:** La rapidez con la que se generan, recopilan y procesan los datos es un factor crítico para la toma de decisiones en tiempo real en el ámbito de la seguridad.
- **Variedad:** Los datos abarcan un amplio rango, desde registros textuales hasta imágenes y videos, pasando por datos geoespaciales y de sensores.
- **Veracidad:** La fiabilidad y precisión de los datos. En seguridad pública, la veracidad es crucial para asegurar que las decisiones se basen en información precisa y confiable.



- **Valor:** La capacidad de extraer información útil y aplicable. En el contexto de la seguridad, el valor se refiere a convertir los datos en insights que mejoren la eficiencia operativa y la toma de decisiones.
- **Variabilidad:** Los datos pueden cambiar en significado en diferentes contextos. Comprender estas variaciones es esencial para la interpretación correcta y para el análisis predictivo en la seguridad pública.
- **Visualización:** Presentar los datos de manera comprensible y útil. Las herramientas de visualización avanzadas son fundamentales para analizar y comunicar tendencias y patrones en el ámbito de la seguridad.
- **Vulnerabilidad:** Consideración de la seguridad y privacidad de los datos. En el ámbito de la seguridad pública, proteger la información sensible y personal es un aspecto clave para mantener la confianza y la integridad del sistema.

### Características clave del Big Data en Seguridad Pública

El uso del BD en el ámbito de la seguridad pública ha revolucionado la forma en que las agencias y departamentos gestionan y responden a los desafíos de seguridad. La integración de grandes volúmenes de datos provenientes de diversas fuentes ha abierto nuevas posibilidades para el análisis avanzado y la toma de decisiones estratégicas. A continuación, exploramos algunas características clave del BD que están jugando un papel transformador en el sector de la seguridad pública:

- **Análisis predictivo:** La aplicación de técnicas de ML y análisis estadístico permite predecir tendencias y patrones en la actividad delictiva.
- **Mejora de la toma de decisiones:** El análisis exhaustivo de datos a gran escala posibilita una toma de decisiones más informada y basada en datos concretos.
- **Interoperabilidad de datos:** La capacidad de integrar y analizar datos de múltiples fuentes es esencial para una operativa de seguridad eficiente y coordinada.

**Impacto en la operativa de seguridad:** El BD permite a las agencias de seguridad adoptar un enfoque más informado y basado en datos, lo que conduce a una prevención y detección más efectiva del crimen. La integración de BD en las estrategias de seguridad pública representa un cambio significativo en la forma en que se abordan los desafíos de seguridad.

### 2.4.2. Revolucionando la investigación forense: El potencial del Big Data

El BD está transformando radicalmente el campo de la investigación forense, proporcionando nuevas herramientas y métodos para el análisis y la resolución de crímenes complejos.

#### Avances actuales en la investigación forense gracias al Big Data

La era del BD ha marcado un punto de inflexión en la investigación forense, ofreciendo capacidades sin precedentes para el procesamiento y análisis de datos. Esta sección explora los avances significativos actuales que están cambiando la forma en que se abordan las ICs.

- **Análisis de datos masivos:** La capacidad de procesar y analizar grandes volúmenes de datos permite a los investigadores forenses examinar y correlacionar información de múltiples fuentes, como registros telefónicos, cámaras de seguridad, y redes sociales. [50]
- **Reconocimiento de patrones:** El uso de algoritmos avanzados para identificar patrones en datos complejos puede llevar a la detección de actividades delictivas y comportamientos sospechosos. [51]
- **Análisis predictivo:** Herramientas de BD permiten predecir tendencias delictivas y posibles amenazas futuras, lo que es esencial para la prevención del crimen. [52]

#### Direcciones futuras y aplicaciones potenciales

Mirando hacia el futuro, el campo de la investigación forense se encuentra al borde de una transformación aún más profunda impulsada por el BD. Esta sección destaca algunas de las aplicaciones futuras más prometedoras y las direcciones de investigación que podrían remodelar aún más el panorama de la IC.

- **IA en análisis forense:** El desarrollo de sistemas de IA que pueden aprender de grandes conjuntos de datos forenses podría revolucionar la forma en que se investigan los crímenes, haciendo el proceso más rápido y preciso. [53]
- **Blockchain para evidencia digital:** La tecnología *Blockchain* podría usarse para asegurar la cadena de custodia de evidencia digital, asegurando su integridad y evitando manipulaciones. [54]

- **Virtual Reality (VR) y reconstrucción de escenas del crimen:** La integración de BD con tecnologías de realidad virtual podría permitir reconstrucciones más detalladas y precisas de escenas del crimen. [55]

En definitiva, el BD está cambiando fundamentalmente la investigación forense, proporcionando métodos más eficaces y precisos para resolver crímenes. Con la continua innovación tecnológica, las futuras aplicaciones prometen una transformación aún mayor en este campo vital.

### 2.4.3. Innovando en la respuesta y Gestión de Emergencias: El Big Data marcando diferencias

El BD está siendo un factor transformador en la manera en que se abordan la respuesta y la GE. Con la creciente complejidad de las crisis modernas, la habilidad para analizar de manera ágil y eficiente grandes cantidades de datos se ha revelado como un componente vital para garantizar una gestión eficiente y proactiva de emergencias.

#### Uso del Big Data en situaciones de emergencia

La integración del BD en la GE está marcando una diferencia significativa en cómo las organizaciones responden a los desafíos y planifican para el futuro.

- **Mejora en la toma de decisiones:** El análisis de datos en tiempo real proporciona información crucial que ayuda a los tomadores de decisiones a reaccionar con rapidez y eficacia ante situaciones de emergencia. [56]
- **Predicción y prevención de crisis:** La utilización de modelos predictivos permite identificar patrones y tendencias que pueden indicar la probabilidad de futuras emergencias, lo que es vital para la planificación y prevención. [57]
- **Coordinación de recursos y respuesta:** El BD facilita la optimización de recursos y personal, permitiendo una distribución y respuesta más eficientes y efectivas. [58]

#### Desafíos y soluciones futuras

A pesar de los avances, aún existen desafíos que deben abordarse para aprovechar plenamente el potencial del BD en la GE.

- **Integración de datos multifuente:** La capacidad para integrar y analizar datos de diversas fuentes es fundamental para una respuesta integral a las emergencias. [59]

- **Privacidad y seguridad de datos:** La gestión segura y ética de datos personales y sensibles es crítica, especialmente en situaciones de crisis. [60]
- **Capacitación y desarrollo de habilidades:** La formación continua del personal en tecnologías de BD es esencial para mejorar la eficiencia y efectividad de las respuestas a emergencias. [61]

Del mismo modo que en la IC, el BD está redefiniendo la respuesta y GE, ofreciendo oportunidades sin precedentes para mejorar la eficacia y la eficiencia. Sin embargo, para aprovechar plenamente estas oportunidades, se deben abordar los desafíos relacionados con la integración de datos, la privacidad y la seguridad, así como el desarrollo de habilidades.

### 2.5. Interoperabilidad entre agencias

En el ámbito de los *Sistemas de Información* (SI) para la gestión de crisis y la IC, existe una diversidad de herramientas que brindan soporte en ambas áreas. Muchas de estas herramientas están diseñadas específicamente para ciertos tipos de crisis o se limitan a la simulación y visualización de información geográfica [62].

En entornos heterogéneos y complejos, como los que se encuentran en la GE y la IC, la interoperabilidad es esencial para manejar los recursos involucrados y permitir una respuesta coordinada y colaborativa. [4] [63]

Además, la interoperabilidad brinda a los responsables de tomar decisiones la información necesaria para definir y administrar continuamente las operaciones, documentar procedimientos, mitigar riesgos y proporcionar los datos necesarios a todos los involucrados para realizar las tareas asignadas [64]. El resultado es una mejora en la efectividad y calidad de las tareas en las diferentes fases de una crisis o investigación.

Para lograr que distintos sistemas intercambien información y, por lo tanto, sean interoperables, es fundamental estudiar los siguientes aspectos: los distintos mecanismos de comunicación, los modelos de datos disponibles, los tipos de bases de datos y las herramientas que proporcionan o requieren información. Estos componentes son fundamentales en el desarrollo de una arquitectura efectiva tanto para la GE como para la IC.

### 2.5.1. La Interoperabilidad como pilar en la resolución de operativas conjuntas

Esta habilidad de compartir información y recursos de manera efectiva es fundamental para el éxito de operaciones conjuntas en estas áreas.

#### **Rol en la Investigación Criminal y la Seguridad Pública**

En el ámbito de la seguridad pública y la IC, la interoperabilidad es clave para el intercambio de información y recursos entre agencias de policía, servicios de inteligencia y otras entidades gubernamentales. Es vital para combatir eficazmente el crimen organizado, el terrorismo y otras formas de delincuencia compleja. La capacidad de integrar datos de manera efectiva permite una recolección y análisis de información más eficientes, conduciendo a una respuesta más rápida y efectiva ante amenazas a la seguridad pública.

#### **Importancia en la Gestión de Emergencias**

En la GE, la interoperabilidad facilita una respuesta coordinada y eficiente ante situaciones críticas como desastres naturales o ataques terroristas. La integración de comunicaciones, tecnología y estrategias entre diferentes agencias, incluyendo bomberos, servicios médicos y fuerzas de seguridad, resulta esencial para manejar estas situaciones de manera efectiva. El intercambio de datos en tiempo real y la coordinación en el terreno son fundamentales para salvar vidas y mitigar el impacto de las emergencias.

#### **Desafíos y soluciones**

Los principales desafíos para lograr una interoperabilidad efectiva incluyen la compatibilidad tecnológica, diferencias en protocolos y procedimientos operativos, así como barreras legales y de privacidad. Para superar estos retos, es necesario establecer marcos de trabajo y estándares comunes, y desarrollar sistemas tecnológicos que faciliten la compatibilidad de datos. La colaboración y comunicación entre las diversas agencias y entidades son también vitales.

#### **Hacia un futuro interconectado**

El futuro de la interoperabilidad no solo representa una necesidad operativa, sino una oportunidad para innovar en ambos campos. El desarrollo de tecnologías como BD, IA y comunicaciones móviles abre nuevas posibilidades para una colaboración más efectiva, mejorando la capacidad de respuesta en situaciones críticas y la prevención de futuras emergencias o delitos.

En definitiva, la interoperabilidad es un componente esencial tanto en la IC como en la GE, proporcionando una base sólida para una cooperación efectiva y una respuesta coordinada ante los desafíos actuales y futuros.

### 2.5.2. Comunicación y colaboración entre agencias

Los mecanismos de comunicación son fundamentales para la interoperabilidad en la IC y la GE, permitiendo establecer conexiones efectivas entre distintas herramientas y sistemas.

#### Investigación Criminal

En el ámbito de la IC, la comunicación eficiente entre las agencias de ley, entidades forenses y otros organismos es vital. Los *Web Services* (WS) [65] son fundamentales para esto, usando estándares abiertos como XML [66], *Simple Object Access Protocol* (SOAP) [67], *Web Services Description Language* (WSDL) [68], *Universal Description, Discovery, and Integration* (UDDI) [69] y *JavaScript Object Notation* (JSON) [70]. JSON, en particular, se ha popularizado por su facilidad de uso y su capacidad para trabajar eficientemente con datos complejos.

#### Gestión de Emergencias

En la GE, la rapidez y precisión en la comunicación son esenciales. Los WS facilitan que diferentes organizaciones intercambien información vital de manera segura y eficiente, lo cual es crucial durante situaciones críticas como desastres naturales o ataques terroristas.

#### Patrones de intercambio de mensajes

Los *Message Exchange Pattern* (MEP) son patrones que definen cómo se comunican las aplicaciones [71]. Los más comunes incluyen:

- **Petición-respuesta:** Ampliamente utilizado en WS. Ejemplo: Un detective solicita información de un caso a una base de datos central y espera la respuesta con los datos relevantes.
- **Unidireccional:** El cliente envía un mensaje sin esperar respuesta. Ejemplo: Un sistema de alerta temprana envía notificaciones de evacuación durante un desastre natural.
- **Petición de respuesta:** El servidor inicia y el cliente responde. Ejemplo: Un sistema de comando de emergencias envía una solicitud de estado a diferentes unidades y estas responden con su situación actual.

## 2.5 Interoperabilidad entre agencias

- **Notificación o publicación-suscripción:** El servidor envía un mensaje sin esperar respuesta. Ejemplo: Un sistema de vigilancia que notifica automáticamente a varias agencias cuando detecta una actividad sospechosa.

Todos ellos se encuentran englobados dentro de las arquitecturas API más utilizadas en el desarrollo de servicios y soluciones interoperables para el intercambio de mensajes. La Figura 2.4 trata de recoger y mostrar de una forma visual los patrones de intercambio de mensajes más utilizados en la actualidad.

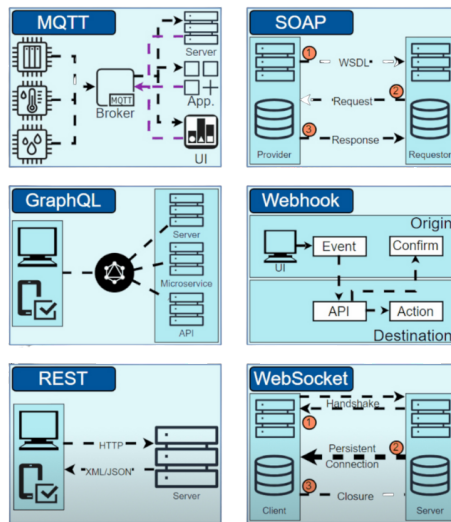


Figura 2.4: Arquitecturas de intercambio de mensajes más utilizadas

### Sincronización de comunicaciones

La sincronización de las comunicaciones es un elemento vital en el contexto de la IC y en la GE. En estos ámbitos, la capacidad de transmitir y recibir información de manera oportuna y precisa es esencial para el éxito de las operaciones. La sincronización en la comunicación no solo afecta la eficiencia de la transmisión de información, sino que también influye en la toma de decisiones, coordinación de equipos y la respuesta general a situaciones críticas.

En el contexto de la IC, la sincronización en las comunicaciones permite a las agencias de ley compartir información sensible y coordinar esfuerzos de manera efectiva, lo que es crucial para la resolución rápida y eficaz de los casos [72]. Por ejemplo, en la investigación de delitos digitales o ciberdelincuencia, donde

## CAPÍTULO 2. ESTADO DEL ARTE

---

la evidencia puede cambiar rápidamente, la comunicación síncrona asegura que los investigadores reciban datos actualizados en tiempo real.

Por otro lado, en la GE, la sincronización en la comunicación garantiza que las distintas agencias y equipos de respuesta puedan actuar de forma coordinada ante desastres naturales, ataques terroristas o emergencias médicas [73]. La capacidad de recibir y enviar información de forma síncrona asegura una respuesta rápida y eficiente, salvando potencialmente vidas y minimizando el daño.

Las comunicaciones pueden clasificarse en dos tipos principales en cuanto a su sincronización:

- **Comunicaciones síncronas:** En este tipo de comunicación, el remitente espera una respuesta inmediata del receptor antes de continuar con el proceso. Esta forma de comunicación es esencial cuando las decisiones deben tomarse rápidamente y dependen de la información recibida. Un ejemplo podría ser un centro de comando y control que coordina una respuesta a un incidente terrorista en tiempo real, donde cada decisión depende de la información más actualizada y precisa.
- **Comunicaciones asíncronas:** En las comunicaciones asíncronas, el remitente no espera una respuesta inmediata. Este método es útil en situaciones donde la información puede ser procesada y respondida a lo largo del tiempo sin afectar las operaciones en curso. Un ejemplo sería la gestión de información recopilada por sensores distribuidos en un área de desastre, donde los datos se recogen y se analizan periódicamente sin necesidad de una respuesta instantánea.

La elección entre comunicación síncrona y asíncrona depende de la naturaleza de la tarea, la urgencia de la situación y los requerimientos específicos de la operación. Ambas formas son complementarias y esenciales en la gestión eficaz tanto de ICs como de emergencias.

Esta comprensión de la sincronización de las comunicaciones es fundamental para diseñar sistemas de comunicación efectivos que puedan adaptarse a las diversas necesidades y desafíos de estos campos críticos.

### Diversidad de sistemas y herramientas

La diversidad de sistemas y herramientas utilizados en la IC y la GE es extensa y variada. Esta gama incluye desde bases de datos forenses y sistemas de vigilancia hasta herramientas de respuesta a emergencias y plataformas de comunicación avanzadas. Esta heterogeneidad presenta desafíos significativos en términos de interoperabilidad y sincronización de la comunicación.



---

## 2.5 Interoperabilidad entre agencias

La eficacia operativa en la IC y la GE depende crucialmente de la capacidad de adaptación de las plataformas a diferentes patrones de comunicación. Por ejemplo:

- **Ejemplo: Lucha contra el tráfico de drogas:** En una operación contra el tráfico de drogas, es esencial que los sistemas de inteligencia y análisis de datos puedan intercambiar información con rapidez y precisión con las bases de datos nacionales e internacionales de criminales.
- **Ejemplo: Lucha contra el fraude financiero:** Durante una investigación de fraude financiero, la integración de sistemas de análisis de transacciones con bases de datos de entidades bancarias y registros públicos es fundamental para rastrear el flujo de fondos ilícitos.

En la GE, la diversidad se refleja en la gama de herramientas y sistemas empleados para la respuesta y recuperación de desastres.

- **Ejemplo: Incendio forestal:** Durante un incendio forestal, la capacidad de integrar sistemas de teledetección y UAVs equipados con cámaras térmicas con plataformas de coordinación de bomberos y servicios de emergencia es crucial para una respuesta efectiva y segura.
- **Ejemplo: Inundaciones:** En situaciones de inundaciones, la integración de sistemas de modelado hidrológico y pronóstico meteorológico con aplicaciones móviles de alerta temprana puede ser vital para advertir a las comunidades en riesgo.

La interoperabilidad efectiva entre estos variados sistemas y herramientas es esencial para una respuesta coordinada en situaciones críticas. Esto implica la capacidad técnica para integrar sistemas dispares y la adopción de estándares y protocolos comunes que faciliten una comunicación fluida y segura.

- **Estándares y protocolos:** La adopción de estándares como XML, JSON, y tecnologías como *REpresentational State Transfer* (REST) [74] y SOAP, facilita la integración de sistemas heterogéneos y garantiza una comunicación eficiente y segura entre ellos.
- **APIs compatibles:** El uso APIs bien documentadas y compatibles entre sistemas facilita el acceso y el intercambio de datos.
- **Seguridad de datos:** Implementar protocolos de seguridad de datos robustos es crucial para proteger la información sensible durante la transmisión y el almacenamiento.

- **Plataformas de integración de datos:** Utilizar plataformas de integración de datos que pueden manejar formatos de datos dispares y realizar transformaciones de datos según sea necesario.
- **Interfaz de usuario unificada:** Desarrollar interfaces de usuario que puedan acceder y controlar múltiples sistemas de forma cohesiva, mejorando la usabilidad y eficiencia.

Finalmente, la diversidad de sistemas y herramientas en la IC y la GE requiere plataformas capaces de adaptarse a diferentes patrones de comunicación y necesidades de sincronización. Esta flexibilidad es crucial para asegurar una interoperabilidad efectiva y una respuesta coordinada en situaciones de alta presión y riesgo.

### 2.5.3. Modelos de datos para la interoperabilidad

En el ámbito de la IC y la GE, se han evaluado diversos modelos de datos que permiten un eficaz intercambio de información. Estos modelos son fundamentales para la integración y análisis de datos provenientes de fuentes diversas.

#### Investigación Criminal

La IC en la era digital enfrenta desafíos únicos y complejos, impulsando la necesidad de modelos de datos avanzados y especializados. Estos modelos deben ser capaces de manejar grandes volúmenes de datos sensibles y variados, provenientes de múltiples fuentes como bases de datos de antecedentes criminales, registros de huellas digitales, y análisis de *Ácido Desoxirribonucleico* (ADN)s [75]. La efectividad de la IC depende en gran medida de la capacidad para integrar, procesar y analizar esta información de manera eficiente y segura, respetando al mismo tiempo las normativas de privacidad y protección de datos. La adopción de modelos de datos adecuados permite a las agencias de justicia y seguridad abordar estos desafíos, mejorando la precisión y rapidez de las investigaciones y fortaleciendo la colaboración interagencial.

- **EDXL:** Desarrollado por el consorcio OASIS, basado en XML, EDXL ha sido ampliamente adoptado para el intercambio de información en situaciones de emergencia. Aunque inicialmente se centraba en la GE, sus especificaciones pueden adaptarse para la IC, particularmente en la coordinación de respuestas a incidentes a gran escala.
- **NIEM:** Un modelo de datos basado en estándares que incluye un dominio de GE. Aunque se centró inicialmente en emergencias, su estructura

flexible permite la adaptación para la IC, facilitando la integración de datos entre agencias de justicia y seguridad.

- **Modelos de datos específicos para la IC:** Además de los modelos generales, existen modelos desarrollados específicamente para la IC, como bases de datos de huellas digitales, ADN, y registros de delincuentes. Estos modelos están diseñados para manejar datos sensibles y específicos de la criminalística.

### Gestión de Emergencias

En el contexto de la GE, la diversidad y complejidad de los datos requieren modelos de datos robustos y flexibles. Estos modelos deben facilitar la rápida recolección, integración y análisis de información proveniente de diversas fuentes, como datos geográficos, comunicaciones de emergencia y reportes de incidentes [76]. La capacidad para compartir información de manera efectiva entre diferentes agencias y organizaciones es vital para una respuesta coordinada y eficaz en situaciones de crisis. Los modelos de datos en la GE deben adaptarse a la naturaleza dinámica y a menudo impredecible de las emergencias, asegurando que las agencias cuenten con la información necesaria para tomar decisiones informadas y actuar rápidamente para proteger a las comunidades y gestionar los recursos de manera óptima.

- **EMERGEL:** Desarrollado en el proyecto *Data Interoperability Solution At Stakeholders* (DISASTER) [77] de la UE, EMERGEL proporciona un modelo de alto nivel abstracto y modelos especializados para la GE, facilitando la representación de eventos, recursos y otros aspectos cruciales en situaciones de crisis.
- ***Driving Innovation in Crisis Management for European Resilience* (DRIVER):** Basado en el proyecto *Aftermath Crisis Management System-of-systems Demonstration* (ACRIMAS) [78], DRIVER propone un banco de pruebas para el desarrollo de soluciones de gestión de crisis. Este modelo se centra en promover el intercambio de información y la colaboración en la gestión de crisis. [79]
- ***European Pool against Organised Crime* (EPOC):** Aunque su enfoque principal es combatir la delincuencia organizada y transfronteriza, EPOC utiliza NIEM como modelo de datos, demostrando su adaptabilidad en diferentes contextos de seguridad.

### Consideraciones adicionales

Estos modelos de datos demuestran la importancia de tener sistemas interoperables y flexibles que puedan adaptarse a las necesidades cambiantes tanto en la IC como en la GE. La capacidad para intercambiar información de manera efectiva y segura es crucial en ambos campos para una respuesta rápida y efectiva.

- **Interoperabilidad:** La capacidad de estos modelos para integrarse con otros sistemas y compartir datos de manera segura y eficiente es clave para operaciones exitosas en ambos campos.
- **Flexibilidad y adaptabilidad:** La naturaleza cambiante de las amenazas y emergencias requiere modelos de datos que puedan adaptarse rápidamente a nuevas situaciones y tipos de datos.

En conclusión, tanto en la IC como en la GE, la selección y adaptación de modelos de datos adecuados es fundamental para el manejo eficiente y efectivo de la información.

#### 2.5.4. Ecosistemas de datos (*DataLakes* Interoperables)

Con el auge del BD, ha surgido la necesidad de repensar los métodos tradicionales de almacenamiento y gestión de datos. Originalmente, las bases de datos relacionales SQL como Oracle DB, SQL Server y MySQL dominaban el panorama, ofreciendo estructuras robustas y estandarizadas para el manejo de datos. Estas bases de datos han sido fundamentales en la infraestructura de datos de muchas organizaciones:

- **Oracle DB:** Destaca en el manejo de grandes volúmenes de datos y es ampliamente utilizado en entornos empresariales.
- **SQL Server [80]** de Microsoft: Ofrece una integración sólida con otras herramientas de Microsoft y se enfoca en la seguridad y el rendimiento.
- **MySQL:** Popular por su naturaleza de código abierto, ligereza y eficacia, especialmente en aplicaciones web.
- **PostgreSQL [81]:** Reconocido por su compatibilidad con estándares y su extensibilidad, es una opción robusta para aplicaciones complejas.

Sin embargo, el rápido crecimiento del volumen, la velocidad y la variedad de los datos ha expuesto limitaciones en estas bases de datos tradicionales, conduciendo a una transición hacia soluciones más flexibles y escalables como

## 2.5 Interoperabilidad entre agencias

---

*Not only SQL* (NoSQL)[82] y *DataLakes* [83]. Estos nuevos enfoques responden a la demanda de manejar grandes cantidades de datos variados, no estructurados o semiestructurados, de manera eficiente. Entre las tecnologías NoSQL más destacadas se encuentran:

- **MongoDB** [84]: Conocida por su flexibilidad y escalabilidad en el manejo de datos variados.
- **Apache Cassandra** [85]: Sobresale en aplicaciones de alta disponibilidad que requieren escalabilidad.
- **Neo4j** [86] y **Redis**: Ofrecen soluciones especializadas para datos relacionales complejos y almacenamiento en memoria, respectivamente.
- **Apache HBase** [87]: Basada en Hadoop, es ideal para aplicaciones que requieren acceso rápido a grandes cantidades de datos.
- **Google BigQuery** [88]: Una solución de almacén de datos empresarial orientada a consultas rápidas y análisis en grandes conjuntos de datos.
- **Hadoop Distributed File System (HDFS)** [89]: Proporciona un sistema de archivos distribuido que maneja grandes conjuntos de datos en un entorno de cómputo distribuido.
- **MinIO** [90]: Ofrece almacenamiento de objetos de alto rendimiento y compatible con APIs de *Simple Storage Service* (S3) [91], ideal para *DataLakes*.

Además, el concepto de *DataLakes* ha emergido como una solución vital en el ecosistema de BD. Un *DataLake* interoperable permite almacenar grandes cantidades de datos en bruto en un formato no estructurado, proporcionando la flexibilidad de estructurarlos según sea necesario. Este enfoque mejora significativamente la agilidad y eficiencia en el análisis de datos, permitiendo a las organizaciones adaptarse rápidamente a las cambiantes demandas de información.

Por lo tanto, un *DataLake* interoperable es esencial para gestionar eficazmente la variedad y el volumen de datos en entornos de BD. La configuración de un *DataLake* efectivo implica la integración de varios motores de almacenamiento y procesamiento de datos para facilitar el acceso y análisis de datos heterogéneos provenientes de múltiples fuentes. A continuación, se presenta un ejemplo de configuración:

- **HDFS para almacenamiento de datos en bruto:** Utilizando HDFS, se almacenan grandes volúmenes de datos no estructurados y semiestructurados. HDFS sirve como la columna vertebral del *DataLake*, proporcionando un almacenamiento distribuido y escalable.
- **Apache Kafka para ingesta de datos en tiempo real:** Kafka [92] actúa como un sistema de mensajería distribuido que permite la ingestión de datos en tiempo real desde diversas fuentes, como sensores IoT, registros de aplicaciones y flujos de datos en vivo.
- **Apache Spark para procesamiento y análisis:** Spark [93] se integra con HDFS y Kafka para realizar el procesamiento en memoria de grandes conjuntos de datos. Permite análisis avanzados, procesamiento de flujos y ML.
- **MinIO para almacenamiento de objetos optimizado:** MinIO se utiliza para el almacenamiento de objetos altamente escalable y accesible, compatible con APIs de S3, facilitando la integración con una variedad de aplicaciones y servicios.
- **Apache Cassandra para bases de datos distribuidas:** Para aplicaciones que requieren alta disponibilidad y rendimiento consistente, Cassandra ofrece un modelo de datos flexible y escalabilidad horizontal.
- **Metadatos y catalogación con Apache Hive:** Hive [94] se emplea para la catalogación y gestión de metadatos, lo que facilita la organización, búsqueda y consulta de los datos almacenados en el *DataLake*.
- **Interfaz de usuario y visualización con Apache Superset:** Superset [95] permite a los usuarios acceder, explorar y visualizar datos a través de una interfaz gráfica, facilitando la interpretación y el análisis de datos complejos.

Esta configuración del *DataLake* es un ejemplo que permite la integración eficiente de datos de diferentes fuentes, ofreciendo flexibilidad y escalabilidad para el manejo de BD. La combinación de estos componentes proporciona una solución robusta y adaptable para diversas necesidades de almacenamiento, procesamiento y análisis de datos en entornos interagenciales y multidisciplinares.

Por lo tanto, mientras las bases de datos SQL tradicionales siguen siendo relevantes para ciertas aplicaciones, la evolución hacia soluciones NoSQL y *DataLakes* es imprescindible para manejar eficientemente el volumen y la complejidad de los datos actuales. La elección de la solución adecuada dependerá

de las necesidades específicas de estructura, volumen y rendimiento de los datos en cada proyecto.

## 2.6. Herramientas de análisis, visualización y toma de decisiones

La era digital actual ha traído consigo una explosión en la cantidad y complejidad de los datos disponibles, especialmente en campos críticos como la IC y la GE. En este contexto, la capacidad de analizar eficazmente estos datos y visualizarlos de manera comprensible se ha convertido en un aspecto fundamental para una toma de decisiones rápida y efectiva. Las herramientas modernas de análisis y visualización de datos brindan oportunidades sin precedentes para descubrir insights valiosos, facilitar la comunicación de información compleja y mejorar los procesos de toma de decisiones en estos campos dinámicos y desafiantes [96]. A continuación se exploran las tecnologías y herramientas clave que están revolucionando la forma en que los profesionales en la IC y la GE manejan, analizan y visualizan datos para tomar decisiones informadas y oportunas.

### 2.6.1. Tecnologías y herramientas para el análisis

En el ámbito de la IC y la GE, el análisis de datos desempeña un papel crucial. Las tecnologías modernas ofrecen soluciones avanzadas para analizar grandes volúmenes de datos, detectar patrones y obtener *insights* valiosos.

- **Análisis forense digital:** Herramientas como EnCase y FTK se utilizan ampliamente en la IC para el análisis forense de dispositivos electrónicos. Estas herramientas permiten la recuperación de datos, incluso de dispositivos dañados o formateados, y ayudan a identificar pruebas digitales clave.
- **Plataformas de análisis de datos:** Soluciones como IBM i2 Analyst's Notebook [97] ofrecen capacidades de análisis visual para descubrir conexiones ocultas entre datos en casos de IC. Similarmente, en la GE, herramientas como Tableau y Microsoft Power BI [98] permiten analizar y visualizar datos para mejorar la toma de decisiones y la respuesta ante emergencias.
- **SIG:** Aplicaciones como ArcGIS, QGIS [99] y Cesium [100] son fundamentales tanto en la IC como en la GE. Permiten analizar datos espaciales y temporales, lo que es crucial para la planificación de operativos y la gestión de recursos en situaciones de crisis.

- **Plataformas de IA:** El uso de la IA y el ML está en aumento tanto en la IC como en la GE. Herramientas como TensorFlow [101] y PyTorch [102] facilitan el análisis predictivo y la detección de patrones en grandes conjuntos de datos.

### 2.6.2. Visualización de datos en la investigación y toma de decisiones

La visualización de datos es un componente clave para interpretar complejos conjuntos de datos y facilitar una toma de decisiones efectiva.

- **Herramientas de visualización en Investigación Criminal:** En el ámbito de la IC, la visualización de datos ayuda a entender mejor las redes criminales y los patrones de delitos. Herramientas como Maltego [103] permiten visualizar relaciones complejas y redes entre entidades en investigaciones de ciberseguridad.
- **Visualización en la Gestión de Emergencias:** En situaciones de crisis, la visualización de datos proporciona una comprensión clara de la situación. Plataformas como Google Earth [104] y Ushahidi [105] ofrecen mapas interactivos que pueden ser cruciales para la coordinación de esfuerzos de respuesta y recuperación.
- **Dashboards y paneles de control:** Dashboards como los ofrecidos por Splunk [106] o Zabbix [107] permiten monitorizar en tiempo real eventos y alertas relevantes, tanto para equipos de IC como para operativos de emergencia, asegurando una respuesta rápida y coordinada.
- **Augmented Reality (AR) y VR:** La implementación de tecnologías de AR y VR está emergiendo como herramientas valiosas para la capacitación y simulación de escenarios en ambos campos, proporcionando entornos inmersivos o aumentados para la preparación y entrenamiento de personal.

Por lo tanto, la combinación de tecnologías avanzadas de análisis y visualización de datos en la IC y la GE permite una comprensión más profunda de los datos, facilitando una toma de decisiones más informada y eficaz.



## 2.7. Otras herramientas de apoyo y optimización de recursos

Las herramientas que hemos mencionado en secciones son solo una minúscula parte del panorama de soluciones que podemos encontrar en el ecosistema BD actual, la Figura 2.5 trata de mostrar la gran cantidad de aplicaciones y servicios que podrían enriquecer tanto el entorno de IC como GE. Además, ambos escenarios pueden beneficiarse del uso de herramientas avanzadas para el despliegue, automatización, comunicación y orquestación de recursos. Estas herramientas no solo mejoran la eficiencia y efectividad operativa, sino que también permiten una respuesta más rápida y precisa en situaciones críticas.

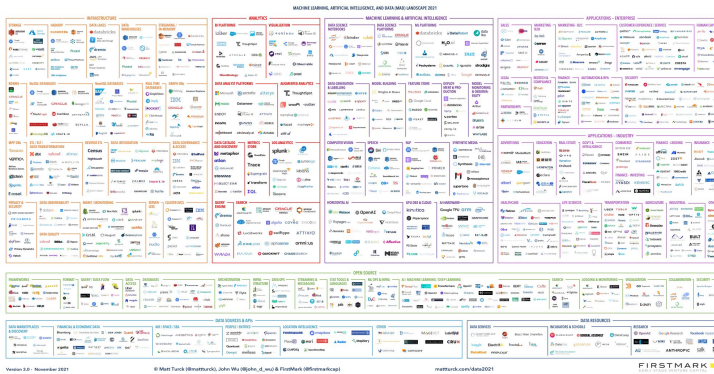


Figura 2.5: Ecosistema Big Data actual

### 2.7.1. Despliegue y automatización

La evolución tecnológica en el despliegue y automatización de aplicaciones y sistemas ha llevado a la adopción de tecnologías de contenedores y orquestación, superando a las soluciones tradicionales de virtualización.

**Ejemplos de herramientas de despliegue y automatización:**

- **Docker [108]** : Utilizado para crear, desplegar y ejecutar aplicaciones en contenedores, proporcionando un entorno consistente y aislado.
- **Kubernetes [109]** : Permite gestionar clústeres de contenedores a gran escala, facilitando la implementación, escalado y mantenimiento de aplicaciones distribuidas.

- **Ansible [110] y Terraform [111]:** Herramientas de automatización que se utilizan para configurar y gestionar infraestructuras, permitiendo despliegues rápidos y consistentes.

### 2.7.2. Comunicación y orquestación

En sistemas complejos, especialmente aquellos que utilizan arquitecturas de micros servicios, la comunicación y orquestación entre servicios son críticas para mantener la integridad, la seguridad y el rendimiento del sistema.

#### **Ejemplos de herramientas de comunicación y orquestación:**

- **API Gateways como Kong [112] y Zuul [113]:** Estas herramientas actúan como intermediarios para el manejo de solicitudes, proporcionando seguridad, registro y balanceo de carga.
- **Service Meshes como Istio [114] y Consul [115]:** Ofrecen una capa de comunicación dedicada para manejar interacciones de servicio a servicio, facilitando el descubrimiento de servicios, la monitorización y la seguridad.
- **Sistemas de mensajería como Kafka y RabbitMQ [116]:** Estos sistemas proporcionan comunicación robusta y escalable a través de colas de mensajes, permitiendo patrones de comunicación asíncronos y duraderos.
- **Herramientas de orquestación como *Amazon Web Services (AWS) [117] Elastic Container Service (ECS) [118] y Azure Kubernetes Service [119]*:** Facilitan la gestión de contenedores a escala, asegurando que los recursos se utilicen de manera eficiente y que las aplicaciones estén disponibles y escalables según sea necesario.

La integración de estas herramientas en plataformas de IC y GE facilita un entorno de trabajo más ágil, escalable y seguro. Su aplicación permite la optimización de recursos, mejorando la capacidad de respuesta y la eficiencia en situaciones críticas.

## Capítulo 3

# Especificación de la Arquitectura

### 3.1. Introducción

Como se discutió anteriormente en el Capítulo 2, los sistemas actuales destinados a optimizar la operativa en la prevención y resolución de crímenes, así como en situaciones de emergencia, enfrentan desafíos importantes en términos de eficiencia y capacidad de interoperabilidad. A pesar de los avances tecnológicos, estos sistemas suelen ser complejos y fragmentados, lo que dificulta la integración y el intercambio efectivo de la información entre las agencias y organismos involucrados. Además, la falta de interoperabilidad limita la capacidad de análisis de información y toma de decisiones basadas en datos. Esto se traduce en demoras en la respuesta ante eventos críticos y en la pérdida de oportunidades para anticiparse y prevenir incidentes. Por tanto, es fundamental desarrollar una arquitectura de interoperabilidad robusta y flexible que permita la comunicación fluida y el intercambio de datos en tiempo real, mejorando así las capacidades de análisis de información y toma de decisiones para reforzar la seguridad y resiliencia en entornos de emergencia y prevención de crímenes.

El objetivo principal de este capítulo es establecer e implementar una arquitectura general innovadora, detallada y cuidadosamente diseñada para evitar las limitaciones que suelen tener los sistemas tradicionales utilizados. Esta arquitectura tiene la versatilidad de ser empleada tanto en entornos estáticos, como en oficinas para el análisis exhaustivo de pruebas, así como en situaciones caóticas y peligrosas en intervenciones de emergencia en campo, donde la dinámica del entorno puede presentar desafíos adicionales. Se examinan

## CAPÍTULO 3. ESPECIFICACIÓN DE LA ARQUITECTURA

---

detalladamente cada uno de los componentes y procesos de la arquitectura, desde la adquisición y fusión de datos hasta el análisis y representación de la información. En ambos contextos, se enfatizará la importancia de la interoperabilidad entre agencias y la optimización de la comunicación y colaboración interagencial. Además, se analizará cómo esta arquitectura puede ser adaptada a diferentes escenarios y entornos, brindando flexibilidad y escalabilidad en su implementación.

En virtud de esta consideración, la arquitectura propuesta se aplicará de manera integral a los requisitos de los usuarios finales tanto del proyecto MAGNETO como del proyecto ASSISTANCE. Sin embargo, es importante destacar que existirán ciertas peculiaridades específicas de cada proyecto, las cuales se explicarán en detalle más adelante en la presente tesis.

### 3.2. Visión general de la arquitectura

La arquitectura propuesta para mejorar las capacidades de análisis de información y toma de decisiones se basa en la integración de diversos componentes software, tanto propios como de colaboradores, con el fin de aprovechar la experiencia y conocimientos complementarios. Debido a que estos componentes pueden pertenecer a diferentes empresas, entornos y lógicas, es necesario establecer una comunicación eficiente entre ellos.

En este sentido, se utilizan llamadas remotas síncronas o mensajería asincrónica a través de diversas tecnologías como *Java Remote Method Invocation* (RMI) [120], SOAP WS, REST o *Java Message Service* (JMS) [121]. Sin embargo, es común encontrar diferentes “silos” de software, es decir, aplicaciones o productos que trabajan de manera aislada. Por tanto, es necesario lograr la comunicación entre ellos para que funcionen de manera conjunta y eficiente.

En la actualidad, se consideran dos arquitecturas principales para lograr esta integración [122]:

1. Basada en *Enterprise Service Bus* (ESB) [123] y SOAP: Esta arquitectura se ha utilizado durante varios años y permite la integración de componentes a través de un bus de servicios empresariales. Permite que las aplicaciones y servicios se comuniquen entre sí de manera desacoplada. Todas las aplicaciones pueden conectarse al bus y publicar y recibir mensajes. Las aplicaciones no son responsables de conectarse entre sí directamente, sino que publican sus mensajes en el bus y todas las partes interesadas escuchan y reaccionan.

2. Microservicios utilizando un API Gateway: Esta arquitectura más reciente es una solución ligera que puede ser óptima en ciertos escenarios [124]. Un API Gateway es un servidor que actúa como el punto de entrada único del sistema. En él se encapsula la arquitectura interna del sistema y se proporciona una API personalizada para cada cliente. Además, se encarga de tareas como la autenticación, la monitorización, el equilibrio de carga, la memoria caché, la gestión y el modelado de solicitudes, así como el manejo de respuestas estáticas. El API Gateway también se encarga del enrutamiento de solicitudes, la composición y la traducción de protocolos. Todas las solicitudes de los clientes pasan primero por el API Gateway y luego se dirigen al microservicio correspondiente. Se han convertido en un componente esencial en el desarrollo moderno de aplicaciones que utilizan la arquitectura de microservicios para permitir comunicaciones internas y externas de alto volumen y baja latencia.

La arquitectura propuesta debe considerar la naturaleza del sistema integrado, ya que busca integrar varios componentes para procesar fuentes complejas de información.

La complejidad de la solución de software se basa en los requisitos que deben cumplirse. El sistema en su conjunto se caracteriza por la necesidad crítica de integración entre diversas tecnologías que hasta ahora han estado aisladas.

En este contexto, los requisitos generales de alto nivel para la plataforma se pueden resumir de la siguiente manera:

1. Heterogeneidad: Los componentes principales pueden ser extremadamente heterogéneos en cuanto a tecnología, comunicación, sincronización, etc. Por lo tanto, cualquier componente debe ser capaz de comunicarse e interoperar con cualquier otro, sin importar la tecnología con la que esté implementado.
2. Escalabilidad: La arquitectura debe ser escalable para manejar grandes volúmenes de flujos de datos de entrada. Por lo tanto, el sistema debe poder adaptarse y escalar según sea necesario. La implementación rápida de nuevas instancias de componentes debe ser una tarea sencilla, con el fin de admitir capacidades de escalamiento sin afectar el funcionamiento normal del sistema.
3. Flexibilidad/Desacoplamiento: La plataforma debe ser capaz de integrar nuevos componentes o reemplazarlos por otros nuevos en cualquier momento, sin interrumpir la operación normal del sistema. Además, sería altamente interesante que los diferentes componentes pudieran comunicarse y operar desde diferentes ubicaciones o entornos de manera federada, ya

## CAPÍTULO 3. ESPECIFICACIÓN DE LA ARQUITECTURA

---

que esto abriría nuevos mercados, reduciría los costos de implementación, aumentaría la velocidad de entrega y facilitaría la escalabilidad. Esto puede ser especialmente interesante en el caso de servicios fundamentales de BD.

4. Eficiencia: La plataforma debe admitir el procesamiento paralelo de datos para lograr eficiencia computacional. Por lo tanto, se requiere una arquitectura avanzada del sistema que proporcione una comunicación no bloqueante, basada en eventos y asíncrona, que permita la integración eficiente entre los componentes del sistema.

Basándose en estos requisitos, la arquitectura propuesta busca garantizar la interoperabilidad, escalabilidad, flexibilidad y eficiencia, permitiendo la integración adecuada de los componentes y optimizando las capacidades de análisis de información y toma de decisiones.

La transición de las arquitecturas basadas en ESB a las arquitecturas basadas en microservicios utilizando API Gateway se ha producido debido a una serie de razones clave que han impulsado este cambio. [125]

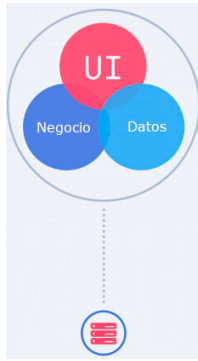
En primer lugar, las arquitecturas basadas en microservicios y API Gateway se alinean perfectamente con la tendencia actual de desarrollo de software hacia la modularidad y la agilidad. Los microservicios permiten que las funcionalidades sean desarrolladas, desplegadas y escaladas de manera independiente, lo que agiliza y simplifica el proceso de desarrollo y actualización de aplicaciones. Esto es especialmente valioso en entornos donde es necesario una rápida adaptación a los cambios del mercado y una mayor agilidad para entregar nuevas funcionalidades a los usuarios.

Además, las arquitecturas basadas en microservicios proporcionan una mayor escalabilidad y rendimiento en comparación con las arquitecturas basadas en ESB. Al permitir que los microservicios sean escalados de manera individual, se puede manejar una mayor carga de trabajo y se pueden soportar picos de demanda sin afectar el rendimiento general del sistema. En cambio, en las arquitecturas basadas en ESB, el escalado suele ser a nivel de todo el bus, lo que puede llevar a ineficiencias y cuellos de botella cuando se manejan cargas de trabajo intensas.

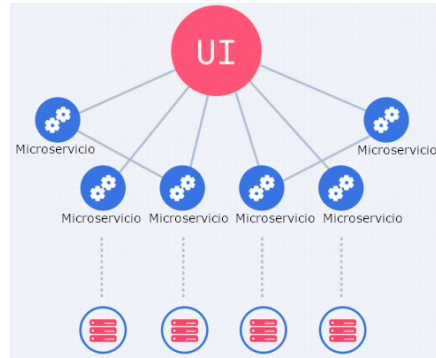
Otra ventaja importante de las arquitecturas basadas en microservicios y API Gateway es la flexibilidad en la elección de tecnologías y lenguajes de programación. Cada microservicio puede estar desarrollado utilizando las herramientas y lenguajes más adecuados para su funcionalidad, lo que permite aprovechar las fortalezas individuales de cada tecnología y facilita la evolución de los componentes del sistema. En cambio, las arquitecturas basadas en ESB a menudo limitan las opciones de tecnología y lenguaje de programación a las que son compatibles con el bus de servicios.

### 3.2 Visión general de la arquitectura

Finalmente, las arquitecturas basadas en microservicios fomentan el desacoplamiento entre los diferentes componentes del sistema, reduciendo las dependencias y facilitando la evolución y mantenimiento de cada microservicio de forma independiente. Esto proporciona una mayor flexibilidad en la adopción de nuevas tecnologías, la implementación de cambios y la escalabilidad, sin afectar a otros componentes del sistema.



**Figura 3.1:** Arquitectura Monolítica



**Figura 3.2:** Arquitectura de Microservicios

En cuanto a la comunicación entre los distintos componentes, en arquitectura de microservicios se ha adoptado el uso de WS y REST en lugar de las arquitecturas basadas en ESB para integrar los componentes de software. Los WS basados en el protocolo *Hypertext Transfer Protocol* (HTTP) [126] son ligeros, flexibles y admiten diferentes formas de transporte de información entre los componentes. Por otro lado, las soluciones de mensajería basadas en colas han ganado popularidad para la integración de sistemas complejos en los últimos años debido a su fiabilidad.

La arquitectura basada en microservicios y REST es una forma de desarrollar aplicaciones como un conjunto de servicios independientes, cada uno ejecutándose en su propio proceso y comunicándose mediante mecanismos ligeros como HTTP. Esto permite que cada microservicio sea independientemente desplegable y escalable, y gestionado y escrito por diferentes equipos. La arquitectura de microservicios se adapta bien a la metodología ágil, los diseños impulsados por el dominio y REST.

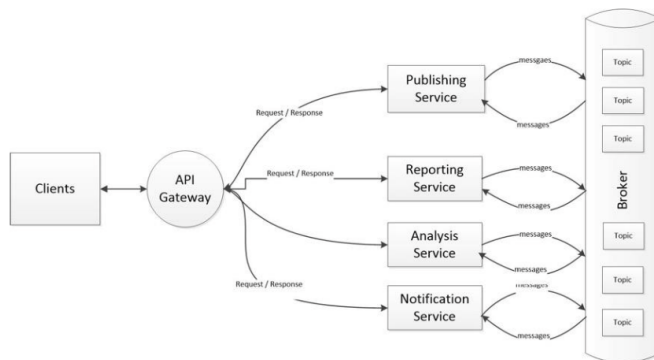
REST web services están diseñados para funcionar mejor en la web. Siguen el estilo arquitectónico REST, que trata a los datos y la funcionalidad como recursos accesibles a través de *Uniform Resource Identifier* (URI)s [127] utilizando operaciones bien definidas como crear, leer, actualizar y eliminar

## CAPÍTULO 3. ESPECIFICACIÓN DE LA ARQUITECTURA

(PUT, GET, POST, DELETE). Estas aplicaciones REST se caracterizan por ser sencillas, ligeras y rápidas, y permiten el acceso a los recursos en diferentes formatos.

En cuanto a la integración de mensajería, el Protocolo *Advanced Message Queuing Protocol* (AMQP) [128] es un estándar abierto para el intercambio de mensajes entre aplicaciones u organizaciones. RabbitMQ es una implementación de AMQP que proporciona una plataforma común para la comunicación basada en mensajes entre los servicios. Ofrece características como confirmaciones de entrega de mensajes, enrutamiento flexible, bibliotecas de clientes para varios lenguajes de programación y alta disponibilidad de colas.

En resumen, la transición hacia WS y REST, así como el uso de soluciones de mensajería como RabbitMQ, se ha producido debido a las ventajas que ofrecen en términos de flexibilidad, escalabilidad, rendimiento y facilidad de desarrollo y mantenimiento de aplicaciones. Estas arquitecturas se adaptan bien a los enfoques modernos de desarrollo y están respaldadas por estándares y herramientas maduras.



**Figura 3.3:** Arquitectura REST + AMQP

Teniendo en cuenta lo expuesto anteriormente, se opta por el diseño de una arquitectura con elementos que potencien la separación de funcionalidades y la escalabilidad de los componentes. Como se observa en la Figura 3.3 la arquitectura está dividida claramente en cuatro grandes partes o procesos: adquisición, fusión, análisis y representación. Para lograr esto, se ha optado por utilizar contenedores Docker, permitiendo desarrollar, probar y desplegar individualmente cada componente en su propio entorno aislado. Esta técnica ofrece flexibilidad y agilidad en el proceso de desarrollo y asegura una integración sin dificultades entre los elementos. Además, cada módulo expondrá una interfaz API REST con los diferentes servicios que permitan:

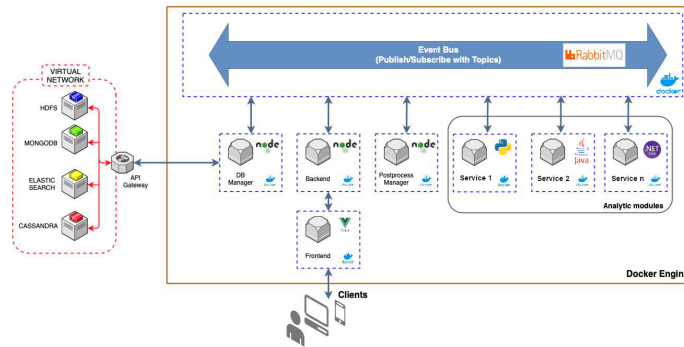


### 3.2 Visión general de la arquitectura

- Realizar pruebas en cada uno de los diferentes módulos con el fin de validar y facilitar la integración.
- Interfaz interna y solicitudes de servicios por parte de otros módulos (utilizando un token validado).
- Acceso directo externo desde usuarios finales/otros procesos a través de la puerta de enlace de la API de MAGNETO.

En cuanto a la comunicación entre los distintos módulos, se ha elegido RabbitMQ, basado en el protocolo AMQP y ofreciendo una transferencia fiable y eficiente de datos entre los diferentes componentes. Mediante la publicación y suscripción de mensajes en colas basadas en temas, se establece una comunicación confiable y transparente. Estos elementos, Docker y RabbitMQ, se combinan para forjar una arquitectura sólida y eficiente, permitiendo un trabajo unificado y colaborativo entre todos los componentes del sistema.

Esta estructura de arquitectura modular y escalable, junto con la división clara en las diferentes etapas de adquisición, fusión, análisis y representación, permitirá mejorar las capacidades de análisis de información y toma de decisiones, optimizando la colaboración y comunicación entre los diferentes procesos.



**Figura 3.4:** Arquitectura Propuesta

Además, la arquitectura propuesta debe estar preparada para recibir y procesar estos datos en su formato original, independientemente del tipo de archivo. Esto requiere contar con algoritmos y herramientas adecuadas para la extracción, transformación y carga de estos datos en la plataforma, así como la capacidad de realizar análisis y procesamiento específicos para cada tipo de archivo.

Es importante considerar la eficiencia en el almacenamiento y procesamiento de estos datos, ya que la plataforma debe ser capaz de manejar volúmenes

masivos de información de manera rápida y eficiente. Esto implica la utilización de tecnologías y técnicas de procesamiento distribuido, como el uso de sistemas de almacenamiento y procesamiento distribuido, paralelización de tareas y elaboración de algoritmos eficientes para el procesamiento de datos.

En las siguientes secciones se detalla cada una de las fases, desde la adquisición hasta la representación de los datos.

### 3.3. Adquisición de datos

Es fundamental destacar la importancia de diferenciar las fuentes de datos en función del entorno específico en el que se aplicarán. En el contexto de prevención e investigación de crímenes, es común recopilar y analizar datos provenientes de diversas fuentes como transferencias bancarias, registros telefónicos, atestados policiales y grabaciones de cámaras de seguridad. Estos datos son fundamentales para realizar análisis retrospectivos y llevar a cabo investigaciones detalladas para identificar patrones, establecer conexiones y obtener pruebas concretas.

Por otro lado, en un entorno de acción rápida, como en la GE o situaciones operativas en tiempo real, las fuentes de datos son distintas y están orientadas a obtener información en tiempo real. En este escenario, las fuentes de datos pueden incluir videos capturados desde UAVs, sistemas de posicionamiento de unidades, grabaciones de cámaras ubicadas en lugares estratégicos, entre otros. Estos datos en tiempo real son cruciales para facilitar la toma de decisiones ágil, la coordinación de recursos y la capacidad de respuesta inmediata ante situaciones críticas.

Distinguir claramente estas dos categorías de fuentes de datos garantiza una comprensión más precisa de los requerimientos y los procesos de adquisición de datos en cada entorno específico. Esto permite establecer los mecanismos adecuados para recopilar, procesar y analizar la información relevante de manera eficiente y efectiva, optimizando así las capacidades de análisis de información y toma de decisiones en cada contexto.

#### 3.3.1. Entorno de Prevención e investigación

Además de distinguir el entorno también hay que caracterizar los datos por caso de uso, así podemos distinguir las distintas fuentes de datos según su caso de uso:

- **Crimen contra personas y propiedad:**
  - *Documentos:* Informes policiales, declaraciones de testigos, registros judiciales.

- *Datos:* Registros de incidentes, bases de datos de huellas dactilares y ADN, imágenes de CCTV, registros de propiedad y vehículos.
- **Crimen económico organizado:**
  - *Documentos:* Registros de auditoría, informes de inteligencia financiera, actas de reuniones corporativas.
  - *Datos:* Transacciones bancarias, registros de empresas y accionistas, patrones de transacciones sospechosas, datos de mercado y comercio.
- **Prevención e investigación de ataques terroristas:**
  - *Documentos:* Informes de inteligencia, resúmenes de vigilancia, transcripciones de interceptaciones.
  - *Datos:* Comunicaciones interceptadas (llamadas, emails, mensajes), publicaciones en redes sociales, datos de viajes y movimientos, bases de datos de listas de vigilancia.
- **Circuitos económicos ilegales paralelos del crimen organizado:**
  - *Documentos:* Informes de transacciones sospechosas, análisis de expertos en lavado de dinero.
  - *Datos:* Flujos financieros ilícitos, transacciones y transferencias, registros de activos, rastreos de bienes inmuebles y de lujo.
- **Crimen de identidad:**
  - *Documentos:* Informes de robo de identidad, historiales de crédito, registros de denuncias.
  - *Datos:* Bases de datos de documentos de identidad emitidos y robados, historiales de transacciones financieras, registros de acceso a servicios y sistemas.

#### 3.3.2. Entorno de intervención rápida

Al abordar la intervención rápida en situaciones críticas, las fuentes de datos y su procesamiento deben adaptarse ágilmente a la naturaleza dinámica y a menudo caótica de las emergencias. En este contexto, cada ámbito de actuación exige un conjunto particular de documentos y datos que faciliten la toma de decisiones y la ejecución eficaz de las operaciones.

- **Gestión de Emergencias y respuesta ante desastres:**

## CAPÍTULO 3. ESPECIFICACIÓN DE LA ARQUITECTURA

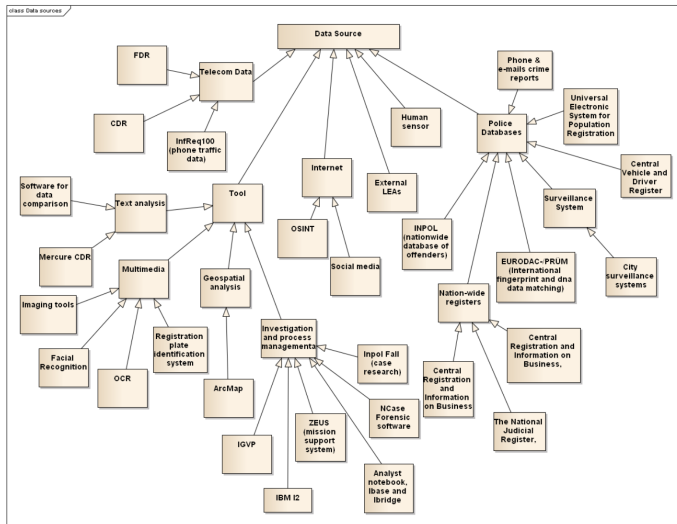


Figura 3.5: Fuentes de Datos Prevención / Investigación

- *Documentos*: Planes de contingencia, reportes de situación, registros de comunicaciones de emergencia.
  - *Datos*: Imágenes y videos de UAVs y robots, registros de posicionamiento GPS de unidades en terreno, entradas de datos de los usuarios, telemetría de sensores.
- **Supervisión y reconocimiento de áreas afectadas:**
    - *Documentos*: Mapas de áreas afectadas, informes de evaluación de daños, actas de coordinación interagencial.
    - *Datos*: Secuencias de vídeo en tiempo real de cámaras de vigilancia, análisis de imágenes satelitales, datos de sensores ambientales.
- **Coordinación de Unidades de Campo:**
    - *Documentos*: Protocolos de actuación, guías de procedimientos operativos, comunicaciones entre equipos.
    - *Datos*: Localización en tiempo real de las unidades de respuesta, datos de seguimiento de recursos, información de estado de las unidades.
- **Análisis de información para toma de decisiones:**

- *Documentos*: Análisis de inteligencia, reportes de progreso, revisiones estratégicas.
- *Datos*: Modelos predictivos basados en datos históricos, estadísticas de incidentes, simulaciones y modelados de eventos.

El enfoque principal de esta fase en la arquitectura de BD es establecer una infraestructura robusta y adaptable que facilite la adquisición y almacenamiento eficientes de grandes volúmenes de datos. Esta infraestructura se estructura en dos capas fundamentales:

1. **Adquisición de datos**: Esta capa se centra en plataformas de procesamiento de flujos como Apache Kafka o RabbitMQ, incluyendo herramientas específicas para la interoperabilidad y la migración y extracción semi-automatizadas desde sistemas legados. Dependiendo del análisis detallado en la fase de implementación, podría integrarse un balanceador de carga como HAProxy [129], NGINX [130] o Tornado [131], para optimizar el flujo de datos entrantes.
2. **Almacenamiento de datos**: Esta capa es crucial para la gestión de las diversas necesidades de almacenamiento del proyecto, no solo en términos de datos sino también para configuraciones y otras bases de conocimiento relacionadas. Se contempla la utilización de múltiples sistemas de bases de datos, cada uno adaptado a requerimientos específicos. Por ejemplo, Cassandra se podrá utilizar para operaciones transaccionales en tiempo real, dada su capacidad de escalado y ausencia de un único punto de fallo. MongoDB se selecciona para casos de uso especializados, como aquellos que involucran datos geolocalizados o en fases de prototipado. Por otro lado, HDFS se destinará para el almacenamiento en *Datalakes* y procesamiento por lotes, adecuado para manejar petabytes de información, como videos, audio, etc.

Los módulos desarrollados para cubrir estas dos capas son los siguientes:

#### 3.3.3. DB-MANAGER

El *DB-Manager* juega un papel crucial como orquestador central para la gestión de datos en la plataforma. Este módulo ha sido diseñado para manejar eficazmente tanto el alto volumen como la diversidad de los datos, permitiendo así una abstracción efectiva para los diferentes servicios que interactúan con los datos, independientemente del motor de almacenamiento utilizado para las operaciones *Create, Read, Update, Delete* (CRUD).

## CAPÍTULO 3. ESPECIFICACIÓN DE LA ARQUITECTURA

El funcionamiento del *DB-Manager* se describe de la siguiente manera:

- Gestión de solicitudes:** El *DB-Manager* utiliza un cliente RabbitMQ que está suscrito a varios Topics para gestionar todas las operaciones CRUD. Los diferentes módulos que requieran realizar estas operaciones solo necesitan formular un mensaje en formato JSON y publicarlo en el *Broker* de RabbitMQ.
- Procesado de consultas:** Al recibir un mensaje, el *DB-Manager* identifica la operación requerida y el motor específico encargado de ejecutarla. A continuación, se genera la consulta específica para ese motor y se lleva a cabo a través de su API.
- Respuesta y Comunicación:** Una vez que el motor de datos proporciona una respuesta, el *DB-Manager* crea un mensaje con esta información y lo envía de vuelta al servicio solicitante.

La arquitectura propuesta permite una distribución eficiente en la ingestión de datos, y establece una relación clara entre el *DB-Manager* y las distintas APIs de los motores implementados en la plataforma. Como se ilustra en la Figura 3.6 se ha optado por un enfoque de despliegue virtualizado, donde todas las máquinas están contenidas dentro de una red virtual. Esta configuración, accesible únicamente a través del *DB-Manager*, aporta una capa adicional de seguridad a los datos almacenados, ya que cualquier operación sobre los motores debe ser autorizada por el *DB-Manager*. Este enfoque garantiza la integridad y la seguridad de los datos, aspectos fundamentales para la eficacia de la plataforma en el análisis de información y la toma de decisiones.

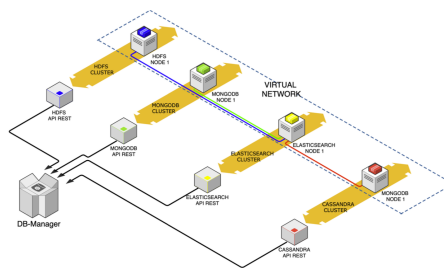


Figura 3.6: DB Manager

La combinación de estos sistemas garantiza una gestión de datos flexible y escalable, adecuada para una amplia gama de aplicaciones y escenarios, desde el

manejo de grandes cantidades de datos en tiempo real hasta el almacenamiento a largo plazo y análisis por lotes de información.

En algunos casos la información se almacena en bruto y en otros casos deben pasar por un proceso previo de preparación e indexación con el fin de extraer características de nivel bajo y medio que serán utilizadas en etapas posteriores de análisis a un nivel más alto por medio de módulos desarrollados específicamente. Como parte de esta fase de preparación, se extraen características visuales de los datos de vídeo e imagen.

Por ejemplo, se puede realizar una separación entre el primer plano y el fondo con el objetivo de mejorar la precisión de otros algoritmos de procesamiento de vídeo e imagen. En ficheros de audio se lleva a cabo la extracción de descripciones de audio y el procesamiento adicional de la señal de audio.

En el caso de archivos de texto en diferentes idiomas, se lleva a cabo una traducción automática al inglés con el objetivo de unificar toda la información en un único lenguaje. Esto permite que durante el proceso de análisis y recuperación de texto, se pueda trabajar de manera coherente y eficiente en un idioma común. Para pasar al siguiente paso (Fusión de datos) es necesario realizar un pre procesamiento de los datos.

### 3.4. Fusión de datos

Tras haber establecido las bases en el apartado de adquisición de datos, donde se delinea el proceso de recolección de datos e indexación de las distintas fuentes, esta fase se enfoca en la fusión de los datos obtenidos, provenientes de diversas fuentes y en diferentes formatos.

Esta etapa es fundamental, ya que permite transformar los datos dispersos y no procesados en información estructurada y coherente. Para lograr esto, se aplican técnicas y algoritmos de fusión de datos, que permiten combinar y agrupar los datos de manera lógica y homogénea.

Posteriormente, esta información fusionada y refinada se almacena utilizando una ontología diseñada a medida, lo que garantiza una organización y un acceso eficiente a la información, de acuerdo con las necesidades específicas de cada proyecto.

#### 3.4.1. Modelo de Representación Común

Una vez que los datos han sido procesados, es fundamental contar con un *Common Representational Model* (CRM) para poder unificar y estructurar la información obtenida de manera coherente. En este sentido, las ontologías juegan un papel clave. Una ontología es un conjunto de conceptos, propiedades y

## CAPÍTULO 3. ESPECIFICACIÓN DE LA ARQUITECTURA

---

relaciones que nos permite definir y representar el conocimiento de un dominio específico. Las ontologías proporcionan una estructura formal que nos permite organizar la información de manera clara y semánticamente rica.

El uso de ontologías en el proceso de fusión de datos nos permite integrar la información proveniente de diferentes fuentes y distintos formatos de manera coherente. Al definir una ontología adecuada, podemos establecer un marco de referencia compartido y estandarizado que facilita la interoperabilidad entre los diferentes sistemas y permite el intercambio y la interpretación adecuada de los datos. [132]

La *Knowledge Base* (KB), o base de conocimiento, juega un papel fundamental en este proceso. La KB es un repositorio centralizado en constante evolución donde se almacena y organiza el conocimiento específico del dominio [133]. Esta base de conocimiento puede incluir diferentes tipos de información, desde hechos y relaciones entre los datos hasta reglas y algoritmos de inferencia. La KB se nutre de la información procesada y estructurada previamente, permitiendo realizar consultas y generar nuevos conocimientos a través de técnicas de análisis y razonamiento [134]. Esto permite tener una visión global y completa de los datos, eliminando duplicidades y redundancias, y facilitando el acceso y la manipulación de la información consolidada.

Conforme se introduce nueva información en el sistema, la KB evoluciona y se enriquece, permitiendo la incorporación de nuevos conocimientos y fortaleciendo la capacidad de análisis y toma de decisiones. Esta evolución constante es esencial para mantener actualizada e integrada toda la información relevante, garantizando una representación precisa y actualizada del dominio de investigación.

Además, la KB también puede beneficiarse de técnicas de procesamiento de lenguaje natural, aprendizaje automático y minería de datos para realizar análisis más avanzados y descubrir patrones ocultos en los datos fusionados. Estos análisis ayudan a extraer conocimiento valioso y a generar recomendaciones útiles.

### 3.5. Análisis de datos

Una vez que se ha establecido un CRM y se han integrado múltiples fuentes de datos en una base de conocimiento coherentes, se da paso a la fase de análisis, mediante la cual los datos estructurados en la base de conocimiento son interpretados, permitiendo identificar patrones, tendencias y anomalías. En este contexto, las ontologías previamente establecidas proporcionan el marco conceptual que guía la interpretación y la extracción de conocimiento.



Esta arquitectura proporciona soporte para una amplia variedad de tipos de análisis, algunos de los cuales pueden ser ejecutados directamente por el usuario a través de la interfaz, mientras que otros pueden llevarse a cabo sin requerir ninguna acción por parte del usuario. Algunos análisis dependerán de la realización de análisis previos, mientras que otros pueden ser independientes.

En todos los casos, cada análisis se implementa como un microservicio dockerizado, lo que permite su ejecución eficiente y aislada. Estos microservicios son orquestados el módulo de post procesamiento (Postprocess-Manager) que asegura su funcionamiento ordenado. Una vez que se completa un análisis y se transfieren los resultados, el microservicio se detiene automáticamente, evitando así la ejecución simultánea y el desperdicio innecesario de recursos. Esta dinámica asegura una utilización eficiente de los recursos disponibles, optimizando el rendimiento y minimizando los costos asociados con la ejecución de múltiples servicios simultáneamente.

#### 3.5.1. Postprocess-Manager

Este módulo desempeña un papel esencial al orquestar y gestionar los diversos análisis realizados en la plataforma. Además de supervisar la ejecución de los análisis, este módulo informa sobre el éxito o los errores que puedan surgir durante dicho proceso. Para garantizar la eficiencia y escalabilidad, este módulo se ejecuta dentro de un contenedor Docker, lo que nos permite ajustar su capacidad según sea necesario. Esta implementación en contenedor se alinea con la estructura general de la plataforma, tal como se muestra en la Figura.

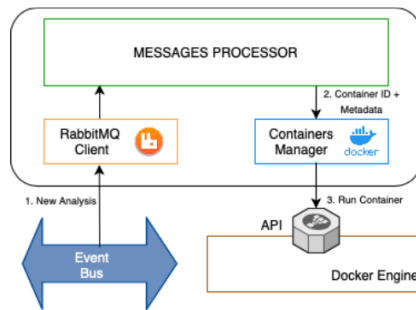


Figura 3.7: Postprocess Manager

En la Figura 3.7 se pueden diferenciar 3 subcomponentes:

- **RabbitMQ Client**

El módulo cuenta con un cliente AMQP que se conecta al *Broker* de

Rabbit y se suscribe a los topics de **analysis.new**, **analysis.success** y **analysis.error**. Esto significa que cualquier componente de la plataforma que publique mensajes con estos topics, serán detectados por el cliente de Rabbit y transmitidos al subcomponente Message Preprocessor.

### ■ Messages Preprocessor

Es responsable de procesar los mensajes JSON recibidos. Dependiendo del *topic* en el que se haya publicado el mensaje, este subcomponente llevará a cabo una tarea diferente.

#### ● Nuevo análisis

Cada vez que se recibe un nuevo análisis o conjunto de análisis, se realiza una identificación de las dependencias entre ellos. A continuación, se colocan en diferentes colas de ejecución para llamar al contenedor designado específicamente para llevar a cabo el procesamiento correspondiente.

En el visor de código 3.1 que tenemos a continuación podemos ver el ejemplo de un mensaje de nuevo análisis.

```
1 {
2   _id : "5e5e4793bd8d3796392507a7",
3   "analysis" : [
4     {
5       "type" : "analysis-type",
6       "status" : true,
7       "result" : null
8     },
9     {
10      "type": "analysis-type.subanalysis",
11      "status" : true,
12      "result" : null
13    }
14  ],
15  "date": "2023-04-06T15:30",
16  "fileName": "audio.mp3",
17  "path": "hdfs/535d9-0e27-43cc-868c-ec98b5ea/audio"
18 }
```

**Listing 3.1:** Mensaje nuevo análisis.

El bloque de código muestra un *array* de análisis, donde cada elemento contiene propiedades que indican el tipo de análisis, el estado (si se debe realizar o no) y el resultado obtenido. Además, el mensaje incluye información adicional relevante, como el `_id` que identifica el archivo almacenado en la base de datos para su análisis, la fecha en la que se solicitó realizar el análisis, el nombre del archivo y su ruta en el sistema de archivos distribuido HDFS.

- **Análisis finalizado con éxito**

Una vez que se ha llevado a cabo un análisis, el contenedor responsable de su ejecución publica un mensaje en el *Broker*. Esto tiene el propósito de informar al Post-Process Manager que el análisis ha finalizado, lo que le permite ejecutar cualquier análisis dependiente si es necesario. Además, se notifica al DB-Manager con el resultado del análisis y se almacena en la base de datos correspondiente.

A continuación, en el visor de código 3.2, se muestra un ejemplo de mensaje recibido tras una ejecución exitosa de un análisis.

```
1 {
2   "_id": "5e5e4793bd8d3796392507a7",
3   "caseId": "535d9f4b_0e27_43cc_868c_ec98b5eae94a",
4   "analysis": [
5     {
6       "type": "speech_to_text",
7       "status": false,
8       "result": "Listen a minute. But on the banks.
9                 Thanks a lot though he biggest fan of banks.
10                Eric s i ve had too many bad experiences over
11                them. Im really dont know how they can have the
                   toys and say they look off to you. They dont.
                   And charges away to college you."
9     }
10  ]
11 }
```

**Listing 3.2:** Mensaje resultado análisis

- **Análisis finalizado con errores**

Cuando un análisis ha finalizado con errores, se publica un mensaje en el *Broker* que contiene la posible causa del error. Esto tiene como objetivo notificar al usuario de que el análisis no se ha realizado correctamente. Los componentes suscritos a este *topic* incluyen el Postprocess-Manager, quien se encarga de manejar análisis dependientes que no se ejecutarían en caso de un error, y el *Backend* del HMI para transmitir el error al usuario a través de notificaciones.

En el visor de código 3.3 que se muestra a continuación, se presenta un ejemplo de mensaje recibido tras una ejecución incorrecta del análisis “speech-to-text”.

```
1      {
2      "_id": "5e5e4793bd8d3796392507a7",
3      "analysis": [
4      {
5      "type": "analysis-type ",
6      "error": true,
7      "message": "Audio format not compatible . "
8      }
9      ]
10 }
```

**Listing 3.3:** Mensaje error análisis.

En el ejemplo mostrado, se puede observar que el análisis lanzado ha tenido un error y ha publicado un mensaje de error correspondiente. En este caso particular, el archivo de entrada utilizado no era compatible con el módulo de transcripción, lo que dio como resultado la falla del análisis.

### ■ Containers Manager

El subcomponente de administración de contenedores, recibe como parámetros de entrada el nombre del contenedor responsable de la ejecución del análisis y los metadatos necesarios para su procesamiento.

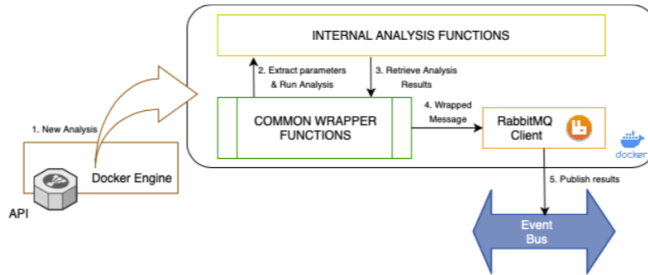
Para llevar a cabo la administración de los contenedores, se utiliza la API REST proporcionada por Docker, la cual permite iniciar y detener los contenedores encargados de realizar los análisis. Esta implementación garantiza que no sea necesario mantener servicios de análisis en ejecución constante, ya que se activan únicamente cuando se recibe un mensaje para realizar un nuevo análisis.

### 3.5.2. Módulos de análisis

Con el objetivo de optimizar y facilitar la escalabilidad de la plataforma, se ha creado una interfaz de programación común. Esta interfaz permite que cualquier análisis o funcionalidad nueva se integre fácilmente en la plataforma, evitando así la necesidad de desarrollos excesivamente complicados.

Cualquier nuevo análisis que se quiera incorporar a la plataforma deberá alinearse con la arquitectura definida, la cual está definida por un conjunto de reglas y especificaciones, como se puede ver en la Figura 3.8

Para integrarse de manera efectiva dentro de la plataforma, cada módulo de análisis debe ser diseñado para operar dentro de un contenedor Docker. Esta disposición posibilita que el Postprocess-Manager interactúe con el módulo de análisis a través de una API REST.



**Figura 3.8:** Módulo de Análisis

Considerando la posibilidad de que el código fuente del análisis no esté accesible — tal vez por no ser propietarios del mismo o porque utilice bibliotecas con licencias restrictivas —, se establece un subcomponente denominado *Common Wrapper Functions*. La tarea de este subcomponente es doble: primero, preparar los datos de entrada para que coincidan con el formato esperado por el módulo de análisis; y segundo, asegurarse de que la salida del análisis se convierta en el formato requerido por la plataforma.

Para completar el proceso, se incluye un cliente AMQP en el diseño, el cual se encarga de publicar los resultados del análisis en el *Broker* de RabbitMQ. De esta manera, los resultados se introducen en la plataforma y pueden ser procesados por los módulos suscritos a ese tipo de mensaje.

La Figura 3.8 ilustra el flujo operativo para cualquier análisis que se acoja a esta metodología propuesta:

1. El Postprocess-Manager inicia el análisis a través de la API REST del Docker Engine.
2. Los datos necesarios para el análisis son adaptados al formato apropiado por el módulo *Common Wrapper Functions*.
3. Terminado el análisis, este módulo también se encarga de transformar los resultados al formato estándar esperado por la plataforma, generando el mensaje JSON que mencionamos anteriormente.
4. Este mensaje JSON es publicado de nuevo en el *Broker* de RabbitMQ a través del cliente que el *Wrapper* incorpora. Se utilizará el *topic* correspondiente, dependiendo si el análisis ha sido exitoso o con errores. Permitiendo en caso de éxito que los resultados se distribuyan por la plataforma para su almacenamiento o uso posterior por otros componentes.

### 3.6. Representación de los datos

Tras abordar en el apartado anterior la fase del análisis de datos, donde se describió el proceso de tratamiento y análisis de extensos conjuntos de información para derivar conclusiones significativas, este apartado se enfoca en la *Representación de los Datos*. Esta fase es esencial para convertir los resultados del análisis en visualizaciones claras y operativas, lo que resulta fundamental para apoyar la labor de los operarios en áreas críticas como la prevención, la investigación y la respuesta rápida ante emergencias.

La representación eficaz de datos cobra especial importancia tras el proceso de análisis. Mientras que el análisis se centra en descubrir patrones, anomalías y correlaciones en los datos, la representación se encarga de convertir estos hallazgos complejos en formatos visuales claros y concisos. Este paso es crucial para asegurar que los *insights* obtenidos sean accesibles y útiles para los operarios, permitiéndoles tomar decisiones informadas basadas en una comprensión profunda y contextualizada de los datos.

En el contexto de la prevención e investigación, una representación de datos intuitiva y detallada permite a los operarios comprender mejor las tendencias emergentes y las interconexiones en los datos. Esto es vital para anticipar posibles situaciones de riesgo y para formular estrategias de investigación fundamentadas. Las herramientas de visualización en este escenario juegan un papel fundamental en simplificar la complejidad inherente a los grandes conjuntos de datos, transformándolos en información manejable y significativa.

En escenarios de intervención rápida, la representación de datos se vuelve aún más crítica. Aquí, la claridad y la capacidad de presentar información de manera directa son esenciales para garantizar que las respuestas sean rápidas y adecuadas. Las visualizaciones en estos casos deben ser diseñadas para enfocarse en la información más crítica, facilitando una interpretación rápida que permita a los operarios actuar con eficacia y precisión bajo presión.

La representación de datos actúa como un puente entre el análisis complejo y las aplicaciones prácticas en el campo. En este apartado, se discutirán las técnicas y herramientas que permiten esta transición, destacando cómo cada enfoque contribuye a mejorar la capacidad de los operarios para actuar de manera efectiva.

En el contexto de la arquitectura que estamos tratando, se han desarrollado diferentes HMIs especializadas que emplean distintas técnicas de visualización adaptadas a la naturaleza de los datos presentados. Además, se han explorado innovadoras pruebas de concepto que incorporan tecnologías de realidad virtual, ampliando así el espectro de herramientas de visualización.

En los apartados 4 y 5, se profundiza en cómo los métodos de visualización se adaptan específicamente dependiendo del contexto al que se aplican. En

el ámbito de la investigación y prevención, donde las operaciones pueden ser más estáticas, un entorno de computadora de escritorio puede ser suficiente para realizar las tareas requeridas. Sin embargo, en escenarios de intervención inmediata, la movilidad es clave; por ello, se integran dispositivos como tablets, diseñadas para ser utilizadas en el terreno. Estas tablets son un complemento esencial para los ordenadores de los centros de mando y control, permitiendo una operativa ágil y efectiva en situaciones críticas.

En la arquitectura diseñada, la representación visual de los datos se selecciona estratégicamente para alinearse con las características inherentes a cada tipo de información. Para datos que poseen una dimensión espacial, por ejemplo, se prefieren visualizaciones *Geographic Information System* (GIS) que proporcionan un contexto geográfico claro y permiten una interpretación intuitiva de la información georreferenciada. En contraste, para ilustrar las interacciones y las conexiones entre distintas entidades o para representar magnitudes y relaciones cuantitativas, se opta por estructuras de grafos, que son particularmente eficaces para desentrañar y mostrar la complejidad de las redes de datos.

La elección de la visualización se realiza de manera deliberada, buscando la más adecuada para la salida de cada análisis, con el fin de maximizar la comprensión y la utilidad práctica de los resultados. Esta personalización asegura que cada conjunto de datos se presente de la manera más reveladora y accesible posible.

Para integrar y simplificar el acceso a estas diversas formas de visualización, se han unificado dentro de un único dashboard web, como se observa en la Figura 3.9. Este entorno centralizado no solo facilita a los usuarios la ejecución de análisis de manera directa y sencilla, sino que también les permite visualizar los resultados de forma consolidada. Esta consolidación es clave para potenciar la conciencia situacional del usuario, proporcionando una visión global y actualizada que respalda la toma de decisiones informadas.

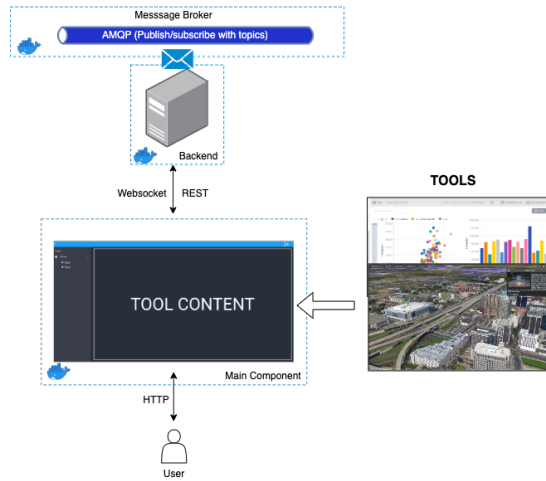
En cuanto a la interacción entre los diferentes HMIs y los datos almacenados, se estructura a través de una capa intermedia, conocida como el *Backend*. Esta capa actúa como el nexo central para todas las solicitudes de datos, orquestando el flujo de información según los requerimientos específicos de cada HMI. Para las situaciones que demandan un análisis en tiempo real, el *Backend* se sincroniza con las actualizaciones mediante suscripciones activas al *Broker* de RabbitMQ por el protocolo AMQP. En circunstancias que requieren una recuperación de datos más tradicional, el *Backend* realiza consultas directas a la base de datos.

La comunicación entre el *Frontend* y el *Backend* se adapta flexiblemente según las necesidades operativas. Utiliza websockets para el manejo eficiente de actualizaciones y notificaciones en tiempo real, garantizando una comunicación bidireccional y asíncrona que es crucial para la respuesta instantánea

## CAPÍTULO 3. ESPECIFICACIÓN DE LA ARQUITECTURA

---

y la interactividad del usuario. Paralelamente, para las operaciones CRUD, el *Frontend* se apoya en la API REST que el *Backend* expone, permitiendo así un intercambio de datos estructurado y estandarizado. Esta arquitectura asegura una integración y un manejo de datos cohesivos y eficientes, tal como se ilustra en la imagen siguiente.



**Figura 3.9:** Arquitectura HMI

En los capítulos dedicados a cada proyecto, se detallan las tecnologías elegidas y empleadas para cada módulo.



# Capítulo 4

## Caso 1: MAGNETO

### 4.1. Introducción

Con el fin de hacer frente a los cada vez más complejos retos a los que se enfrentan las LEAs en un contexto donde las actividades delictivas han evolucionado hacia la digitalización y la diversificación, se ha desarrollado el proyecto **MAGNETO**. Este proyecto se concibió con la finalidad de proporcionar una respuesta avanzada y multifacética a esta tendencia. La plataforma **MAGNETO** se presenta como un sistema modular diseñado para el procesamiento y análisis de grandes volúmenes de datos multimedia, brindando a las LEAs la capacidad de llevar a cabo ICs de forma más efectiva. A través de la utilización de tecnologías innovadoras y enfoques de vanguardia, **MAGNETO** tiene como objetivo potenciar la capacidad de las LEAs para enfrentar de manera eficiente los retos presentes en la era digital.

En la sociedad actual, caracterizada por la generación masiva de información digital, **MAGNETO** ofrece un marco estructural para mejorar la capacidad operativa de las LEAs en su lucha contra el crimen organizado y el terrorismo. Este marco proporciona la integración de múltiples fuentes de evidencia, incluyendo video, audio, datos de redes sociales y bases de datos policiales, ofreciendo herramientas analíticas flexibles para generar respuestas detalladas a las consultas de investigación.

La plataforma se basa en modelos de datos representativos, procesamiento semántico de información e inteligencia aumentada, y se centra en la anticipación y predicción de tendencias futuras, como amenazas, para establecer una base para el razonamiento y la cognición. **MAGNETO**, al aplicar un enfoque científico multidisciplinario, desarrolla nuevas tecnologías y componentes eficientes que permiten a las LEAs correlacionar datos, descubrir relaciones

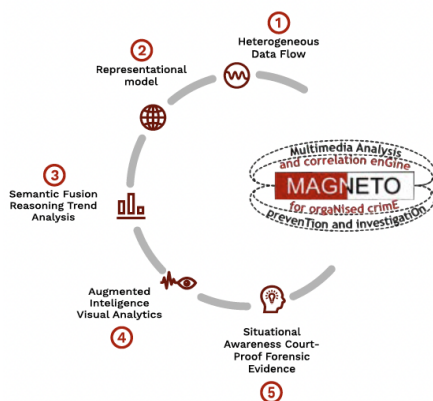


Figura 4.1: Concepto MAGNETO

ocultas, seleccionar y clasificar pruebas, evaluar y clasificar amenazas, razonar sobre casos criminales y visualizar y comprender las acciones pasadas o en tiempo real, todo ello desde un punto seguro y único.

## 4.2. Objetivos de MAGNETO

La visión global de MAGNETO se desglosa en dos categorías de objetivos detallados del proyecto: **científicos-técnicos** y **operativos**. Cada uno de estos objetivos seguirá el enfoque **S.M.A.R.T.** (Specific, Measurable, Attainable, Realistic and Timely). Esto garantiza un enfoque claro y medible para lograr los objetivos planteados en cada área del proyecto.

### 4.2.1. Objetivos Científicos-Técnicos

#### 1. Desarrollo de un CRM abierto

Desarrollar y estandarizar un CRM abierto para datos, que permita la explotación conjunta de diversas fuentes de datos multimedia. Este modelo facilitará el procesamiento semántico avanzado y la predicción de tendencias futuras, mejorando la interoperabilidad y el intercambio de información entre diferentes LEAs.

#### 2. *Framework* para la minería y etiquetado de datos heterogéneos

Crear un *Framework* para la minería, indexación y etiquetado de datos

heterogéneos, mejorando la interoperabilidad y la recopilación contextualizada de evidencias. Esto incluirá el desarrollo de herramientas modulares para el análisis y etiquetado de datos primarios.

### 3. **Herramientas de fusión de información semántica y razonamiento**

Investigar y desarrollar herramientas de fusión de información semántica y razonamiento, potenciando a las LEAs con capacidades superiores de análisis e investigación de crímenes. Esto incluirá técnicas avanzadas para descubrir nuevas relaciones y evidencias forenses.

### 4. **Desarrollo de HMIs orientadas al usuario**

Desarrollar HMIs centrados en el usuario que aumenten la conciencia situacional y la capacidad operativa de los agentes. Esto incluirá soluciones de minería visual dinámica y tecnologías hápticas para mejorar la eficiencia en rutinas diarias.

### 5. **Demostración y evaluación de tecnologías en casos realistas**

Integrar las herramientas de MAGNETO en una plataforma común y realizar demostraciones y evaluaciones en casos realistas con la ayuda de LEAs, siguiendo una metodología de desarrollo ágil.

### 6. **Organización de actividades de capacitación para la adopción de resultados con respecto a la UE**

Realizar actividades de capacitación y ejercicios como parte integral del proyecto para garantizar el uso adecuado y eficiente de las herramientas desarrolladas, y hacer el material de capacitación públicamente disponible.

### 7. **Framework para la transferencia de conocimientos y experiencias**

Establecer un marco para permitir la transferencia de conocimientos y experiencias en el uso de las herramientas de MAGNETO de una LEA a otra, lo que permitirá la identificación de las mejores prácticas para la implementación de las soluciones de MAGNETO más allá de la finalización del proyecto, y asegurar el efecto multiplicador del financiamiento de la UE

## 4.2.2. Objetivos Operacionales

### 1. **Facilitar a los investigadores afrontar los desafíos del crimen organizado y el terrorismo**

## CAPÍTULO 4. CASO 1: MAGNETO

---

Habilitar a los investigadores a enfrentar los crecientes desafíos planteados por el crimen organizado y los grupos terroristas, proporcionando modelos representativos de datos sofisticados y herramientas de análisis y razonamiento avanzadas, interoperables, modulares y escalables.

### 2. Gestión eficiente de investigaciones de crímenes

Proveer una gestión de investigaciones de crímenes más ágil y eficiente, lidiando mejor y correlacionando enormes cantidades de datos heterogéneos. MAGNETO permitirá a los oficiales de las LEAs consolidar consultas y buscar respuestas mediante un *Framework* escalable y un único punto de entrada.

### 3. Mejora en la prevención de crímenes organizados

Contribuir a la prevención mejorada de crímenes organizados a través del análisis de tendencias avanzado y el aumento de la conciencia situacional. MAGNETO dotará a las LEAs con herramientas analíticas de vanguardia, empleando procesamiento y fusión de información semántica avanzada, análisis de tendencias, técnicas de predicción y correlación, y métodos de aprendizaje automático adaptados.

### 4. Entrega de un *Framework*, interoperable y preparado para el futuro

Desarrollar un *Framework*, interoperable y preparado para el futuro, que cumpla con las directrices y mejores prácticas legales, éticas, procedimentales y de aceptación judicial en Europa. Esto incluirá la estandarización, definición de interfaces abiertas y la adopción de las mejores prácticas de la UE, asegurando la conformidad con las directrices éticas y legales relevantes, así como teniendo en cuenta las disposiciones del estándar de Privacidad por Diseño.

## 4.3. Arquitectura de MAGNETO

La complejidad integral del sistema MAGNETO se debe principalmente a la necesidad de integrar múltiples tecnologías que anteriormente operaban de manera aislada. Los requisitos de alto nivel para la plataforma MAGNETO, que se tuvieron en cuenta durante su desarrollo, se pueden resumir de la siguiente forma:

- **Heterogeneidad:** Los elementos esenciales de la plataforma presentan una gran diversidad en términos de tecnología, comunicación y tiempos de respuesta.

### 4.3 Arquitectura de MAGNETO

- **Escalabilidad:** La infraestructura de MAGNETO está diseñada para expandirse y manejar eficazmente un creciente volumen de datos, adaptándose a un aumento en la demanda de procesamiento.
- **Flexibilidad y Modularidad:** La plataforma permite la incorporación o sustitución de componentes de manera modular, garantizando que estos cambios no afecten su funcionamiento regular.
- **Eficiencia:** MAGNETO está equipado para realizar procesamiento de datos en paralelo, buscando maximizar la eficiencia computacional.

Como se puede observar en la Figura 4.2 los pilares que constituyen la plataforma de MAGNETO son:

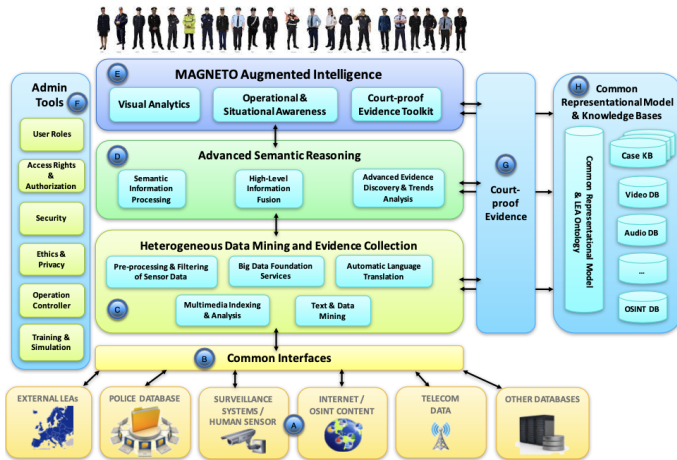


Figura 4.2: Arquitectura Plataforma MAGNETO

- El módulo de **Minería de Datos Heterogéneos y Recolección de Evidencias** (Heterogeneous Data Mining and Evidence Collection) en MAGNETO se ocupa de la evaluación y anotación de datos básicos. Este módulo utiliza los resultados de varias herramientas especializadas, que incluyen:
  - **Indexación y Análisis Multimedia** (Multimedia Indexing & Analysis): Convierte el contenido multimedia en metadatos digitales para su análisis.
  - **Minería de Texto y Datos** (Text & Data Mining): Extrae información valiosa de fuentes textuales.

## CAPÍTULO 4. CASO 1: MAGNETO

---

- **Preprocesamiento y Filtrado de Datos de Sensores** (Pre-processing & Filtering of Sensor Data): Se centra en la indexación de patrones en videos.
- **Servicios Esenciales de Big Data** (BD Foundation Services): Proporcionan acceso y manejo de infraestructuras de BD.
- **Traducción Automática** (Automatic Language Translation): Ofrece servicios de traducción automática para la plataforma MAGNETO.

Dentro de este componente, los Servicios Esenciales de BD juegan un papel crucial al proporcionar almacenamiento y manejo de grandes volúmenes de datos a todos los módulos y componentes de MAGNETO. Esto facilita una interfaz unificada de conocimiento accesible a todos los componentes de la plataforma. Entre otras funcionalidades, esto posibilita la integración de:

- Fragmentos de audio y vídeo etiquetados con caracterización según criterios de la LEA.
  - Ontologías relevantes para la estructuración de datos.
  - Datos de telecomunicaciones sobre sesiones y eventos de comunicación.
  - Información de Inteligencia de Fuentes Abiertas (OSINT [135]) y datos de las LEAs que describen actividades sospechosas.
  - Segregación y manejo de distintos casos de investigación.
- El **Módulo de Razonamiento Semántico Avanzado** (Advanced Semantic Reasoning) se compone de varias herramientas y mecanismos diseñados para facilitar la fusión de información y el razonamiento semántico, utilizando los datos de las Bases de Conocimiento (Knowledge Bases). Este módulo incluye:
- **Procesamiento Semántico de Información** (Semantic Information Processing): Herramienta que permite al sistema manejar y procesar el conocimiento de manera estructurada y formalizada.
  - **Fusión de Información de Alto Nivel** (High-Level Information Fusion): Emplea modelos basados en grafos para representar eficazmente la información y el conocimiento semántico.
  - **Descubrimiento Avanzado de Evidencias y Análisis de Tendencias** (Advanced Evidence Discovery & Trends Analysis): Aplica

técnicas de correlación y aprendizaje automático para proporcionar a los usuarios herramientas avanzadas para el análisis de datos heterogéneos.

La información y resultados generados por estos procesos se almacenan en las Bases de Conocimiento para su uso y análisis posteriores.

- La Inteligencia Aumentada de MAGNETO (MAGNETO Augmented Intelligence) incluye una serie de herramientas y HMIs para asistir a los usuarios en el manejo de datos y situaciones. Este módulo está compuesto de los siguientes elementos:
  - **Conciencia Operativa y Situacional** (Operational & Situational Awareness): Proporciona a los operadores de las LEAs herramientas para representar y visualizar la evolución de los eventos.
  - **Análisis Visual** (Visual Analytics): Ofrece métodos analíticos para garantizar una interfaz de usuario accesible y fácil de usar.
  - **Herramientas de Pruebas Legales de Evidencia** (Court-proof Evidence toolkit): Asegura que todos los hechos y conclusiones sean válidos y aceptables en un entorno judicial.

Funcionalmente, estos módulos están interconectados y se estructuran siguiendo un modelo arquitectónico N-tier clásico, que comprende:

- **Capa de Datos:** En la base del modelo arquitectónico N-tier de MAGNETO, incluye el componente de Minería de Datos Heterogéneos y Recopilación de Evidencias, junto con interfaces comunes que facilitan el acceso a los datos.
- **Capa de Lógica Empresarial:** Representada por el componente de Razonamiento Semántico Avanzado.
- **Capa de Presentación:** Donde se encuentran las capacidades de la Inteligencia Aumentada, compuesta por módulos dedicados que proporcionan las funcionalidades específicas del componente.

Además, la plataforma MAGNETO incorpora componentes adicionales que mejoran sus capacidades funcionales. Entre ellos, se encuentran:

- **Interfaces Comunes** (Common Interfaces): componente clave que facilita la integración de fuentes de datos externas. Una vez que se ha establecido el acceso, estas fuentes se incorporan sin problemas al sistema, mejorando la interoperabilidad de la plataforma MAGNETO con otros sistemas existentes.

- **Herramientas de Administración** (Admin Tools): ofrece un conjunto de herramientas esenciales para la operación del sistema. Entre estas herramientas se destacan:
  - **Roles de Usuario y Derechos de Acceso y Autorización** (User Roles & Access Rights & Authorisation): Estos elementos forman parte del sistema de seguridad y se implementan globalmente para asegurar un funcionamiento coherente del sistema.
  - **Técnicas de Seguridad** (Security): Incluyen el uso de firmas y cifrado de mensajes para proteger la confidencialidad de los datos.
  - **Manejo de Ataques Externos**: El sistema de seguridad aborda ataques como Denegación de Servicio (DDoS), Hombre en el Medio (MITM), Puertas Traseras, etc., y contará con un sistema de detección de intrusos.
  - **Ética y Privacidad** (Ethics & Privacy): Esta herramienta se encarga de la anonimización de datos y personas no relevantes o involucradas, así como del control de aspectos legales específicos de los estados participantes.
  - **Control de Operaciones** (Operation Controller): La consola proporciona herramientas para la gestión general del sistema.

Conforme se detalló previamente en el Capítulo 4, la arquitectura de MAGNETO adopta un enfoque basado en microservicios, como se muestra en la Figura 4.3. Esta estrategia se seleccionó con el objetivo de mantener un alto nivel de descomposición y modularidad de los servicios. Al hacerlo, se facilita significativamente el desarrollo y la integración de diversos componentes y módulos. Cada microservicio funciona de manera independiente, pero al mismo tiempo, está diseñado para integrarse de manera eficiente dentro del ecosistema más amplio de MAGNETO.

Este enfoque modular no solo mejora la flexibilidad y la escalabilidad del sistema, sino que también permite una colaboración más efectiva entre diferentes equipos y colaboradores. Al dividir el sistema en servicios más pequeños y manejables, se reduce la complejidad inherente al desarrollo de una plataforma tan avanzada como MAGNETO. Además, esta estructura facilita la actualización y el mantenimiento continuo del sistema, permitiendo a los desarrolladores implementar y probar cambios en un servicio específico sin afectar el funcionamiento global de la plataforma.

La división de una aplicación en una serie de servicios independientes conlleva la necesidad de establecer una comunicación efectiva entre ellos para brindar funcionalidades avanzadas y sofisticadas. Esto generalmente implica combinar



### 4.3 Arquitectura de MAGNETO

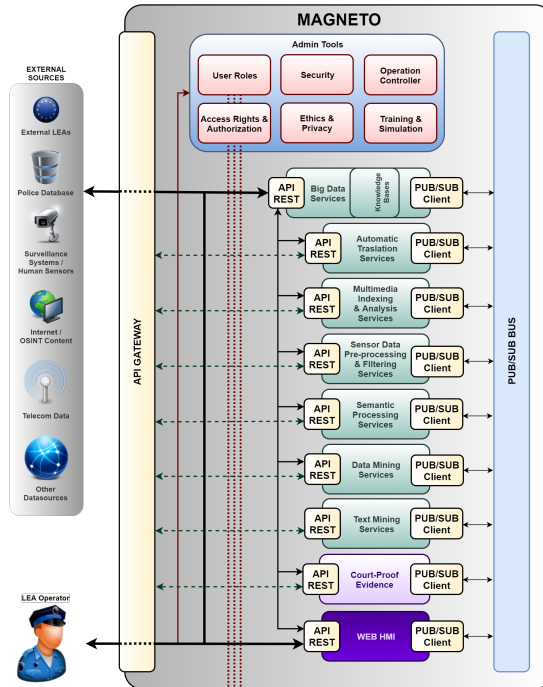


Figura 4.3: Arquitectura MAGNETO basada en microservicios

resultados de múltiples servicios, lo que puede presentar ciertas dificultades dependiendo de la aplicación específica. En algunos escenarios, se hace necesario implementar mecanismos de orquestación para obtener los resultados deseados. La orquestación se refiere a la secuencia de acciones necesarias para producir el resultado final, las cuales deben ser coordinadas temporalmente.

Por este motivo es crucial contar con una API unificada y coherente para acceder al sistema. Por ello, se ha incorporado un patrón de agregación conocido como API Gateway, un concepto ampliamente utilizado en múltiples frameworks y soluciones de microservicios, y que funciona como un proxy inverso.

Desde la implementación inicial de la arquitectura, se ha adoptado la herramienta Kong API Gateway por varias razones:

- Es uno de los API Gateways de código abierto más utilizados
- El sistema se percibe como una única aplicación monolítica con una API coherente.

- Gracias a su arquitectura basada en plugins, ofrece facilidad de extensión y adaptación del portafolio de funcionalidades según las necesidades del usuario. Actualmente, tiene más de 300 plugin divididos en cuatro categorías: Autenticación, Control de Tráfico, Transformaciones y Registro.
- Permite implementar funciones específicas en la propia puerta de enlace, como la autenticación y autorización.
- Capacidad de escalado. Cada servidor no tiene estado, lo que significa que se puede agregar o quitar tantos nodos como sea necesario bajo el balanceador de carga.

Además, la comunicación entre los diversos servicios de la plataforma se realizará de manera asíncrona, utilizando un bus de publicación y suscripción, concretamente con el *Broker* de mensajería RabbitMQ.

A continuación, se describirá cada uno de los servicios de microservicios en detalle, destacando su función específica y cómo contribuyen al conjunto total de la arquitectura de MAGNETO.

### 4.3.1. Servicios Big Data

El módulo de Servicios de BD también nombrados como *MAGNETO Big Data Framework* (MBDF) abarca las operaciones de almacenamiento, accesibilidad e interoperabilidad, procesado y gestión de los datos.

Con el fin de lograr las operaciones planteadas, El MBDF incorpora una variedad de componentes de software de código abierto. Cada uno de estos componentes estará encargado de realizar tareas específicas y, al trabajar en conjunto, contribuirán a la prestación de servicios dentro de la plataforma MAGNETO.

Los principales componentes para el almacenamiento de datos son los siguientes:

Componente	Función
HDFS	Almacenamiento archivos multimedia
MongoDB	Knowledge Database
ElasticSearch	Almacenamiento de Logs
Cassandra	Knowledge Database
Apache Jena	Semantic Database

**Tabla 4.1:** Componentes del MBDF y sus Implementaciones

Como se expuso en el Capítulo 4 el elemento central de este módulo es el DB Manager. Es el encargado de orquestar la ingestión de datos a la plataforma MAGNETO.

El DB-Manager utiliza un cliente RabbitMQ que está suscrito a una serie de **topics** para manejar operaciones CRUD. Para realizar estas operaciones, las distintas herramientas que quieren almacenar los datos tienen que crear un mensaje JSON y publicarlo en el *Broker* de RabbitMQ. Cuando el DB-Manager recibe un mensaje, identifica qué operación se debe realizar y cuál motor de base de datos debe ejecutarla. Se crea una consulta específica para ese motor y se lanza a través de su API correspondiente. Después de recibir la respuesta del motor de base de datos, el DB-Manager prepara un mensaje con esta respuesta y lo envía de vuelta al servicio que originó la consulta.

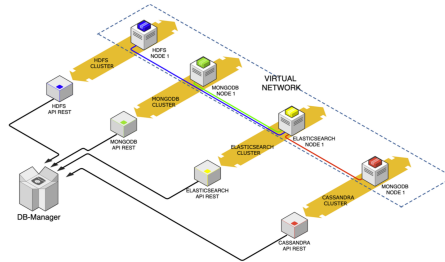


Figura 4.4: Orquestación Bases de datos

Cada uno de los componentes ha sido virtualizado y se encuentran dentro de una red virtual a la que solo tiene acceso el DB-Manager, proporcionando así un nivel de seguridad adicional.

## HDFS

Aunque HDFS es un sistema de archivos distribuido y no una base de datos en el sentido estricto, lo consideraremos como tal debido a su función de almacenamiento de información. En el contexto de las pruebas y demostraciones llevadas a cabo, se configuró una única instancia de HDFS en una máquina virtual. Esta configuración permite la posibilidad de replicar la máquina para crear un clúster de instancias HDFS, proporcionando a la plataforma escalabilidad, redundancia y tolerancia a fallos.

La máquina se configuró partiendo de una instalación limpia de Ubuntu Server 18.04 [136], sobre la cual se instalaron los paquetes necesarios para ejecutar los servicios del sistema de archivos distribuido de Hadoop. Además, para facilitar el acceso al servicio desde el DB-Manager, se habilitó WebHDFS

## CAPÍTULO 4. CASO 1: MAGNETO

---

[137], una API REST que permite efectuar una amplia gama de operaciones en HDFS mediante llamadas REST estándar (GET, PUT, POST y DELETE).

Operación HTTP	Acción
GET	OPEN, GETFILESTATUS, LISTSTATUS, GETCONTENTSUMMARY, GETFILECHECKSUM, GETHOMEDIRECTORY, GETDELEGATIONTOKEN
PUT	CREATE, MKDIRS, RENAME, SETREPLICATION, SETOWNER, SETPERMISSION, SETTIMES, RENEWDELEGATIONTOKEN, CANCELDELEGATIONTOKEN
POST	APPEND
DELETE	DELETE

**Tabla 4.2:** Operaciones HTTP y sus Acciones

### MongoDB

Similar a HDFS, MongoDB también soporta configuraciones tanto de instancia única como en *Cluster*, proporcionando escalabilidad, redundancia y tolerancia a fallos.

La configuración de la máquina se realizó desde cero, utilizando una instalación limpia de Ubuntu Server 18.04, sobre la cual se instalaron los paquetes necesarios para poner en marcha los servicios de MongoDB. Además, en la misma máquina se configuró una API REST basada en Node.js (mongodbr-rest), facilitando al módulo DB-Manager la realización de operaciones sobre MongoDB mediante peticiones HTTP de manera eficiente y sencilla.

### Cassandra

Al igual que con otros motores ya mencionados, Cassandra también admite implementaciones tanto en modo de instancia única como en configuración de *Cluster*, ofreciendo mejoras significativas en términos de rendimiento, escalabilidad, redundancia y tolerancia a fallos para despliegues en entornos de producción.

Para este componente también se ha realizado una instalación desde cero utilizando Ubuntu Server 18.04 y se ha instalado todo lo necesario para activar los servicios del motor de Cassandra.

Adicionalmente, en esta misma máquina se ha instalado y configurado una API REST basada en Python [138], denominada CassandraRestfulAPI [139],

Operación HTTP	Formato
<b>GET</b>	
Listar Bases de Datos	GET /dbs
Listar Colecciones	GET /<db>
Listar Documentos	GET /<db>/<collection>
Salida CSV de Colección	GET /<db>/<collection>?output=csv
Consulta de Documentos	GET /<db>/<collection>?query={key:value}
Retornar Documento por ID	GET /<db>/<collection>/id
<b>POST</b>	
Insertar Documentos	POST /<db>/<collection>
<b>PUT</b>	
Actualizar Documento	PUT /<db>/<collection>/id
<b>DELETE</b>	
Eliminar Documento por ID	DELETE /<db>/<collection>/id

**Tabla 4.3:** Operaciones HTTP y sus Formatos

que facilitará al módulo DB-Manager la ejecución de diversas operaciones sobre Cassandra de manera eficiente y sencilla, a través de peticiones HTTP específicas.

#### ElasticSearch

Como en el caso de HDFS, Elasticsearch [140] no es una base de datos en el sentido estricto. Como se mencionó en el estado del arte, su principal función es la indexación de elementos almacenados en bases de datos de terceros, mejorando así la eficiencia de las búsquedas.

Elasticsearch ofrece configuraciones tanto en modo de instancia única como en modo *Cluster*. Al igual que los demás componentes mencionados, su instalación fue desde cero en una máquina Ubuntu Server 18.04 y se instalaron los componentes necesarios para el motor de ElasticSearch.

Además, Elasticsearch está equipado con numerosos conectores para bases de datos. Conforme a la Figura 4.4, la plataforma se ha configurado para que los tres sistemas de almacenamiento principales (HDFS, MongoDB y Cassandra) estén conectados al nodo de Elasticsearch. De esta manera, cualquier información introducida en la plataforma se indexará automáticamente, facilitando búsquedas futuras.

También se ha habilitado la API REST de Elasticsearch en el nodo, lo que permite al módulo DB-Manager realizar diversas operaciones sobre Elasticsearch de forma sencilla mediante peticiones HTTP específicas.

## CAPÍTULO 4. CASO 1: MAGNETO

---

Categoría	Formato
<b>NODES</b>	
Listar	GET /nodes
Información	GET /nodes/:id
Crear	POST /nodes
Eliminar	DELETE /nodes/:id
<b>KEYSPACES</b>	
Listar	GET /keyspaces
Información	GET /keyspaces/:id
Crear	POST /keyspaces/
Actualizar	PUT /keyspaces/:id
Eliminar	DELETE /keyspaces/:id
<b>COL. FAM</b>	
Listar	GET /keyspace/:id/columnfamilys/
Información	GET /keyspace/:id/columnfamilys/:id
Crear	POST /keyspace/:id/columnfamilys/
Eliminar	DELETE /keyspace/:id/columnfamilys/:id
<b>ENTRIES</b>	
Listar	GET /keyspace/:id/columnfamilys/:id/entrys/
Información	GET /keyspace/:id/columnfamilys/:id/entrys/:name
Crear	POST /keyspace/:id/columnfamilys/:id/entrys/
Eliminar	DELETE /keyspace/:id/columnfamilys/:id/entrys/:name

**Tabla 4.4:** Operaciones API y sus Formatos

### 4.3.2. Servicios de Traducción Automática

Se utiliza para identificar los documentos que deben ser incluidos en el análisis semántico, por lo que el objetivo principal de este módulo es traducir aquellos documentos que utilicen un lenguaje diferente al inglés, que es el lenguaje en el que opera MAGNETO.

Debido a que hay varios LEAs en el proyecto cuyo lenguaje son el alemán, italiano, polaco o catalán, este módulo debe soportar la traducción a estos idiomas. En algunos casos será una traducción directa y en algunos casos se debe hacer una doble traducción, como es el caso del lenguaje catalán, el cual primeramente se traduce al castellano y luego al catalán.

Con todo ello y dado que el módulo de traducción automática debe funcionar en local y debe trabajar con un número limitado de documentos paralelos de entrenamiento, se diseñó la siguiente arquitectura:

### 4.3 Arquitectura de MAGNETO

Categoría	Acción y Formato
<b>DOCUMENTS</b>	
Recuperar	GET /my_index/my_type/0?pretty
Añadir/Actualizar	PUT /my_index/my_type/1?pretty
Eliminar	DELETE /my_index/my_type/0?pretty
Copiar	POST /_reindex?pretty
<b>SEARCH</b>	
Consulta de Búsqueda	GET /my_index/my_type/_search?q=field:value&pretty
Contar Coincidencias	GET /my_index/my_type/_count?q=field:value&pretty
Validar Consulta	GET /my_index/my_type/_validate
Calcular Puntaje	GET /my_index/my_type/0/_explain
<b>INDICES</b>	
Crear	PUT /my_index?pretty
Eliminar	DELETE /my_index?pretty
Cerrar/Abrir	POST /my_index/_close?pretty
<b>CAT</b>	
Acceso a Información	GET /_cat/indices?v&health=red&pretty
Vista General Índices	GET /_cat/health?v&pretty
Información Nodos	GET /_cat/nodes?v&pretty
<b>Cluster</b>	
Salud del Cluster	GET /_cluster/health?pretty
Informe Detallado	GET /_cluster/state_cluster
Métricas Índices	GET _cluster/stats?my_node&pretty

Tabla 4.5: Operaciones y Formatos en Elasticsearch

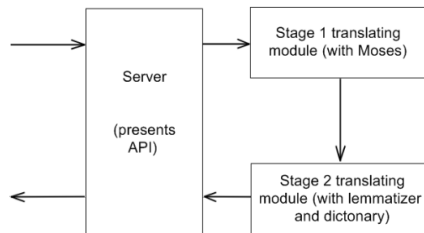


Figura 4.5: Arquitectura módulo Traducción Automática

#### 1. Servidor con Moses:

El primer módulo opera con Python3 y emplea el sistema de traducción Moses 4.0 [141]. Los datos de entrada para este componente provienen directamente de la API. Tras el proceso de traducción, es posible que el texto resultante incluya términos sin traducir, y la cantidad de estos

depende de la efectividad del modelo que ha sido previamente entrenado. A pesar de ello, no hay garantía por parte de Moses de que todas las palabras sean traducidas, incluso si forman parte del conjunto de datos utilizado para el entrenamiento.

### 2. Servidor con la traducción adicional + lematizador y diccionarios:

Este subsistema se encarga de mejorar la traducción obtenida en la etapa anterior y proporcionar una salida más precisa y coherente. Utiliza Python3 como lenguaje, la librería Treetagger [142] para lematización, la librería *Natural Language Toolkit* (NLTK) [143] para etiquetado de texto y un vocabulario preentrenado.

Así, el texto parcialmente traducido entra en esta segunda etapa y se inicia con el lematizador, que convierte todas las palabras del texto a su forma base o lema. Posteriormente, estas formas lematizadas se cotejan con un diccionario. En caso de encontrar correspondencias en el diccionario, las palabras son traducidas. Este método logra disminuir de manera notable la cantidad de palabras que quedan sin traducir en el texto. Además, el segundo subsistema ofrece la posibilidad de incorporar una variedad de diccionarios adicionales, siendo crucial añadir aquellos que pertenecen al contexto de delitos y crímenes.

### 4.3.3. Servicios de Indexado y Filtrado Multimedia

Tras su almacenamiento en el módulo MAGNETO BD *Framework*, los archivos multimedia son sometidos a un proceso de extracción de características relevantes. Este procedimiento se realiza utilizando el módulo de Indexación y Filtrado Multimedia, que se bifurca en dos arquitecturas especializadas según la naturaleza del archivo, diferenciando entre formatos de vídeo y audio.

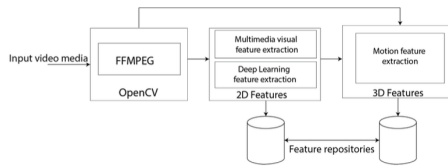
En el caso de procesado de vídeo se utiliza la librería OpenCV [144] para manejar formato de vídeo heterogéneos a través del uso de la librería integrada FFMPEG [145]. Como se puede ver en la Figura 4.6 se integran dos categorías de componentes de extracción de características: los que se enfocan en el análisis de características puramente espaciales, conocidas como 2D, y aquellos que examinan las características espacio-temporales, referidas como 3D.

La librería dedicada a las características espaciales se encarga de identificar elementos distintivos en el dominio espacial, tales como descriptores generales, detalles locales basados en canales de color o a través de transformaciones matemáticas. Esta extracción se enriquece con el empleo de modelos avanzados de *Deep Neural Network* (DNN) [146] que capturan vectores de características



complejas y de alta dimensionalidad, los cuales son esenciales para el manejo de tareas avanzadas de procesamiento de vídeo.

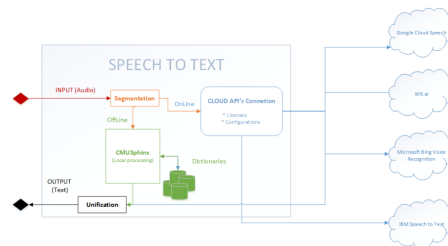
Por otro lado, la incorporación de elementos temporales mediante características de movimiento permite una evaluación más rica, combinando el espacio y el tiempo, indispensable para el tratamiento de eventos complejos de alto nivel. Finalmente, las características identificadas son catalogadas e indexadas en los repositorios de MAGNETO. Estos almacenes de datos, situados dentro del HDFS, son accesibles para operaciones subsecuentes a través de servicios especializados en BD.



**Figura 4.6:** Extracción Características Vídeo

El procesamiento de audio se utiliza básicamente para transferir el audio a texto para posteriormente realizar análisis de Data Mining. Para el procesamiento de audio se pueden utilizar tanto diferentes APIs de proveedores *CLOUD* Speech-Text, como Google [147], Wit [148], Microsoft [149] and IBM [150] si se ejecuta en un entorno conectado a internet o el motor CMU Sphinx [151] para cubrir los casos donde la conexión a internet no está permitida o debido a la confidencialidad de los datos que se trata en casos policiales.

Se ha seleccionado Python como lenguaje de programación para el desarrollo debido a su amplio repertorio de bibliotecas especializadas en el procesamiento de archivos de audio, que facilitan la realización de tareas requeridas de manera eficiente.



**Figura 4.7:** Esquema Speech-to-Text

Como se observa en la Figura 4.7, el primer paso es dividir un archivo de audio en frases distintas. Utilizando la biblioteca `pyAudioAnalysis` [152], el módulo de segmentación aprovecha las herramientas ofrecidas para la extracción, clasificación y división de los archivos de audio. Se llevaron a cabo múltiples pruebas para detectar pausas y ajustar los parámetros de segmentación hasta lograr una división precisa de las frases.

Posteriormente, los fragmentos resultantes del audio se procesan utilizando servicios en el *CLOUD* o localmente con ayuda de la biblioteca `pocketsphinx`, la cual se basa en el motor CMU Sphinx para la transcripción del audio. Tras la transcripción de todos los segmentos, estos se consolidan para formar un texto completo, el cual se entrega como resultado final. El texto resultante se guarda en base de datos para posteriores análisis.

### 4.3.4. Servicios de Procesamiento Semántico

El Servicio de Razonamiento de *Markov Logic Network* (MLN) [153] es una herramienta avanzada que ayuda a comprender y predecir el comportamiento en situaciones inciertas. Funciona estableciendo reglas en colaboración con los LEAs. Este servicio mejora la información de la que ya se dispone y descubre conexiones y hechos nuevos al analizar diferentes objetos y datos [154].

MLN utiliza probabilidad y lógica avanzada para hacer suposiciones educadas sobre cosas de las que no se está completamente seguro. Se utiliza la versión *Tuffy* [155] para el razonamiento de MLN, dada su capacidad para escalar.

Para lograr el funcionamiento de Tuffy, es necesario que primero adquiera conocimientos provenientes de una base de datos especializada en ***Resource Description Framework (RDF) Triple Store Fuseki*** [156]. Posteriormente, se procede a convertir la información a un formato comprensible por Tuffy, concretamente mediante modelado *Ontology Web Language (OWL)* [157], utilizando una herramienta conocida como Incerto.

En la etapa final, una vez que se transforma el modelo, se preparara para ser utilizado por el razonador Tuffy. Para hacerlo, se crean archivos separados para las evidencias de probabilidad y las fórmulas ponderadas, y las fórmulas se representan de una manera específica. Luego, Tuffy realiza el razonamiento y nos devuelve los resultados en un formato llamado Lógica de Primer Orden. Estos resultados se almacenan de nuevo en RDF Triple Store FUSEKI. En resumen, esta etapa nos permite ajustar el modelo y adaptarlo para que Tuffy pueda trabajar con él, y luego almacenamos los resultados en un sistema adecuado para su posterior uso.

Las reglas para la generación de nuevo conocimiento se desarrollarán en colaboración con las LEAs, y se espera que den como resultado un conjunto

estándar aplicable en varios contextos, así como conjuntos específicos adaptados a casos de investigación particulares.

### 4.3.5. Servicios de minería de Texto y Datos

La finalidad del módulo de minería de texto en MAGNETO es ofrecer métodos y algoritmos que permitan extraer información valiosa de textos. Esta información luego se integra en la base de conocimientos de MAGNETO. Para lograr esto, se realiza primero un análisis lingüístico detallado de los datos textuales, seguido de la interpretación del significado de las palabras dentro del contexto en que se encuentran. Estos análisis se fundamentan en marcos teóricos de NLP, tanto en el enfoque basado en reglas como en el enfoque estadístico, este último empleando algoritmos de ML o, más recientemente, técnicas DNN [134].

El mapeo del conocimiento extraído que representa un modelo lingüístico del idioma con el dominio específico de MAGNETO, enfocado en el ámbito de la aplicación de la ley, básicamente consiste en relacionar los roles semánticos (como sujeto, objeto, tiempo o ubicación) con la clase “*Evento*” de la ontología MAGNETO, asignando las coincidencias adecuadas:

- Para una instancia de ‘**Evento**Categoría’, la categoría del evento se construye a partir del predicado (verbo) mediante la consulta del verbo en las listas de *Event and Situation Ontology* (ESO)[158] y *Suggested Upper Merged Ontology* (SUMO)[159] y una lista específica de MAGNETO. Si el verbo se encuentra en alguna de estas listas, se convierte en un candidato para la categoría del evento y se mapea a una categoría apropiada modelada en la ontología.
- Por ejemplo, una ‘**Persona**’ con la relación ‘*involucraPersona*’ derivada de una posición de sujeto o un rol de agente,
- Por ejemplo, una ‘**Persona**’ con la relación ‘*involucraPersona*’ derivada de una posición de sujeto o un rol de agente,
- Un intervalo de tiempo para las relaciones ‘*tieneHoraInicioEvento*’ y ‘*tieneHoraFinEvento*’, y una instancia de ‘**Lugar**’ con la relación ‘*tieneUbicaciónEvento*’,
- Y un ‘**Recurso**’ para vincular el evento con el documento correspondiente.

El servicio utiliza la *Uniform Resource Locator* (URL) [160] del almacén FUSEKI para acceder a las instancias creadas que se almacenan allí. Para

## CAPÍTULO 4. CASO 1: MAGNETO

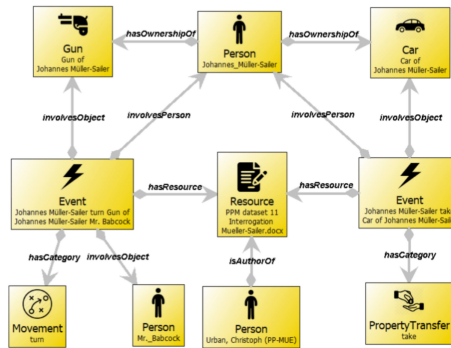


Figura 4.8: Ejemplo de Text Mining - Interrogatorio Sospechoso

mantener un registro claro y permitir su uso como prueba en procedimientos legales, todas las instancias de conceptos generadas se vinculan al documento original de texto. Se ha desarrollado un adaptador específico para manejar declaraciones de testigos proporcionadas en un caso de homicidio. Estas declaraciones, que originalmente se encontraban en formato de documentos Microsoft Word[161] han sido exportadas para su procesamiento. El desafío del modelo es identificar y referenciar a personas específicas, en lugar de usar pronombres personales genéricos.

Por consiguiente, es necesario llevar a cabo un análisis y procesamiento detallado de las declaraciones de testigos. Una particularidad de estas declaraciones es que están redactadas en primera persona, lo que requiere una extracción y procesamiento cuidadosos del conocimiento para su integración en el CRM.

El *Framework Apache Tika*[162] se emplea para leer los documentos, obtener los metadatos y extraer el texto en formato simple. Es esencial identificar el nombre del testigo y vincularlo con la declaración correspondiente. Tras determinar el idioma del documento, se utiliza un servicio de traducción para convertir el texto al inglés. Posteriormente, se reemplazan todos los pronombres por el nombre del testigo para mantener la claridad y consistencia. Este proceso también se aplica a los interrogatorios de los sospechosos.

Además de enriquecer la información y profundizar en el contexto de una IC, el módulo tiene la capacidad de procesar conjuntos de datos en formato Microsoft Excel[163], como, por ejemplo, los registros de viviendas. Este proceso implica la identificación y creación de instancias de conceptos tales como personas, lugares y direcciones, estableciendo vínculos entre ellos. El servicio utiliza como entrada un archivo de Excel que contiene las siguientes colum-

## 4.3 Arquitectura de MAGNETO

nas: Apellido, Nombre, Fecha de Nacimiento, Código Postal, Ciudad, Calle y Número.

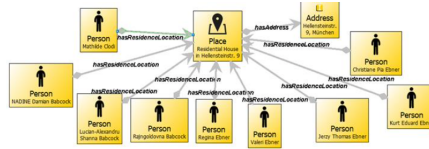


Figura 4.9: Ejemplo salida Text Mining - Registro viviendas

### 4.3.6. Inteligencia Aumentada

Uno de los principales objetivos del proyecto MAGNETO es **“Desarrollar HMIs orientadas al usuario que aumenten la Conciencia Situacional y la Capacidad Operativa de los Agentes”**.

La Figura 4.10 muestra cómo integra MAGNETO las tareas de Inteligencia Aumentada, este módulo cubre dos tipos de interfaces:

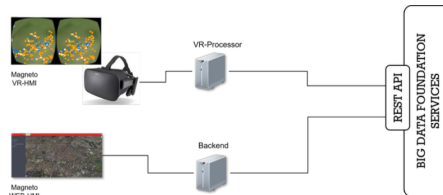


Figura 4.10: Esquema Inteligencia Aumentada MAGNETO

### VR-HMI

La solución VR-HMI aprovecha la tecnología de realidad virtual a través de las gafas Oculus Rift [164] y el sistema GIS de Luciad [165]. Este prototipo se conecta con los Servicios Fundamentales de BD de MAGNETO mediante su API, procesando información georreferenciada almacenada en la plataforma. El VR-Processor adapta estos datos para su visualización inmersiva, la cual es presentada a través de las gafas Oculus Rift. Su principal misión es visualizar elementos georreferenciados sobre un mapa utilizando la herramienta Luciad.

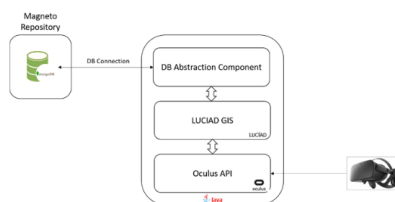


Figura 4.11: Esquema Módulo de VR

### WEB-GIS

El Web-GIS es una herramienta dedicada a la visualización de recursos geospaciales provenientes de diferentes servicios. Específicamente, se utilizará una visualización en 3D que ofrece varias capas. El objetivo del de Web-GIS es el mismo que el del VR-HMI. Se pretende representar información geolocalizada vinculada a incidentes registrados en la base de datos policial.

La arquitectura utilizada para el desarrollo del prototipo se divide en dos componentes principales: el **Frontend**, que es la interfaz de usuario, y el **Backend**, que comprende la lógica y la gestión de datos. Este desarrollo se ha llevado a cabo empleando un *Framework* de JavaScript conocido como *VueJS* [166], seleccionado por varias razones:

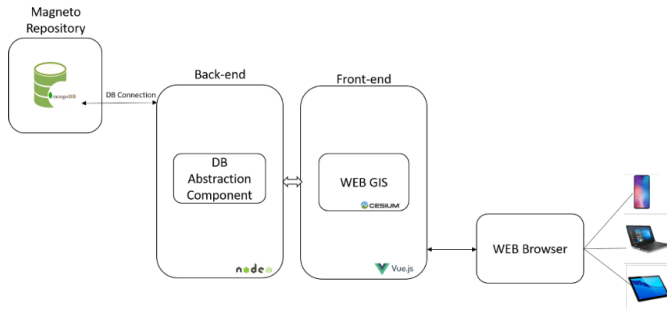
- Integración fluida de componentes (*Framework* progresivo).
- Comunidad de código abierto amplia y activa.
- Características intuitivas, modernas y fáciles de usar.
- Facilidad de aprendizaje para el desarrollo e integración de componentes.

Es relevante mencionar que una distinción entre el VR-HMI y el WEB-GIS reside en el GIS utilizado. Mientras que el VR-HMI emplea visualización inmersiva con LUCIAD, para el prototipo II se ha optado por la biblioteca JavaScript Cesium.

El flujo de datos se gestiona de la siguiente manera:

- **Frontend**: Se conecta al *Backend* a través de la biblioteca Axios. [167]
- **Backend**: Utiliza *ExpressJS* [168], un *Framework* de aplicaciones web para NodeJS [169], para manejar las solicitudes. Se conecta a la base de datos MongoDB mediante Mongoose, con la base de datos alojada en un repositorio de MAGNETO.

Como se muestra en la Figura 4.12



**Figura 4.12:** Esquema Módulo Web-GIS

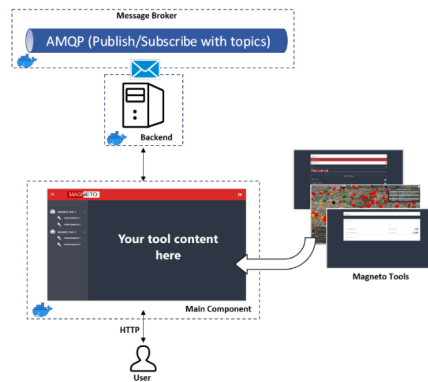
### WEB-HMI

Esta solución web se basa en NodeJS y VueJS. Ofrece una interfaz de usuario unificada para que las LEAs accedan e interactúen con los datos y servicios de MAGNETO. Se busca centralizar todas las interacciones con la plataforma en un solo punto, donde se visualizan los resultados de los análisis realizados, incluyendo la fusión de datos, procesamiento multimedia y extracción semántica. Este módulo también facilita la capacitación de las LEAs al requerir entrenamiento en una sola herramienta en vez de múltiples interfaces.

Como se ilustra en la Figura 4.13 los componentes clave de la arquitectura, específicamente el *Frontend* y el *Backend*, se han contenerizado usando Docker, tal como se describió en el Capítulo 4. La interacción entre el *Frontend* y el *Backend* se establece de manera direccionada y puede ser en tiempo real, empleando Web Sockets. Para ello, se utiliza la biblioteca Socket.IO [170], que facilita una comunicación fluida y eficiente. Alternativamente, las interacciones también pueden ser manejadas mediante peticiones CRUD, utilizando el *Framework* Express.js.

En esta arquitectura, el *Backend* actúa como un nexo central entre el *Frontend* y el resto de herramientas y servicios de la plataforma. Esta conexión se gestiona mediante un sistema de publicación y suscripción en los distintos topics definidos dentro del *Message Broker*, asegurando así un flujo de datos coherente y organizado entre los diferentes componentes del sistema.

En el *Frontend*, se dispone un área de visualización para cada una de las herramientas y funciones desarrolladas por los socios técnicos. Las herramientas tendrán servicios internos que también deben ser contenerizados. Además, el *Backend* estará conectado a los diferentes servicios y herramientas desarrolladas.



**Figura 4.13:** Esquema Integración Servicios WEB HMI

### Mejora Háptica con LEAP Motion

Integración del sensor LEAP Motion [171] en conjunto con el WEB-GIS para brindar una experiencia de realidad virtual aún más inmersiva. Esta integración se ha realizado mediante la librería Cesium Leap, que permite leer los gestos captados por el Leap Motion e interactuar con la API de cámara de Cesium y así, extrapolarlos a movimientos espaciales sobre el mapa.

Gracias a esta tecnología, los LEAs pueden interactuar con el mapa de una manera mucho más natural e intuitiva, utilizando simplemente los movimientos de sus manos. Las funcionalidades implementadas incluyen la capacidad de mover el mapa, realizar zoom, desplazarse por diferentes áreas, e incluso hacer *Click* en puntos específicos, todo ello mediante gestos manuales. Esta interacción directa y mejorada representa una novedad en la forma en que los LEAs interactúan con los datos geoespaciales.

### 4.3.7. Herramientas de Administración

Este módulo ofrece una serie de herramientas esenciales para el correcto funcionamiento y asegurar la seguridad de la plataforma de MAGNETO.

### Servicio de Autenticación y Autorización

Componente esencial que garantiza la integridad y la protección de los datos y operaciones dentro del sistema. Este servicio no solo establece la primera línea de defensa contra accesos no autorizados, sino que también asegura que cada usuario tenga los permisos adecuados para realizar acciones específicas.



Juega un papel crucial en el mantenimiento de la confianza y la seguridad en un entorno donde se manejan datos sensibles y críticos para la seguridad. Al implementar mecanismos de autenticación robustos y políticas de autorización detalladas, MAGNETO puede ofrecer un entorno seguro y controlado, fundamental para operaciones efectivas y confiables en el ámbito del análisis y la gestión de información en contextos de seguridad y emergencia.

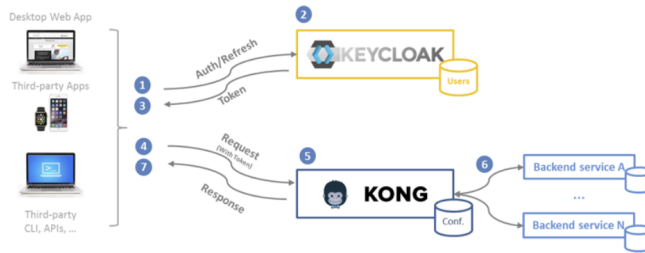
La interacción entre el entorno externo y los servicios internos de la plataforma MAGNETO se facilita mediante el API Gateway. En nuestra arquitectura, las funcionalidades de *Autenticación y Autorización* (AA) se centran en torno a Keycloak, un sistema de Gestión de Identidad y Acceso de código abierto. Keycloak [172] ofrece una variedad de mecanismos para garantizar la seguridad en un extenso espectro de servicios y aplicaciones *Backend*, proporcionando una capa robusta y confiable de protección de identidades.

Existen varios escenarios para adaptar este servicio [154]:

- Cuando un cliente no autenticado intenta ingresar, se le redirige inicialmente a la página de inicio de sesión de Keycloak. Una vez completado el inicio de sesión con éxito, el cliente es reconducido a la aplicación original, portando un token de seguridad. En este contexto, la responsabilidad de la aplicación *Backend* se limita a verificar la validez de dicho token.
- En el caso de que un servicio interno de MAGNETO necesite realizar una llamada a la API de otro servicio que exige autenticación, dicho servicio interno almacena de forma segura las credenciales asociadas a sí mismo (y no a un usuario), autenticándose a través de un canal HTTP(S).
- Por otro lado, si un servicio interno de MAGNETO requiere utilizar las credenciales del usuario para realizar llamadas a la API de otros servicios, la autorización recae en Keycloak. Tras una autorización exitosa, se entrega un token de seguridad que el servicio utiliza para interactuar con otros servicios en representación del usuario.

En la 4.14 se puede ver el flujo completo. La autorización llevada a cabo por Keycloak y la autenticación por parte de Kong.

1. **Autenticación del Cliente:** El cliente inicia un proceso de autenticación enviando una solicitud hacia Keycloak.
2. **Keycloak:** Funciona como el sistema de *Identity and access management* (IAM), procesando las solicitudes de autenticación y autorización. Aquí es donde se registran los usuarios.



**Figura 4.14:** Flujo Autorización y Autenticación

3. **Token de Autenticación/Refresco:** Después de una autenticación exitosa, Keycloak emite al cliente un token de seguridad que verifica la identidad del usuario.
4. **Solicitud con Token:** El cliente procede a enviar una solicitud a un servicio *Backend* a través del API Gateway de Kong, incluyendo el token de seguridad en la cabecera de la solicitud.
5. **Kong API Gateway:** Actúa como el punto de control para todas las solicitudes entrantes, donde se gestionan y aplican las configuraciones de seguridad, como la validación de tokens.
6. **Servicios Backend:** Representan los servicios finales que el cliente desea acceder. Cada servicio está configurado para procesar solicitudes específicas y llevar a cabo operaciones de negocio.
7. **Respuesta al Cliente:** Una vez que el token es validado y la solicitud es procesada por el servicio *Backend* adecuado, la respuesta es enviada de vuelta al cliente a través de Kong.

### 4.4. Logros de MAGNETO

MAGNETO, concebida como una solución innovadora en el campo de la seguridad y aplicación de la ley, representa una plataforma integral cuyo diseño se enfoca en la optimización y eficiencia en la gestión de información y comunicaciones. Esta plataforma se destaca por su capacidad de integrar y procesar datos provenientes de una amplia gama de fuentes, incluyendo sensores, bases de datos y sistemas de comunicación, lo que permite a las LEAs acceder a información vital de manera rápida y coordinada. La funcionalidad de

MAGNETO abarca desde la recopilación de datos en tiempo real hasta el análisis avanzado de estos, facilitando la toma de decisiones críticas y la respuesta rápida en situaciones de emergencia. Algunos de los logros más significativos de MAGNETO incluyen:

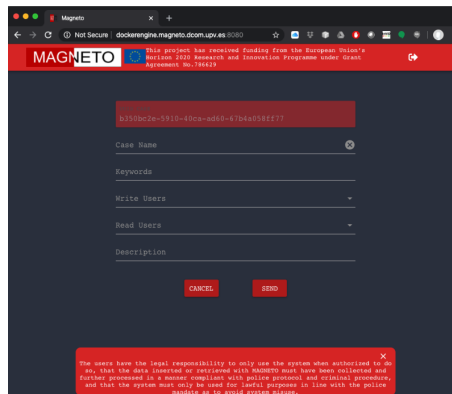
1. **Centralización de datos para análisis eficiente:** La implementación del CRM abierto en MAGNETO ha sido un logro clave en la consolidación de información de diversas fuentes. Este modelo permite a las agencias de seguridad y a los organismos de aplicación de la ley acceder a una visión unificada y detallada de los datos, lo que facilita la interoperabilidad entre diferentes sistemas y plataformas. Al estandarizar la forma en que se representan y procesan los datos, MAGNETO acelera significativamente la evaluación y el análisis de casos. Esta centralización de datos no solo mejora la eficiencia en el procesamiento y análisis de la información, sino que también contribuye a una mejor predicción y anticipación de tendencias futuras, fortaleciendo las capacidades de las agencias en la toma de decisiones críticas.
2. **Plataforma modular y escalable:** Uno de los logros más notables de MAGNETO en el ámbito de la seguridad y aplicación de la ley es su desarrollo como una plataforma modular y escalable. Esta característica aporta múltiples beneficios:
  - a) **Flexibilidad en la integración de módulos:** La arquitectura modular de MAGNETO permite adaptar la plataforma a diversas necesidades operativas, ofreciendo una solución personalizable y orientada al usuario.
  - b) **Capacidad de escalabilidad:** Diseñada para manejar un aumento en el volumen de datos y complejidad de operaciones, MAGNETO mantiene un alto rendimiento y eficiencia incluso bajo demandas crecientes.
  - c) **Interoperabilidad con diversas fuentes de datos:** La integración con una amplia gama de fuentes de datos y sistemas de información permite una recopilación de datos más completa, mejorando la toma de decisiones.
  - d) **Adaptabilidad a cambios y evoluciones tecnológicas:** La estructura modular y escalable facilita la actualización y la incorporación de nuevas tecnologías, manteniendo la relevancia de la plataforma.
  - e) **Soporte para colaboración y trabajo en red:** La capacidad de integrar múltiples módulos y sistemas fomenta la colaboración eficaz entre diferentes agencias y departamentos.

## CAPÍTULO 4. CASO 1: MAGNETO

---

3. **Integración de tecnologías de vanguardia:** Uso de tecnologías avanzadas como el procesamiento de lenguaje natural y el aprendizaje automático para enriquecer la toma de decisiones operativas.
4. **HMI intuitivo:** El diseño de MAGNETO está enfocado en la usabilidad, permitiendo una interacción eficiente y efectiva con la plataforma, una característica esencial en situaciones de alta presión.

La pieza fundamental de este módulo es el WEB-HMI de MAGNETO, que actúa como el principal punto de interacción con los usuarios finales. Esta interfaz está meticulosamente organizada en torno a Casos de Uso específicos, cada uno de los cuales está asociado a usuarios con roles definidos y claramente diferenciados, asegurando que cada caso sea independiente y esté adaptado a las necesidades particulares de sus usuarios. El WEB-HMI contiene todas las herramientas necesarias para realizar una amplia gama de análisis, proporcionando una visión integral del caso en cuestión. Esto permite a los usuarios no solo acceder y analizar datos detallados, sino también sintetizar esta información para sacar conclusiones fundamentadas. La personalización según los roles y las funcionalidades específicas de cada Caso de Uso garantizan que la plataforma sea tanto versátil como específica en su aplicación, asegurando que cada usuario tenga las herramientas y la información adecuadas para su función particular en la gestión y resolución de casos.



**Figura 4.15:** Creación Caso de uso

Además, incorpora robustas funciones de seguridad. Esto incluye un sofisticado control de acceso y mecanismos de cifrado y pseudo anonimización para proteger la información sensible (Figura 4.16). En este sistema, los

## 4.4 Logros de MAGNETO

usuarios necesitan ingresar claves específicas para descifrar los datos, asegurando así que solo el personal autorizado tenga acceso a la información crítica.

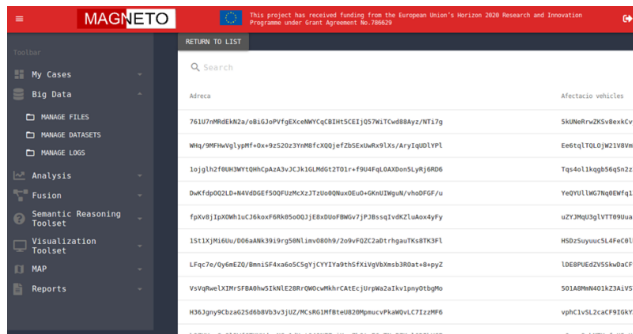


Figura 4.16: Ejemplo Dataset Cifrado

Se ha implementado un sistema avanzado para la visualización de datasets georreferenciados, como se ilustra en las imágenes siguientes. En estas, se muestra cómo un dataset (Figura 4.17) proporcionado por la Policía de Sabadell en formato Microsoft Excel es procesado, almacenado en MongoDB (Figura 4.18) y luego visualizado a través de las Oculus Rift (4.20) y el Web HMI (Figura 4.21) desarrollado específicamente para este propósito.

Month of Area (a)	Territorial Area fact	Territorial Area det	Month/Quality CAI	Month/Quality CAI	Police force, Detention	Detention date	Dispatch date (p.)	Start date, opening fact	Time from, opening fact (p.)	Start time, opening fact	Defensive time	Procedure	Type of fact (level 1)	Type of fact (level 2)
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	23/01/2019	30/01/2019	50	18:15:00	19:25:00	1	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	23/01/2019	23/01/2019	58	00:00:00	1:10:00	2	OTHERS	VARIOUS FACTS
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	24/01/2019	23/01/2019	50	20:00:00	20:25:00	3	COURT ORDER PROCEDURE	WARRANTY FACTS
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	24/01/2019	23/01/2019	50	23:25:00	—	4	COURT ORDER PROCEDURE	WARRANTY FACTS
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	24/01/2019	23/01/2019	50	18:00:00	18:34:00	5	OTHERS	VARIOUS FACTS
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	24/01/2019	23/01/2019	71	17:00:00	17:24:00	6	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	24/01/2019	24/01/2019	71	00:00:00	14:34:00	7	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	24/01/2019	24/01/2019	71	17:00:00	17:34:00	8	OTHERS	VARIOUS FACTS
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	24/01/2019	23/01/2019	72	12:00:00	13:25:00	9	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	26/01/2019	23/01/2019	74	15:00:00	15:55:00	10	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	26/01/2019	26/01/2019	75	13:45:00	14:55:00	11	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	23/01/2019	19/01/2019	77	14:30:00	12:25:00	12	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	23/01/2019	23/01/2019	78	09:00:00	10:35:00	13	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	23/01/2019	20/01/2019	79	11:30:00	10:25:00	14	OFFENSES	13. PROPERTY CRIME
January 2019	SABADELL	Sabadell	APP	APP	Sabadell	Municipal Police of Sabadell	23/01/2019	23/01/2019	79	09:00:00	10:10:00	15	OTHERS	VARIOUS FACTS

Figura 4.17: Dataset Policía Sabadell

Este dataset específico incluye varios incidentes ocurridos en la ciudad de Sabadell, clasificados por tipo, ubicación, fecha, entre otros detalles. Para facilitar su identificación, se asigna un color distinto a cada tipo de incidente. Posteriormente, la información procesada y georreferenciada se almacena en MongoDB en formato JSON, lo que permite que los diversos

## CAPÍTULO 4. CASO 1: MAGNETO

---

HMIs accedan a estos datos y los representen visualmente de manera efectiva y accesible.

Color	Tipo de Incidente
Naranja	Hechos Diversos
Rojo	Delito Contra la Propiedad
Azul	Lesiones
Blanco	Contra la Libertad Sexual
Verde	Ley 4/15 de Protección de la Seguridad Ciudadana
Rosa	Delito Contra la Intimidación
Violeta	Contra la Seguridad Vial
Negro	Otros

**Tabla 4.6:** Colores y Tipos de Incidentes

Una vez procesado, se almacena en MongoDB en formato JSON, con la información georreferenciada.

```
{
  "_id" : ObjectId("5cf8b5cb309ebe6298102867"),
  "id" : "1",
  "month_year" : "january 2018",
  "municipality" : "Sabadell",
  "date" : "01/01/2018",
  "tipus_fet" : "OFFENSE",
  "fact_type_level_0" : "13.-CRIME AGAINST PROPERTY",
  "fact_type_level_1" : "OTHERS scams",
  "type_of_road" : "polygon",
  "name_of_road" : "dels Merinals",
  "number" : "115",
  "coordinate_x_fact_point" : "424060",
  "coordinate_y_fact_point" : "4599354",
  "geometry_geo" : {
    "lat" : 41.542241460825,
    "lng" : 2.08954606352401
  }
}
```

**Figura 4.18:** JSON Dataset

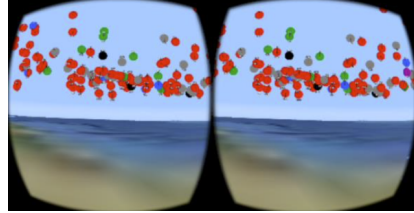
El siguiente paso es representar esta información mediante los distintos HMIs que han sido diseñados para la plataforma.

Por último, se desarrolló un prototipo para la integración de un dispositivo háptico, concretamente Leap Motion, con el GIS HMI.

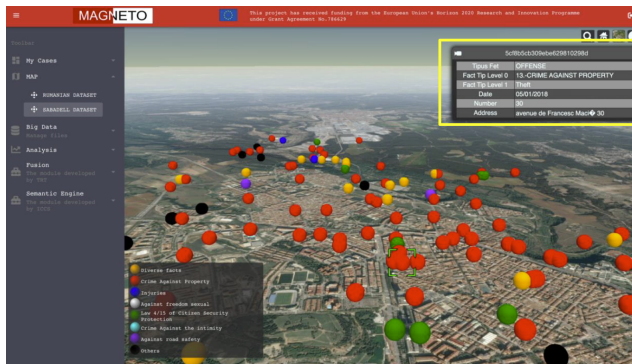
5. **Herramientas avanzadas de análisis y visualización de datos:** MAGNETO integra una gama de herramientas sofisticadas para el análisis y visualización de datos, abarcando no solo el análisis semántico de



**Figura 4.19:** Prueba Visualización VR



**Figura 4.20:** Dataset en Gafas VR



**Figura 4.21:** Dataset en GIS HMI

textos, sino también el análisis de contenido multimedia, como imágenes, vídeos y audio. Estas herramientas permiten una comprensión profunda y una interpretación precisa de una amplia variedad de datos. La capacidad de procesar y analizar diferentes formatos de datos enriquece significativamente la inteligencia y la toma de decisiones, ofreciendo una visión holística y detallada de las situaciones y casos. La visualización avanzada de estos análisis facilita la presentación de información compleja de manera intuitiva y accesible, lo que es crucial en operaciones de seguridad y emergencia.

Algunos ejemplos de estos análisis son:



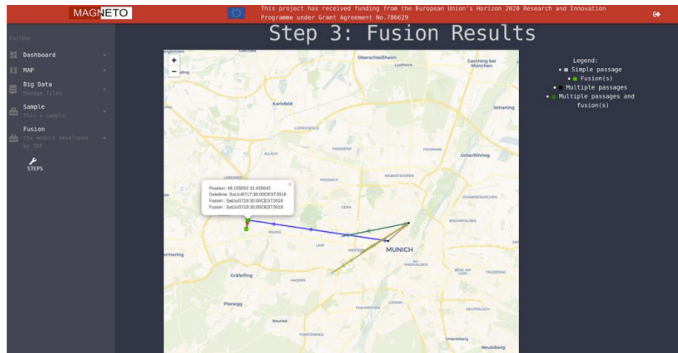
**Figura 4.22:** Prototipo Leap Motion

- **Trajectory Fusion:** Este módulo proporciona una herramienta de fusión de información semántica de alto nivel basada en datos y algoritmos de grafos.

Está diseñada para combinar y analizar información espacial proveniente de múltiples fuentes, como las localizaciones de personas a partir de registros de posicionamiento de teléfonos móviles o las ubicaciones de vehículos rastreadas a través del reconocimiento de matrículas por cámaras CCTV. El módulo procesa estos datos para calcular y fusionar las trayectorias de los diferentes elementos. Como resultado, genera un mapa detallado donde cada trayectoria se destaca con un color específico, resaltando los puntos de cruce y proporcionando información temporal asociada a estos encuentros, como se ilustra en la Figura 4.23. También puede ayudar a eliminar duplicaciones en la ontología de MAGNETO y aumentar su nivel de calidad.

- **DROP component:** El módulo *Distinctive Region or Pattern* (DROP) está diseñado para explorar extensas bases de datos de grabaciones de CCTV con el fin de identificar patrones visuales distintivos y únicos. La particularidad de este módulo radica en su capacidad para detectar patrones que no se definen hasta el momento de su uso, cuando un usuario selecciona una región específica en un fotograma de vídeo a través de la interfaz del sistema. Esta





**Figura 4.23:** Trajectory Fusion

región seleccionada se convierte entonces en una consulta de muestra para rastrear patrones similares en las amplias colecciones de grabaciones de CCTV. Esta funcionalidad permite un análisis detallado y específico de las grabaciones, facilitando la identificación de elementos visuales relevantes en grandes volúmenes de datos de vídeo.

En el ejemplo de la Figura 4.24 se ha definido el patrón de una figura sonriente que un individuo porta en su camiseta, se aprecia como la herramienta es capaz de detectar este patrón en diversos *Frames* del vídeo, por lo que permite detectar al individuo en diversas imágenes de vídeo de cámaras diferentes y seguir sus pasos.



**Figura 4.24:** Ejemplo DROP Component

- **Face Detection and Recognition:** Esta herramienta es capaz de identificar y verificar rostros en una variedad de entornos y condiciones, lo que representa un avance crucial en las operaciones de

## CAPÍTULO 4. CASO 1: MAGNETO

---

seguridad y vigilancia. Utilizando algoritmos de IA y DL, esta herramienta no solo detecta rostros en imágenes y vídeos, sino que también los compara con bases de datos existentes para reconocer individuos. Esto es particularmente útil en la identificación de sospechosos o en la verificación de identidades en investigaciones.

En la Figura 4.25 se observa el funcionamiento de esta herramienta. En la grabación de una cámara exterior, se identifica un rostro y se muestra junto a un porcentaje que indica la fiabilidad de la identificación, así como el nombre de la persona reconocida.



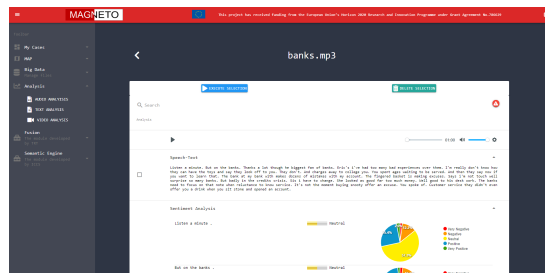
**Figura 4.25:** Face Detection & Recognition

- **Sentiment Analysis y Keyword Extraction:** Se implementan técnicas avanzadas de Sentiment Analysis (Análisis Sentimental) y Keyword Extraction (Extracción de Palabras Clave) aplicadas específicamente a las transcripciones de audio, de llamadas e interrogatorios a sospechosos. En este enfoque, los análisis automatizados desempeñan un papel esencial al identificar rápidamente indicadores de riesgo o elementos clave que podrían no ser evidentes en un análisis manual tradicional. Al aplicar estos métodos a las transcripciones, se puede identificar rápidamente el tono emocional y las palabras clave relevantes en el discurso, lo que permite a los analistas y agentes de seguridad enfocarse en partes específicas del contenido sin tener que dedicar horas a revisar exhaustivamente grandes volúmenes de grabaciones. Esta eficiencia no solo ahorra tiempo valioso, sino que también realza la precisión y efectividad en la identificación de información crucial, facilitando una respuesta más rápida y efectiva en situaciones de seguridad y emergencia.

El análisis de sentimientos se centra en clasificar las opiniones o emociones expresadas en los textos como negativas, neutrales o positivas. Este proceso implica identificar la polaridad de la opinión (positiva o negativa), el sujeto del que se habla y el portador de la opinión. Por otro lado, la extracción de palabras clave busca identificar términos relevantes dentro del texto, agrupando las ideas más importantes para ofrecer una visión general, clara y concisa del contenido analizado [154].

La salida de este módulo proporciona una matriz que relaciona las palabras clave con sus valores correspondientes, que varían entre 0 y 1. Un valor más bajo indica una mayor relevancia de la palabra clave en el contexto del texto analizado.

Para presentar los resultados de estos análisis, se ha diseñado un componente que integra varios elementos clave: el audio original analizado, su transcripción correspondiente, y los resultados del Keyword Extraction Y Sentiment Analysis. Este último se desglosa frase por frase, acompañado de un gráfico que ilustra la probabilidad de que la polaridad de cada segmento sea positiva, neutra o negativa (Figura 4.26).



**Figura 4.26:** Resultados Sentiment Analysis

Respecto al análisis de Keyword Extraction (Figura 4.27), se visualiza a través de una nube de palabras (Word Cloud), donde el tamaño de cada palabra indica su relevancia dentro del texto. Esta representación gráfica proporciona una interpretación visual e intuitiva de los aspectos más destacados del análisis, facilitando la comprensión y el posterior análisis detallado por parte de los usuarios.

- **Semantic Reasoning:** Proporciona un razonamiento probabilístico que tiene como objetivo enriquecer la información existente, así como descubrir nuevos conocimientos y relaciones entre diferentes

## CAPÍTULO 4. CASO 1: MAGNETO

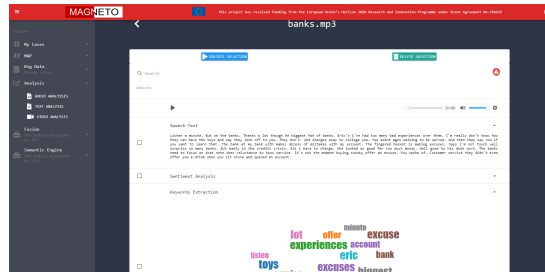


Figura 4.27: Resultados Keyword Extraction

objetos y elementos de datos. En colaboración con las LEAs, se ha desarrollado un conjunto de reglas para diferentes casos de uso. Una regla es una expresión lógica de primer orden con un antecedente y un consecuente, utilizando conceptos y relaciones de la ontología. El antecedente de una regla especifica la condición que debe cumplir la evidencia dada. El consecuente expresa la evidencia inferida.

El fin es detectar personas sospechosas en investigaciones de homicidios, amenazas terroristas o fraudes financieros.

En el siguiente caso de uso se investiga el autor de una ataque con bomba. Una de las reglas aplicadas aquí tiene el siguiente antecedente: una persona ha realizado una planificación de ruta a un lugar cercano a una antena de telecomunicaciones donde ha ocurrido el ataque. El consecuente indica que esa persona es un sospechoso del ataque con bomba.

El resultado del razonamiento se presenta al usuario en este formato: Contiene la evidencia en lenguaje natural, el valor de confianza y las reglas aplicables. En este caso, *Franz Fuchs* ha sido identificado como sospechoso en dos casos de atentados con bomba.

La Figura 4.29 muestra cómo se almacena la evidencia inferida en la KB. La relación que está marcada con un eclipse rojo es el resultado del razonamiento. Conecta al sospechoso *Franz Fuchs* en el recuadro verde con el evento *atentado con bomba* (recuadro rojo) que tiene adjunta la ubicación del lugar del crimen representada como recuadros azules. Las condiciones de comprensión se tienen en cuenta mediante los recuadros amarillos que explican la fuente de la relación como resultado de un proceso de razonamiento y suministran las reglas adjuntas.

## MLN Rule for Suspects of Planned Attacks

**Reasoning Results**

**Franz Fuchs is suspected to plan an attack on "Telecommunication-Mast at Ackermannstraße 65" with a confidence value of 0.4677.**  
 Following rules have been used to generate this result:  
 If a suspect for a bomb attack has performed a routeplanning to a place of a telecom mast, he is a suspected to plan an attack on it. If a suspect for a bomb attack has performed a routeplanning to a place of a telecom mast given in geo coordinates, he is a suspected to plan an attack on it.

**Franz Fuchs is suspected to plan an attack on "Telecommunication-Mast at Hans-Preifinger-Straße 8" with a confidence value of 0.4639.**  
 Following rules have been used to generate this result:  
 If a suspect for a bomb attack has performed a routeplanning to a place of a telecom mast, he is a suspected to plan an attack on it. If a suspect for a bomb attack has performed a routeplanning to a place of a telecom mast given in geo coordinates, he is a suspected to plan an attack on it.

**Franz Fuchs is suspected to plan an attack on "Telecommunication-Mast at Meineckestraße 35" with a confidence value of 0.4663.**  
 Following rules have been used to generate this result:  
 If a suspect for a bomb attack has performed a routeplanning to a place of a telecom mast, he is a suspected to plan an attack on it. If a suspect for a bomb attack has performed a routeplanning to a place of a telecom mast given in geo coordinates, he is a suspected to plan an attack on it.

FETCH DATA
INFER DATA

Figura 4.28: Resultado Semantic Reasoning

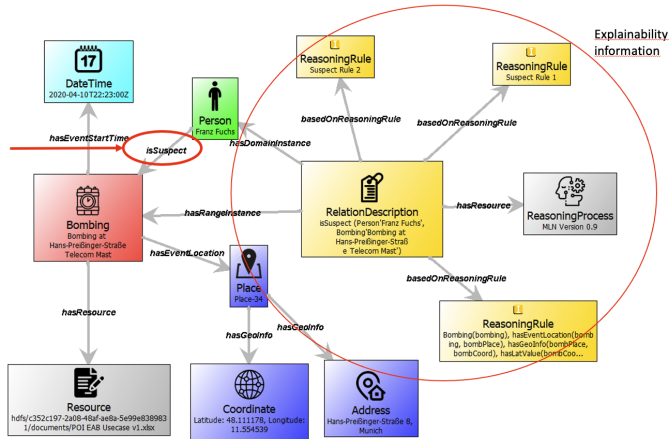


Figura 4.29: Semantic Reasoning - Knowledge Base

Todos estos logros subrayan el papel crucial de MAGNETO en la modernización y mejora de las operaciones de las agencias de seguridad y emergencia, proporcionando una herramienta poderosa para la gestión eficaz en una variedad de escenarios.



# Capítulo 5

## Caso 2: ASSISTANCE

### 5.1. Introducción

En respuesta a la creciente necesidad de colaboración entre distintas entidades de respuesta a emergencias (*First Responder* (FR)s de sus siglas en inglés) frente a desastres de gran envergadura y complejidad, que se han visto agravados por nuevas amenazas como el cambio climático en desastres naturales (como inundaciones de gran extensión o incendios forestales extensos) y el aumento de radicalización en desastres causados por el ser humano (como incendios forestales provocados o grandes ataques terroristas combinados en ciudades europeas), surge el proyecto **ASSISTANCE**. Esta iniciativa aborda directamente las consecuencias potencialmente desastrosas para las regiones de los estados miembros de la UE y el bienestar social en su conjunto. Los FRs, ya sean servicios de emergencia médica, bomberos, fuerzas del orden o profesionales de la protección civil, se encuentran frecuentemente en situaciones donde enfrentan peligros inesperados que amenazan su integridad personal.

El proyecto ASSISTANCE propone una solución completa e integradora, que se centra en potenciar la *Situational Awareness* (SA) de los FRs ofreciendo diferentes modos de configuración que proveerán la información específica requerida por cada organización de FRs en su labor conjunta para mitigar desastres, tales como la transmisión de vídeo en tiempo real y la ubicación de recursos para bomberos, o el estado de las rutas de evacuación para los servicios de salud de emergencias [173]. La plataforma proporciona medios esenciales para la mitigación de desastres, facilitando así la toma de decisiones críticas durante las emergencias.

Mejorando la SA a través de la integración de nuevas tecnologías, como UAVs y robots con sensores avanzados y capacidades robustas de comunica-

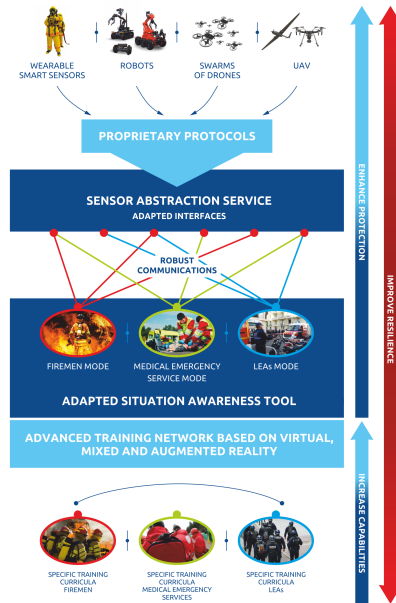


Figura 5.1: Concepto ASSISTANCE

ción, ASSISTANCE tiene como fin último incrementar la protección y eficiencia de los FRs. Además, el proyecto se compromete a mejorar sus habilidades y capacidades mediante la creación de una red avanzada de formación en Europa. Esta red se basará en metodologías innovadoras de aprendizaje como la realidad virtual, mixta y aumentada, y permitirá compartir entornos virtuales de formación y el intercambio de experiencias y procedimientos operativos.

La visión de ASSISTANCE incluye el uso estratégico de UAVs, sensores inteligentes portátiles, y enjambres de UAVs, todos equipados con sensores específicos para cubrir las demandas detalladas por los FRs. Estas herramientas no solo se integrarán como soportes para sensores, sino también como activos operativos en el campo, mejorando así la plataforma completa de SA para una ejecución más segura y eficaz de las tareas de los FRs.

El compromiso del proyecto con los valores sociales europeos es firme, asegurando que todos los desarrollos se realicen en conformidad con los derechos fundamentales, la privacidad, la protección de datos personales, y teniendo en cuenta la dimensión de género y los aspectos sociales. La descripción detallada de la plataforma de SA y la red de formación avanzada, que constituyen los



pilares de ASSISTANCE, así como la sinergia obtenida a través de su integración, se expondrá en las secciones subsiguientes, delineando un enfoque que no solo está alineado con las necesidades actuales de los FRs, sino que también está preparado para adaptarse a los retos futuros.

## 5.2. Objetivos de ASSISTANCE

ASSISTANCE tiene un objetivo principal de doble propósito. Por un lado, el proyecto busca salvaguardar y brindar apoyo a las distintas FRs que trabajan de manera conjunta durante la mitigación de grandes catástrofes, tanto naturales como provocadas por el ser humano. Por otro lado, ASSISTANCE tiene como meta mejorar las capacidades y habilidades de las FRs para hacer frente a este tipo de eventos. Esto se logrará mediante la consecución de los siguientes objetivos:

1. **Atender las necesidades específicas de los FRs expresadas durante la fase de preparación del proyecto, incrementando sus capacidades mediante la incorporación de tecnologías útiles y la integración de nuevos sensores** en plataformas no tripuladas y equipos portátiles.
2. **Desarrollar una plataforma de SA avanzada que integre UAVs, Robots y enjambres de UAVs**, incluyendo módulos innovadores que se adaptarán a las necesidades informativas específicas de las organizaciones de FRs durante las respuestas a grandes desastres, ya sean naturales o antrópicos.
3. **Establecer una infraestructura de formación avanzada basada en realidad virtual y realidad aumentada**, en colaboración con instituciones reconocidas de formación de FRs, para ofrecer currículos de capacitación personalizados que mejoren las habilidades actuales de diversos tipos de FRs.
4. **Proveer una infraestructura de red robusta para garantizar la conectividad de los FRs y las plataformas no tripuladas** durante las operaciones de mitigación, proporcionando soluciones de rendimiento de red ad hoc en situaciones donde la conectividad estándar no está disponible.
5. **Validar los resultados del proyecto en un entorno controlado y rentable**, bajo condiciones reales, involucrando a FRs de diversas organizaciones en simulacros y demostraciones para probar la eficacia de las soluciones propuestas.

6. **Evaluar el impacto social del proyecto, asegurando la conformidad con las leyes, la igualdad de género y las consideraciones éticas**, identificar obstáculos y desarrollar recomendaciones concretas para políticos y FRs con el fin de mejorar el nivel de protección y aumentar sus capacidades de forma legal y ética.

### 5.3. Arquitectura de ASSISTANCE

La base para la plataforma de SA de ASSISTANCE es una combinación entre la arquitectura propuesta en el Capítulo 3 y una adaptación de la versión civil del sistema de seguimiento de fuerzas amigables del Ejército Español, SIMACET-FFT [174], desarrollado por *Universitat Politècnica de València* (UPV) [175] y operativo actualmente en Afganistán, Líbano y Malí. ASSISTANCE incorpora y actualiza varias de estas capacidades de SA ya existentes para su plataforma central durante el transcurso del proyecto.

Se planifica el desarrollo e integración de módulos y capacidades de SA novedosos para complementar la infraestructura preexistente y conformar la plataforma completa de SA de ASSISTANCE. El diseño de alto nivel de la *Situational Awareness Platform* (SAP) de ASSISTANCE se muestra en la Figura 5.2.

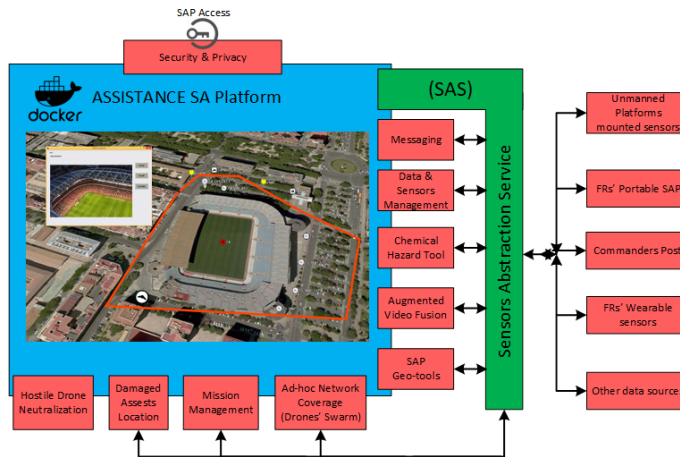
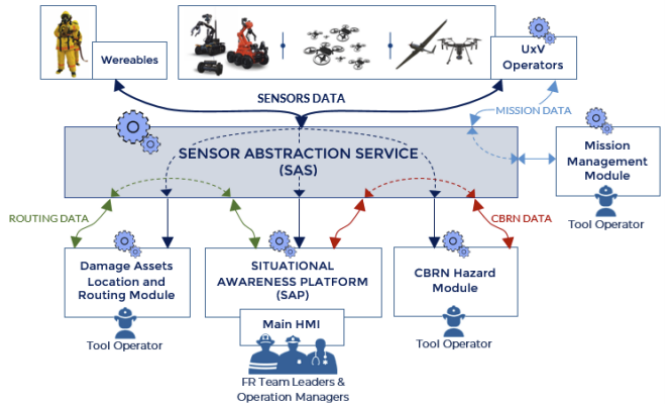


Figura 5.2: Arquitectura ASSISTANCE alto nivel

El sistema ASSISTANCE se caracteriza por una integración completa de todos los módulos y componentes ilustrados en la Figura 5.2, creando una dinámica de colaboración que potenciará la capacidad de los FRs más allá de su enten-

## 5.3 Arquitectura de ASSISTANCE

dimiento actual de la SA. La estructura detallada del sistema ASSISTANCE se presenta en la Figura 5.3.



**Figura 5.3:** Arquitectura Sistema ASSISTANCE

La SAP de ASSISTANCE se diseñó para captar y sintetizar datos de una variedad de sensores y sistemas, presentando la información consolidada de forma personalizada a los distintos FRs a través del HMI. Adicionalmente, los módulos y sistemas dentro de ASSISTANCE procesan los datos de múltiples sensores y fuentes para ejecutar sus operaciones internas y posteriormente enviar los resultados hacia la SAP.

Para la integración eficaz de estos componentes, ASSISTANCE adopta un esquema de intercambio de información basado en el modelo de *publicación/suscripción*, implementado a través del *Sensors Abstraction Service (SAS)*. El SAS es un componente crucial que actúa como intermediario entre la diversidad de sensores y sistemas de recopilación de datos y las plataformas de análisis y procesamiento. Su función principal es abstraer la complejidad inherente a la gestión de múltiples tipos de sensores y formatos de datos, proporcionando una interfaz unificada para el acceso y la manipulación de esta información.

El SAS es esencialmente una capa de software que normaliza y estandariza los datos de diferentes fuentes, permitiendo que sistemas heterogéneos y aplicaciones puedan comunicarse y compartir datos de manera eficaz. Al hacerlo, el SAS facilita una integración más fácil y flexible de tecnologías de sensores variados, desde cámaras de video hasta sensores ambientales y meteorológicos, en una única red cohesiva.

En el proyecto ASSISTANCE, el SAS está preparado para trabajar con diversos protocolos de comunicación como AMQP, *Message Queuing Telemetry*

## CAPÍTULO 5. CASO 2: ASSISTANCE

---

*Transport* (MQTT) [176], *Neural Autonomic Transport System* (NATS) [177] o *Datagram Delivery Protocol* (DDP) [178]. Esta capacidad multifacética del SAS es una evolución del *Broker* diseñado en la arquitectura original y utilizado en la arquitectura del proyecto MAGNETO. El SAS responde a la necesidad de integrar las fuentes de datos heterogéneas que se manejan en ASSISTANCE. La adaptabilidad del SAS a diferentes protocolos es crucial, dado que facilita la recopilación y el análisis de datos de múltiples fuentes en un entorno operativo altamente dinámico y variado, asegurando así que los datos recopilados sean accesibles, confiables y útiles para la toma de decisiones en situaciones de emergencia.

En la arquitectura del sistema de ASSISTANCE, se opta por una estructura híbrida, combinando los beneficios del *CLOUD* y las capacidades del *EDGE Computing* [179]. Se elige la modalidad de microservicios en lugar de una estructura monolítica, lo que aporta ventajas como mayor facilidad en el desarrollo y mantenimiento, incremento de la productividad y velocidad, y una mayor flexibilidad tecnológica con escalabilidad. Además, esta arquitectura impulsa la formación de equipos autónomos y multifuncionales.

En esta arquitectura híbrida, componentes críticos como bases de datos se alojan en el *CLOUD* para aprovechar su robustez, capacidad de almacenamiento expansible y alta disponibilidad. Esto permite un acceso centralizado y seguro a los datos, esencial para el análisis y la toma de decisiones a largo plazo. Por otro lado, componentes como el SAS y la SAP se sitúan en el *EDGE* para garantizar una baja latencia y una respuesta rápida, crucial en operaciones en tiempo real donde cada segundo cuenta.

En la parte del *EDGE*, todos los componentes están dockerizados, lo que permite un despliegue rápido, eficiente y modular. La contenerización asegura que cada servicio sea ligero, independiente y pueda ser desplegado o escalado de manera ágil, adaptándose a las necesidades cambiantes del entorno operativo. Esta estrategia de dockerización en el *EDGE* maximiza la eficiencia operativa y minimiza el tiempo de inactividad, asegurando una alta disponibilidad y tolerancia a fallos de los servicios críticos en situaciones de emergencia.

En la Figura 5.4 se muestra el Modelo de datos de la información ofrecida por el SAS relacionada con los sensores, UAVs y unidades desplegadas.

- **Mission:** Asociada con una colección de recursos a través del atributo “*missionId*”. Todos los recursos usados en la misión estarán vinculados a este objeto.
- **Resource:** Identifica recursos de la misión mediante el atributo “*\_Id*”. Incluye marcas de tiempo y atributos geojson para posiciones y rutas, un “*array of sensors*” para sensores asociados, y un “*array of camera*” para cámaras asociadas. El tipo de recurso se define con el atributo “*type*”.

## 5.3 Arquitectura de ASSISTANCE

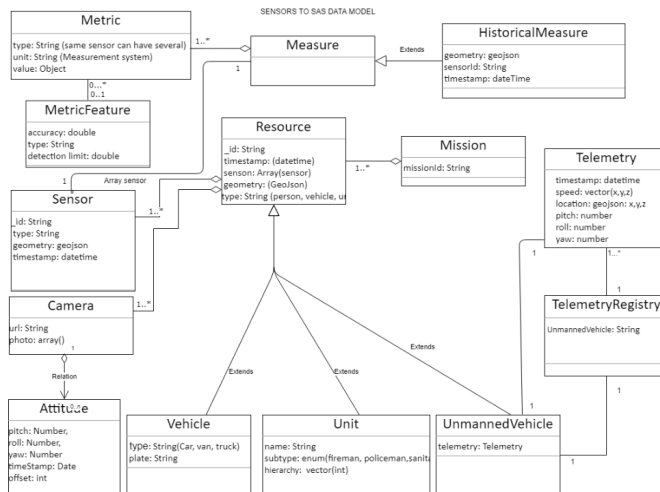


Figura 5.4: Modelo de Datos Sensores

- **Vehicle:** Un recurso que especifica el tipo y la placa mediante los atributos *“type”* y *“plate”*.
- **Unit:** Representa a una persona, con atributos como *“name”*, *“subtype”* y *“hierarchy”* para indicar el nombre, el tipo de FR y la jerarquía en su organización.
- **UnmannedVehicle:** Se define por el atributo *“telemetry”*, relacionado con telemetría a través del *“telemetryRegistry”*.
- **Camera:** Tiene un atributo *“url”* para la transmisión de vídeo y *“photo”* para una matriz de imágenes accesibles desde la SAP.
- **Telemetry:** Incluye atributos como *“timestamp”*, *“speed”*, *“location”* y ejes de movimiento (*“Pitch”*, *“roll”*, *“yaw”*).
- **Attitude:** Los ejes de la cámara (*“Pitch”*, *“roll”*, *“yaw”*) se definen en relación con el UAV, con *“timestamp”* para el momento de captura y *“offset”* para la distancia desde el centro del UAV.
- **TelemetryRegistry:** Representa el historial de telemetría, con medidas anteriores accesibles.

- **Sensor:** Identificado únicamente por “*\_id*”, con “*type*” para el nombre del tipo de recurso, “*timestamp*” para el tiempo de medición y “*geojson*” para la ubicación geográfica.
- **Measure:** Asociada con una colección de métricas del sensor.
- **Metric:** Indica valores medidos por un sensor, con “*type*” para el tipo de medida y “*unit*” para la unidad de medida.
- **MetricFeature:** Compuesto por “*accuracy*”, “*Detection limit*” y “*type*”, asociando métricas con características comunes.
- **HistoricalMeasure:** Representa medidas históricas, con “*timestamp*”, “*geojson*” y “*sensor id*” para identificar datos del sensor relacionado.

Una vez que los datos se encuentran en el SAS, se distribuyen a los distintos subsistemas mediante el empleo de diversas tecnologías. Entre ellas, se incluyen Websockets y principalmente AMQP, para la transmisión en tiempo real. Además, implementa una API REST, que facilitará operaciones CRUD. Para acceder a los datos de un elemento específico, los usuarios necesitarán especificar la categoría y el identificador único del elemento, como se ilustra en la ruta de acceso `/sensores/id`.

### 5.3.1. Módulo SAP

La interfaz de usuario avanzada y el sistema analítico diseñados en ASSISTANCE brindan a los FRs y a los centros de comando una visión integral y actualizada de las situaciones de emergencia. Estos componentes trabajan en conjunto para presentar la información de manera fácilmente accesible y comprensible, brindando una visión completa de la situación en tiempo real.

La SAP es el núcleo del sistema ASSISTANCE, consolidando datos de múltiples fuentes, como sensores *in situ*, *Wearables* y cámaras, además de integrar la información de ubicación y las comunicaciones en tiempo real. Esta plataforma no solo facilita una percepción detallada del entorno operativo, sino que también permite la identificación y seguimiento de amenazas, la gestión eficiente de recursos y la coordinación de equipos. La SAP se apoya en tecnologías punteras para la visualización de datos, la toma de decisiones basada en información de inteligencia y la colaboración interagencial, todo dentro de un marco que prioriza la respuesta rápida y la seguridad en las operaciones de emergencia.

La SAP está compuesto por varios módulos que brindan funcionalidades específicas para mejorar la gestión de situaciones de emergencia. A continuación se detallan cada uno de estos módulos.

### Fusión de Vídeo Aumentada

La fusión de vídeo aumentada es una capacidad innovadora desarrollada completamente durante el proyecto ASSISTANCE permite la superposición de flujos de vídeo en tiempo real provenientes de UAVs sobre el SIG integrado en la interfaz de usuario. Mediante esta avanzada funcionalidad, se proyecta el campo de visión del UAV en un modelo de terreno tridimensional, lo que proporciona una perspectiva más rica y detallada de la zona de operaciones.

El UAV capturará flujos de vídeo en tiempo real, así como datos en bruto de varios sensores montados a bordo. Para capturar el estado actual del área bajo vigilancia y la ubicación del UAV, los elementos clave son la cámara y el *Global Positioning System* (GPS). Para las demostraciones y ejercicios de ASSISTANCE, se utilizará un UAV de la familia Matrice de DJI [180] (Figura 5.5).



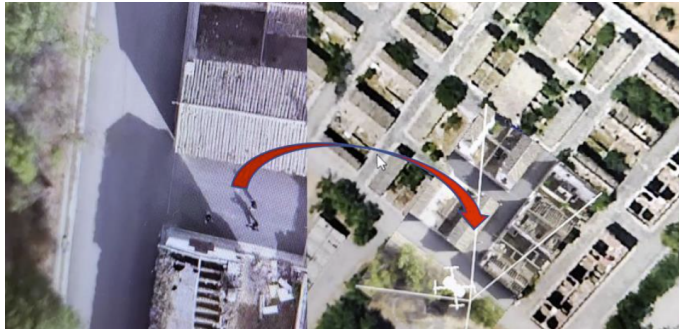
**Figura 5.5:** UAV Matrice DJI

La posición del UAV se determina utilizando un receptor GPS y el subsistema correspondiente en la plataforma del UAV proporciona la altitud. Los datos se recopilan para cada fotograma de vídeo y se reciben a través del mensaje de telemetría.

Los UAVs envían imágenes codificadas y su telemetría sincronizada para cada fotograma a través de MQTT. El SAS recibe esta información de los UAVs conectados al sistema y la publica para que sea procesada por los módulos de Fusión de Vídeo Aumentada en tiempo casi real.

### Módulo de Riesgo CBRN

Este módulo calcula la huella potencial de peligro *Chemical, Biological, Radiological and Nuclear* (CBRN), presentada en un mapa, basado en la descripción del usuario sobre el tipo de peligro. La salida se adapta y ajusta continuamente en función de la información en tiempo real de los datos del sensor, los datos meteorológicos y la entrada de los recursos FR.



**Figura 5.6:** Video Fusion SAP

Produce y muestra los límites de las áreas en el mapa donde las concentraciones de gases superan ciertos niveles de toxicidad, y puede predecir la evolución de dicha nube de gases [181]. Muestra la posición y el tamaño más probable de la nube (actual y predicha), pero también las incertidumbres en cuanto a su posición y tamaño, que se deben a incertidumbres en, por ejemplo, la cantidad de gas liberado, la dirección del viento y la turbulencia del viento.

Esto ayuda a los FR a saber dónde tener precaución para evitar el peligro tóxico y dónde realizar mediciones para determinar las concentraciones reales de gases. Además, las mediciones de gases disponibles del SAS se utilizan en el módulo para recalculer la posición y el tamaño de la nube de gases.

En la Figura 5.7 se muestra el flujo de datos. La aplicación Traccar transmite las posiciones de las unidades al SAS mediante un servicio de retransmisión. En el núcleo del sistema, el SAS centraliza estos datos, que luego se utilizan junto con información de un servidor web que ejecuta Node.js para alimentar la *Graphical User Interface* (GUI) con mapas interactivos (Figura 5.8). Paralelamente, el servicio de dispersión utiliza datos de predicción de peligros y datos meteorológicos, como la velocidad del viento del servicio meteorológico, para calcular y predecir la dispersión de sustancias químicas en el ambiente. Estos cálculos se integran en la GUI, proporcionando a los FRs una herramienta visual para evaluar y responder a incidentes químicos en tiempo real.

### Ubicación y Enrutamiento de Activos Dañados

El *Damaged Assets Location Routing* (DALR) utiliza imágenes en tiempo real proporcionadas por cámaras y UAVs para apoyar los procesos de toma de decisiones de los FRs. Este módulo implementa tres funcionalidades principales [182]:



## 5.3 Arquitectura de ASSISTANCE

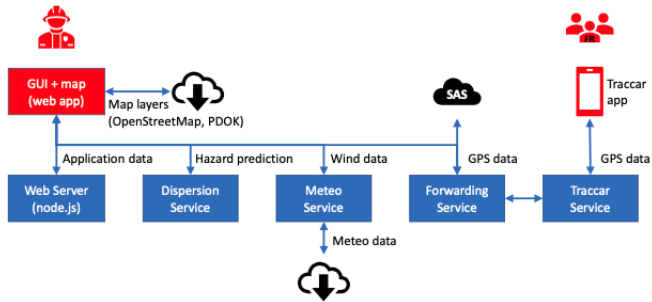


Figura 5.7: Flujo datos CBRN



Figura 5.8: Visualización Pluma Tóxica

- Identificar ubicaciones de activos o infraestructuras dañadas o áreas intransitables.
- Proporcionar un mecanismo de enrutamiento para obtener rutas de intervención o evacuación, evitando los activos dañados identificados.
- Ayudar en el proceso de gestión de evacuación, proporcionando tiempos de intervención y evacuación basados en algoritmos de optimización y toma de decisiones adecuados.

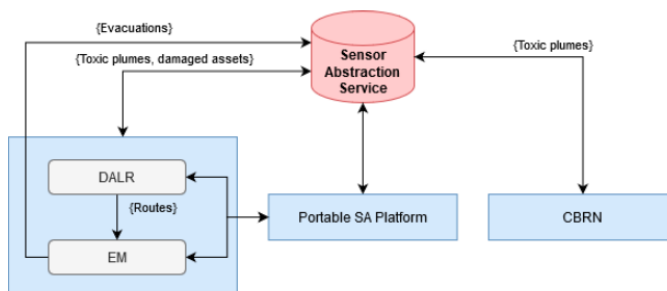
Todas estas funcionalidades, junto con el trabajo conjunto y los datos obtenidos por otros módulos (por ejemplo, datos de sensores, módulo CBRN, etc.), almacenados en el SAS, representan un importante paso innovador gracias a la interacción en tiempo real entre los FRs y los módulos de simulación.

## CAPÍTULO 5. CASO 2: ASSISTANCE

---

En la arquitectura del módulo DALR (Figura 5.9) destacan dos módulos principalmente:

- **DALR:** Combina imágenes de vídeo reales con cartografía 3D y herramientas de manipulación de mapas. Estas características permiten a los usuarios:
  1. Analizar el vídeo grabado por un UAV.
  2. Detectar áreas dañadas o cualquier elemento que pueda influir en la gestión de una emergencia.
  3. Interactuar con el mapa superponiendo objetos geométricos y clasificándolos para que otros servicios como la *Evacuation Management* (EM) los tengan en cuenta al realizar sus cálculos.
- **EM:** Capaz de proporcionar estrategias de evacuación completas mediante el procesamiento de información geográfica que incluye áreas de evacuación, ubicación de activos dañados y plumas tóxicas. Las principales variables utilizadas para caracterizar una estrategia particular de evacuación son:
  - Ubicaciones de puntos de reunión
  - Ubicaciones de refugios
  - Rutas de evacuación
  - Resultados de simulación de tráfico



**Figura 5.9:** Arquitectura módulo DALR

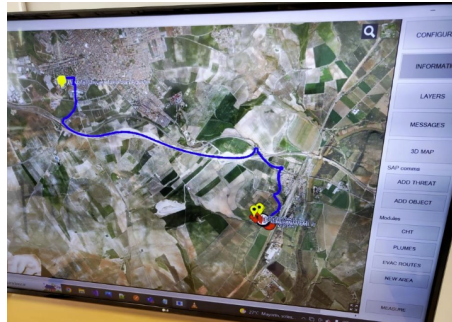


Figura 5.10: Ejemplo Ruta Evacuación

### SAP HMI

EL HMI de la SAP representa una de las innovaciones destacadas del proyecto ASSISTANCE. Esta interfaz versátil ha sido diseñada para ser utilizada tanto en emplazamientos fijos, como Puestos de Control operados a través de ordenadores, como en el terreno, a través de tablets ruggedizadas que aseguran durabilidad y funcionamiento bajo condiciones adversas. La flexibilidad de la SAP HMI permite que los FRs en el campo tengan acceso en tiempo real a las funcionalidades críticas de la SAP, lo que facilita la toma de decisiones informadas y la coordinación efectiva durante las operaciones de emergencia.

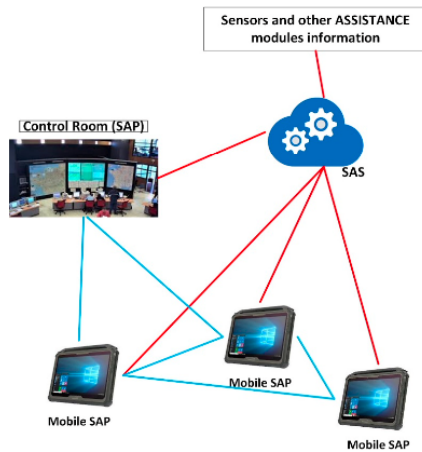
Las unidades SAP constituyen un sistema interconectado que permite una comunicación fluida y el intercambio de información entre la instalación principal de la SAP y todos los dispositivos, la SAP portátiles (flechas azules Figura 5.11), asegurando que datos críticos como mensajes internos, áreas designadas, puntos de interés y perfiles de perímetros sean consistentemente replicados y actualizados entre todas las instancias de la SAP.

Además, al igual que la SAP de escritorio, la SAP portátil mantiene sus propias interfaces dedicadas para la recepción de información directamente del SAS, tales como datos de sensores, información de vehículos no tripulados *Unmanned eXpeditory Vehicle* (UxV), y alertas (enlaces rojos Figura 5.11).

Este módulo integra en una interfaz todas las herramientas y componentes que forman la SAP de ASSISTANCE, a continuación se listan algunas de ellas.

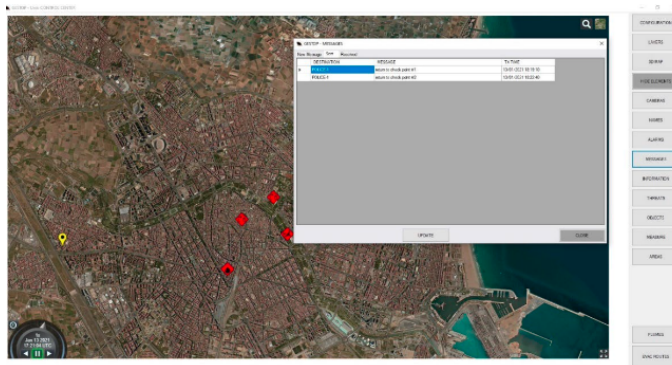
### Intercambio de mensajes

Todas las instancias de la SAP (general y portátil) cuentan con su propio servicio de mensajería interna que permite enviar y recibir mensajes de texto



**Figura 5.11:** Intercambio Información SAP

de manera fácil y segura durante las operaciones entre las distintas unidades SAP.



**Figura 5.12:** Mensajes

### Herramientas geográficas

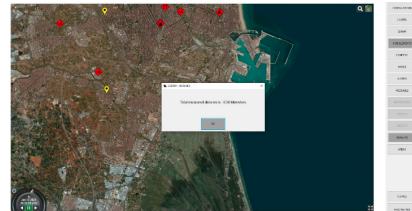
Estas capacidades permiten realizar acciones en los mapas de manera fácil y rápida con el fin de ayudar a los FRs y a sus comandantes durante la planificación o mitigación de un gran desastre. Estas acciones serían las siguientes.

## 5.3 Arquitectura de ASSISTANCE

- **Definición de polígonos como áreas seguras o de peligro:** Los usuarios pueden definir y modificar polígonos sobre el mapa para demarcar áreas específicas. Estos polígonos pueden representar zonas de peligro, como áreas químicas contaminadas o en llamas, o áreas seguras designadas para la evacuación y la asistencia. La herramienta de polígonos es interactiva y permite la personalización en tiempo real para adaptarse a la dinámica cambiante de una situación de emergencia (Figura 5.13).
- **Medición de distancias sobre el mapa:** La funcionalidad de medición permite a los usuarios calcular con precisión las distancias entre varios puntos en el mapa. Esta herramienta es esencial para planificar rutas de evacuación, establecer perímetros de seguridad y coordinar el despliegue de recursos y personal. La interfaz gráfica proporciona una lectura directa de las distancias, facilitando la toma de decisiones estratégicas basadas en la geolocalización (Figura 5.14).
- **Visualización de mapa en 3D:** La SAP ofrece una poderosa visualización tridimensional del terreno, permitiendo a los usuarios obtener una perspectiva más realista del área de operaciones. Esta vista 3D es particularmente útil para comprender mejor la topografía del terreno, planificar el despliegue de UAVs y otros recursos, y mejorar la SA al agregar una dimensión adicional a la representación del mapa (Figura 5.15).



**Figura 5.13:** Definición de Áreas



**Figura 5.14:** Medida de Distancia



**Figura 5.15:** Vista 3D

### Integración de sensores

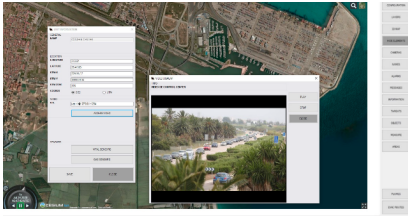
La SAP recibe automáticamente del SAS información sobre los sensores montados en UAVs y robots. Entre los datos recibidos se incluyen:

- **Flujos de vídeo en tiempo real:** Los UAVs, robots y FR equipados con cámaras proporcionan flujos de vídeo que la SAP recibe y muestra. Esta visualización en tiempo real es esencial para la monitorización operativa, permitiendo a los usuarios de la SAP obtener una vista inmediata y precisa de las áreas afectadas, así como supervisar las acciones y movimientos en escenarios críticos (Figura 5.16).
- **Señales vitales:** La SAP también procesa y presenta datos de las señales vitales recogidos por el dispositivo Cosinuss. Estos datos incluyen, la frecuencia cardíaca y la temperatura corporal de los FRs. Estos datos se muestran en forma de gráfica para monitorizar en todo momento los cambios o alteraciones que puedan producirse, además el sistema permite definir unos valores umbrales, los cuales si son sobrepasados nos informará en forma de alerta. Este enfoque que es crucial para monitorizar la salud y seguridad de los FRs durante las operaciones de alto riesgo. (Figura 5.17).
- **Mediciones de gases:** Los sensores montados en vehículos no tripulados pueden detectar y medir la concentración de gases peligrosos en el ambiente. La SAP visualiza estas mediciones en forma de puntos sobre un GIS, mostrando además metadatos asociados como la hora de la medición. Esto permite a los comandantes identificar áreas de riesgo químico y tomar medidas preventivas para proteger a los equipos y al público (Figura 5.18).

La integración de estos datos sensoriales en la SAP proporciona una vista comprensiva del ambiente operativo, potenciando la SA de todos los agentes involucrados y facilitando una respuesta coordinada y eficiente ante emergencias.

### 5.3.2. Sensores

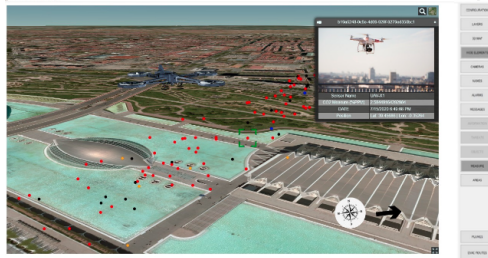
Esta sección aborda una amplia gama de tecnologías de detección y monitorización que son cruciales en el contexto de operaciones de emergencia y rescate. Principalmente, se centra en vehículos no tripulados, como robots y UAVs, además de una variedad de sensores especializados, incluyendo cámaras, sensores de campo (temperatura, gas, etc.) y dispositivos *Wearables*. Estos sensores desempeñan un papel fundamental en la recopilación de información



**Figura 5.16:** Video UAV



**Figura 5.17:** Señales Vitales FR



**Figura 5.18:** Medidas Sensores Gas

crítica en tiempo real, permitiendo a los equipos de respuesta rápida obtener una comprensión detallada y actualizada de las condiciones en el terreno. Los vehículos no tripulados y los robots, equipados con estos sensores, pueden acceder a áreas que pueden ser inaccesibles o peligrosas para los humanos, mientras que los dispositivos *Wearables* proporcionan datos vitales sobre las condiciones y el bienestar de los FRs en acción. La integración y análisis de los datos recopilados por estos sensores son fundamentales para una toma de decisiones efectiva y una respuesta rápida.

### Plataformas no tripuladas

La selección de plataformas no tripuladas se basa en una evaluación detallada de las condiciones externas, incluyendo factores como el tipo y características del terreno o espacio de operación, la resistencia y durabilidad de la plataforma, así como las especificaciones de la carga útil, incluyendo su tipo y peso. Además, se considerarán las dimensiones y peso de la plataforma, su autonomía operativa y otros requisitos funcionales esenciales para cumplir con los objetivos establecidos en cada misión piloto.

La plataforma terrestre requerirá estar dotada de interfaces adecuadas que permitan la integración eficiente de sensores y otros dispositivos. Es esencial que estas interfaces sean bidireccionales, proporcionando al operador la capacidad

## CAPÍTULO 5. CASO 2: ASSISTANCE

---

de controlar los dispositivos adicionales según sea necesario. Las adaptaciones se enfocarán en preservar la modularidad de la solución, garantizando así la facilidad para modificar la carga útil en respuesta a variaciones en el escenario o en los casos de uso específicos.

Las plataformas no tripuladas están equipadas con una variedad de sensores e interfaces para la recolección y transmisión de datos, que incluyen:

- **Cámaras:** Proporcionan imágenes de vídeo en tiempo real de la situación para los usuarios finales.
- **Cámaras Térmicas:** Sensores térmicos para la detección de temperatura.
- **Sensores de Gases:** Detectan la concentración de *Monóxido de Carbono* (CO) y *Dióxido de Carbono* (CO<sub>2</sub>).
- **Estación Meteorológica:** Mide parámetros como viento, temperatura y humedad.

Además, es crucial el intercambio de datos relacionados con la misión, que comprende:

- **Ruta de Vuelo:** Lista de puntos de paso que el robot debe seguir, recibida a través del SAS desde el *Mission Management Module* (MMM).
- **Datos de Telemetría:** Incluyen información sobre el estado del robot como posición, velocidad, actitud, etc. Estos datos se envían al MMM a través del SAS.

La elección de UAVs y los sensores que llevan varía según las demandas específicas de cada escenario y caso de uso. Esta flexibilidad en la selección permite una respuesta más efectiva y adaptada a las condiciones particulares de cada situación. En el Capítulo 6 se detalla la selección de UAVs y sensores apropiados para cada Caso de Uso.

Para la comunicación de los UAVs con el SAS se sigue el flujo de la Figura 5.19.

En los tres escenarios propuestos, se implementan tres interfaces esenciales para la adquisición y solicitud de datos al SAS:

1. **Descarga de misiones entrantes:** Las misiones son descargadas al *Ground Control Station* (GCS) mediante la API REST desde el SAS. Una vez procesadas en el ordenador, pueden ser cargadas en el UAV por el piloto.





Figura 5.19: Flujo dato UAV

2. **Transmisión de video de cámaras a bordo:** El flujo de vídeo de las cámaras a bordo del UAV se transmite a un receptor de vídeo, que posteriormente lo envía al ordenador. Este vídeo se transfiere al SAS utilizando el protocolo *Real Time Streaming Protocol* (RTSP) [183], permitiendo su visualización en tiempo real.
3. **Publicación de telemetría y datos sensoriales del UAV:** El UAV envía al SAS su telemetría, las lecturas de los sensores y las capturas de pantalla, todo sincronizado con la telemetría. Estos datos se estructuran en formato JSON y se transmiten mediante MQTT. Un *Broker* intermedio en el ordenador de abordaje asegura la entrega de los mensajes en caso de pérdida temporal de la comunicación con el SAS. La conexión entre el UAV y el SAS se realiza a través de un enlace de datos de radio conectado a un módem en tierra, facilitando la visualización de los datos durante el vuelo.

Este diseño garantiza una transmisión de datos continua y eficaz, esencial para operaciones con UAVs, donde la estabilidad de la comunicación no siempre puede ser garantizada.

En cuanto a la plataforma de Robots se comunican con el SAS de una forma parecida a cómo lo hacen los UAVs, como se observa en la Figura 5.20.

Concretamente en ASSISTANCE se utilizó el ROBOT PIAP GRYP proporcionado por los socios PIAP [184] (Figura 5.21). El PIAP GRYP® [185] es un robot de reconocimiento móvil diseñado para una amplia gama de aplicaciones

## CAPÍTULO 5. CASO 2: ASSISTANCE

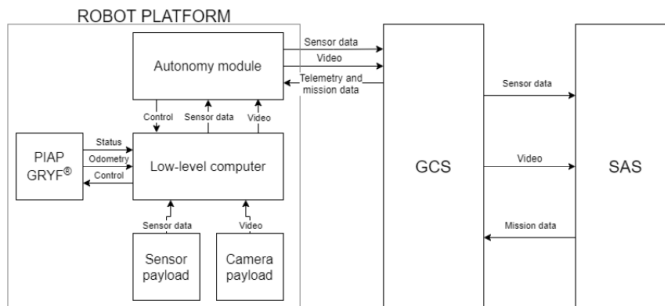


Figura 5.20: Plataforma Robot

y se destaca por su versatilidad. Este robot se caracteriza por su excepcional maniobrabilidad y su peso ligero, lo que facilita tanto su transporte como su manipulación en el campo. Además, su diseño modular permite un cambio rápido y eficiente del equipo adicional.



Figura 5.21: PIAP GRYF

El PIAP GRYF® es controlado por GCS dedicado a través de una conexión inalámbrica personalizada utilizando el protocolo estándar *Joint Architecture for Unmanned Systems* (JAUS). El estándar JAUS [186] define múltiples protocolos de comunicación para conectarse con sistemas de control remoto.

Entre los módulos que componen la plataforma Robot destacan:

- **Módulo Autónomo:** Captura los datos en bruto de los componentes del robot y los ingresa en la pila de autonomía. Esto incluye tanto los datos en bruto utilizados internamente como los datos que se envían a través de JAUS al GCS. Los datos internos incluyen, por ejemplo, odometría de

## 5.3 Arquitectura de ASSISTANCE

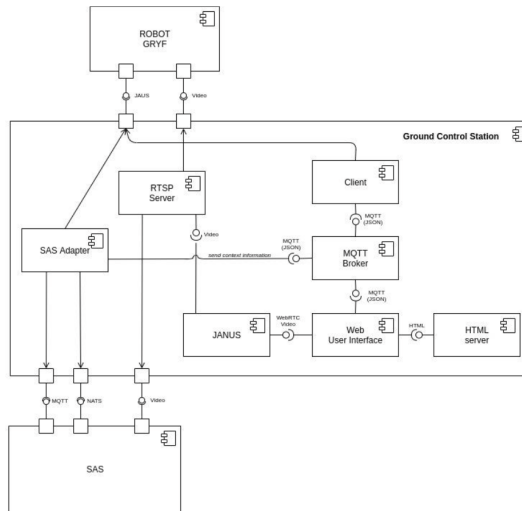


Figura 5.22: GCS Robot

los servos de las ruedas, lecturas en bruto de la *Inertial Measuring Unit* (IMU), etc. Los datos se recopilan a través de múltiples interfaces, siendo la más relevante el bus *Controller Area Network* (CAN), que proporciona datos como las lecturas de los sensores, la odometría, la posición de las articulaciones del manipulador y el nivel de la batería.

- GCS: Es una combinación de hardware y software que actúa como interfaz entre el robot y el SAS o el usuario.

La GCS incluye los siguientes componentes:

- **Adaptador SAS:** Este componente actúa como un adaptador para asegurar la comunicación con el SAS en varios niveles, procesando y convirtiendo la información recibida de/al protocolo JAUS. Entre sus funciones clave se encuentran la gestión de misiones, donde maneja tareas específicas programadas para momentos determinados; la conversión de datos entre los formatos SAS JSON y la interfaz del robot JAUS; la validación de la estructura de los datos recibidos para garantizar su precisión; el almacenamiento de datos que no están disponibles en el robot o que no se transmiten a través del protocolo JAUS; y el mantenimiento y gestión de las conexiones, incluyendo la gestión de solicitudes de control y la reconexión en caso de interrupciones.

- **Cliente:** Es un componente que traduce los datos de la interfaz JAUS a la interfaz MQTT operada en el navegador. Simultáneamente, convierte el formato de los datos de/a JAUS a JSON.
- **Servidor HTML:** Proporciona una aplicación para el control del robot, creada utilizando el *Framework* Vue.js.
- **Broker MQTT:** Soporta el protocolo MQTT utilizando el *Broker* de mensajes de código abierto Mosquitto [187]. Este protocolo facilita la mensajería ligera mediante un modelo de publicación/suscripción.
- **Servidor RTSP:** Ofrece varias transmisiones de vídeos de forma simultánea e independiente.
- **Janus:** Un servidor *Web Real-Time Communications* (WebRTC) [188] de propósito general que se comunica con el navegador. Consta de un módulo principal y complementos para implementar funcionalidades específicas, como la transmisión de vídeo.
- **Interfaz de Usuario Web:** Aplicación de software para el control del robot, integrando todas las funcionalidades mencionadas.

### Wearables

La integración de *Wearables* en el sistema ASSISTANCE permite una comunicación más efectiva, un seguimiento constante de las condiciones del personal en el campo y una mejor coordinación durante las misiones críticas.

En esta sección se proporciona una descripción detallada del diseño, las capacidades y la integración de los dispositivos *Wearables*.

Concretamente, para los Casos de Uso de ASSISTANCE se han integrado los siguientes *Wearables*:

- **Cosinuss Two: Señales vitales y sensor de temperatura:** El cosinuss Two [189] (Figura 5.23) monitoriza de manera precisa múltiples signos vitales, como la frecuencia cardíaca, la temperatura corporal y el SpO<sub>2</sub>, entre otros. Pesa 6,5 gramos y tiene un tamaño de 4 x 4 cm, siendo un tapón auricular ergonómico, pequeño y ligero, sin pérdida de audición.

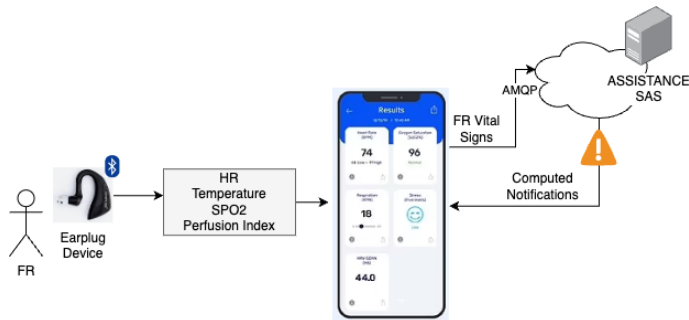
El desarrollador de Cosinuss realiza estudios exhaustivos en cooperación con reconocidos asociados. Para obtener la media y la desviación estándar, el sensor cosinuss two fue probado con instrumentos de medición estándar aprobados médicamente.

Para la integración de los datos de los dispositivos Cosinuss con el SAS (Figura 5.24), se ha desarrollado una aplicación móvil específica que fun-



**Figura 5.23:** Dispositivo Cosinuss Two

ciona como una puerta de enlace. Esta aplicación se comunica con los dispositivos Cosinuss utilizando el protocolo *Bluetooth Low Energy* (BLE) [190] para acceder a las mediciones recopiladas. Una vez que los datos son recogidos, la aplicación los transmite al SAS mediante el protocolo de mensajería AMQP. Esta operación asegura que la información sea enviada de forma eficiente al SAS, donde posteriormente puede ser procesada y visualizada en la SAP.



**Figura 5.24:** Flujo Datos Cosinuss

- **Cámaras de vídeo portátiles AXIS:** permite visualizar en tiempo real la operativa de los FRs que la portan. La cámara **AXIS M1045-LW** [191] se destaca por su bajo coste y excelente calidad de vídeo.

La cámara ofrece una amplia gama de resoluciones, desde *Full High Definition* (HD) 1920x1080 hasta 320x240, lo que permite su configuración y adaptación al entorno. En condiciones de ancho de banda suficiente, proporciona transmisión de vídeo en HD, mientras que en situaciones de ancho de banda limitado, ajusta automáticamente la resolución para asegurar la continuidad de la transmisión.

Una característica notable es su capacidad para utilizar diferentes algoritmos de compresión de vídeo, adaptándose así a condiciones de baja

## CAPÍTULO 5. CASO 2: ASSISTANCE

---

velocidad de conexión y garantizando una transmisión continua incluso en redes deficientes.

Además, la cámara tiene un bajo consumo de energía, lo que permite su operación con una pequeña batería externa durante horas, facilitando la movilidad completa de los FRs en sus tareas.



**Figura 5.25:** Cámaras AXIS

El flujo de vídeo de estas cámaras son enviadas por retransmisión RTSP al SAS y, por tanto, accesibles en tiempo real por el SAP. Además, todos los flujos de vídeo recopilados durante la operación se almacenan en el HDFS para ser consultados después del evento a través de su API dedicada.

- **Localización GPS:** para el posicionamiento de unidades sobre el terreno se utilizó el software de servidor GPS Traccar [192] autónomo y de código abierto, ya que admite una amplia gama de dispositivos GPS, tiene una API y puede configurar propiedades del cliente de forma remota a través de una interfaz web. Además, proporciona un cliente para teléfonos móviles tanto para Android [ ] como para iOS [ ], lo que amplía aún más los dispositivos GPS compatibles (Figura 5.26).

El propósito de la integración es enviar la localización GPS de los FRs a la base de datos del SAS, para ello se sigue el flujo de datos de la Figura 5.27.

Traccar, actúa como un concentrador que recibe y reenvía actualizaciones de ubicación. Estos datos son luego procesados por un intermediario denominado SAS *Forwarder*, que adapta y valida la información según el modelo de datos del Sensor SAS. Dependiendo de si la información pertenece a un nuevo recurso o a uno ya existente, el SAS *Forwarder* crea o actualiza estos recursos en el SAS, permitiendo que la información de ubicación sea almacenada y gestionada de manera centralizada para su posterior uso y análisis dentro del sistema.

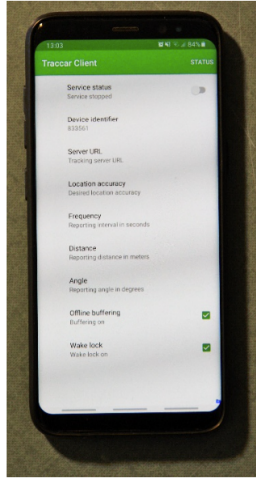


Figura 5.26: Aplicación Traccar

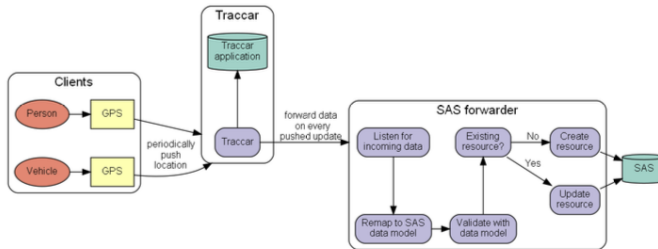


Figura 5.27: Flujo datos Traccar

### 5.3.3. Capa de red

La Capa de Red en la Arquitectura de ASSISTANCE se enfoca en garantizar una conectividad fiable y segura, esencial para la coordinación efectiva entre las unidades en el campo, los comandos operativos y los centros de mando y control a nivel táctico. La estrategia de comunicación de ASSISTANCE se cimienta en una red híbrida segura, diseñada para ofrecer una alta disponibilidad, especialmente en zonas remotas o en áreas donde las redes convencionales de comunicación no están disponibles o han sido interrumpidas debido a emergencias. Esta red híbrida es clave para proporcionar las tasas de datos y la baja latencia necesarias, soportando así una amplia gama de interacciones críticas

## CAPÍTULO 5. CASO 2: ASSISTANCE

y en tiempo real entre las unidades de campo y los centros de mando y control durante operaciones de misión crítica.

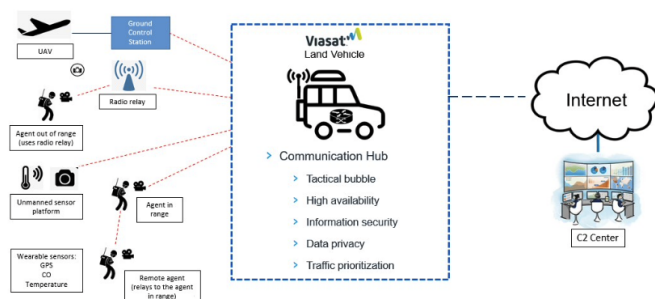


Figura 5.28: Arquitectura de Red ASSISTANCE

Esta sección detalla una descripción de la arquitectura de red de ASSISTANCE. Como se observa en la Figura 5.28 está conformada básicamente por tres elementos clave, la **Red Inalámbrica**, para conectar los FRs, UAVs y otros sensores con el **Centro de Comunicación**. El **Centro de Comunicación** es un vehículo estacionado que actúa como red de enlace, es decir, el nodo de comunicación que conecta la red de radio con el **Centro de Mando y Control** a través de Internet, que es la entidad que tiene una vista y control global de todos los componentes del proyecto ASSISTANCE.

### Red Inalámbrica

El objetivo principal de la Red de Inalámbrica en ASSISTANCE es asegurar la conectividad para los operadores de campo, como FRs, y para los UAVs y sensores no tripulados en zonas de operaciones remotas que están fuera del alcance de las redes de comunicación convencionales. Esta situación puede presentarse, por ejemplo, debido a la destrucción de infraestructuras como resultado de un desastre. La red también está diseñada para proporcionar conectividad de largo alcance y baja latencia a unidades tanto estacionarias como altamente móviles, esencial para misiones críticas en tiempo real.

Esta conectividad se logra mediante el despliegue de una *Mobile Ad Hoc Network* (MANET), que es autónoma y auto-reparable. La MANET [193] es crucial para proporcionar transmisión de vídeo, comunicación de voz, SA y el intercambio de datos sin depender de infraestructuras preexistentes. Se configura entre radios adaptadas para dispositivos portátiles de alta capacidad, que se llevan por los FRs y vehículos, así como en módulos más pequeños para una integración sencilla en sistemas no tripulados como UAVs y robots.





**Figura 5.29:** Terminales radio

Cada módulo de radio en esta red no solo transmite audio, sino que también es capaz de enviar múltiples transmisiones de vídeo de alta definición (con una tasa de 16 Mbps), y puede funcionar como un repetidor para otras radios dentro de su alcance. Esto crea una red de malla de radio con un amplio alcance, de hasta 20 km de línea de visión por salto de red. Los módulos de radio montados en los FRs y UAVs transmiten o retransmiten todos los flujos de datos hacia el centro de comunicación, que luego los dirigirá al centro de mando y control. Además, el centro de comunicación ofrece diversas interfaces de red para permitir conexiones de los usuarios finales a través de cables Ethernet o conexiones ópticas.

### Centro de Comunicación

El centro de comunicaciones actúa como el enlace entre la red inalámbrica y los centros de mando y control, utilizando para ello dos tipos de redes: la red de *Long Term Evolution* (LTE) [194] y la red por satélite.

Esta configuración dual permite que el centro de comunicaciones emplee la red LTE, que ofrece alta capacidad, en áreas donde esta cobertura está disponible. En situaciones donde la cobertura LTE no es accesible, lo cual es frecuente en los escenarios previstos por el proyecto ASSISTANCE, el sistema cambia automáticamente a la red por satélite.

La Figura 5.30 presenta un esquema detallado de la arquitectura de la red utilizada en ASSISTANCE, ilustrando cómo se integran estas diversas tecnologías para mantener la comunicación continua y efectiva en todas las circunstancias.

Con el fin de asegurar la confiabilidad y disponibilidad en diversos escenarios de red, se establecen dos túneles *Virtual Private Network* (VPN) independientes (uno a través de LTE y otro a través de enlace satélite) entre la Unidad de Equilibrio de Enlaces (Link Balancing Unit) ubicada en el centro de comunicaciones (vehículo) y el concentrador VPN alojado en un *Virtual Private*

## CAPÍTULO 5. CASO 2: ASSISTANCE

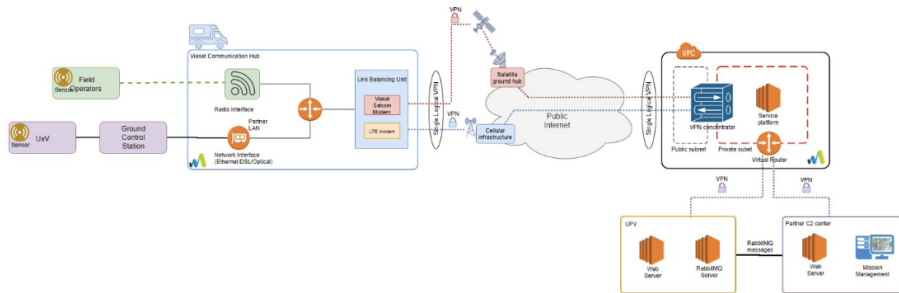


Figura 5.30: Esquema Red ASSISTANCE

*Cloud* (VPC) que termina los túneles VPN. La Unidad de Equilibrio de Enlaces y el concentrador VPN administran los túneles VPN para ofrecer conmutación activa/pasiva entre los dos enlaces (LTE y satélite). Los túneles VPN actúan como un único túnel VPN lógico al realizar conmutación por paquetes entre los enlaces. Esto implica que las sesiones establecidas se conservan en caso de un fallo en el enlace y no requieren ser restablecidas (conmutación con estado).

### Centro de Mando y Control

El *Command & Control* (C2) avanzado es la entidad que tiene una visión global y control de todos los componentes del sistema ASSISTANCE, lo que significa que es crucial que el intercambio de datos cumpla con requisitos estrictos de seguridad y latencia.

Esto se puede lograr estableciendo una conexión VPN de extremo a extremo entre el centro de C2 y el Centro de Comunicaciones. Cada socio de ASSISTANCE puede establecer una VPN con la VPC que permitirá el intercambio bidireccional de datos con los componentes remotos de ASSISTANCE (operadores de campo, UAVs, sensores).

En las implementaciones de los pilotos de ASSISTANCE, se dispone de dos tipos diferentes C2: el C2 avanzado y el C2 móvil.

Mientras que el C2 avanzado es un puesto fijo, el C2 móvil se desplegará en el campo y puede estar compuesto por varias tablets ruggedizadas que obtienen información directamente de sensores desplegados en el campo. Esta información se utiliza para tomar decisiones tácticas y también para proteger a las unidades desplegadas en el campo. Es posible que diferentes tipos de FRs tengan su propio C2 avanzado en el campo.



**Figura 5.31:** C2 móvil

### 5.3.4. Módulo SAS

#### Sistema de Recopilación de datos

El *Data Collection System* (DCS) dentro del SAS se encarga de la tarea fundamental de conectar con los sensores disponibles, empleando los distintos protocolos. Esto se logra mediante la suscripción a los temas específicos de cada sensor. Cada vez que se registra un cambio en los datos de un sensor, el DCS lo recopila y lo almacena en la base de datos del SAS. Posteriormente, todos los sistemas que estén suscritos a estos datos recibirán automáticamente las actualizaciones.

#### Sistema de entrega de datos

El *Data Distribution System* (DDS) se especializa en la distribución de los datos recogidos a los sistemas y aplicaciones correspondientes. Este sistema se adapta a los requerimientos y limitaciones de los sistemas receptores utilizando una variedad de protocolos y métodos de entrega. El DDS puede facilitar la transmisión de datos en tiempo real a través de WS, distribuir información en colas de mensajes o almacenar los datos en bases de datos que los sistemas receptores pueden consultar. Su función principal es asegurar una entrega de datos segura y fiable, permitiendo así el procesamiento y análisis eficiente por parte de los sistemas y aplicaciones destinatarios.

### 5.3.5. Intercambio de información entre diferentes módulos

En esta sección, se describen los patrones de intercambio de información dentro del sistema ASSISTANCE, se centra en la dinámica de comunicación entre los distintos módulos y subsistemas. Cada interacción específica entre dos entidades se define como un Servicio de Comunicación. Es importante destacar que todos los flujos de información en ASSISTANCE se centralizan a través del módulo de SAS. Este módulo juega un papel esencial en la estandarización del intercambio de datos, asegurando una comunicación coherente y uniforme entre los diversos módulos y subsistemas.

Los servicios de comunicación que se describen se alinean con el esquema ilustrado en la Figura 5.3. Este enfoque comienza con la recopilación de datos de los sensores y los recursos, como UxVs, vehículos y personas, realizada por el SAS. Luego, estos datos son distribuidos de manera eficiente a todos los sistemas que requieren esta información. Posteriormente, se detalla el intercambio bilateral de datos e información entre los demás módulos, proporcionando una visión integral de la interacción y la transferencia de datos dentro de la plataforma.

#### Servicios de Comunicación SAS

Los Servicios de Comunicación entre los sensores y el SAS se fundamentan en el uso del protocolo de publicación/suscripción para la recopilación de datos. Estos servicios se encargan de conectar los sensores disponibles, recibiendo y almacenando datos en la base de datos del SAS.

La información es luego distribuida a todos los sistemas suscritos, utilizando tecnologías como WebSockets, DDP y NATS para una transmisión eficiente en tiempo real. Además, la API REST permite operaciones CRUD, asegurando una gestión de datos flexible y accesible.

La Figura 5.32 muestra este flujo. Este flujo es en el que se basa todo el intercambio de información dentro de la plataforma.

Por último, en la Figura 5.33 se pueden observar los diferentes protocolos de comunicación entre Sensores-SAS y SAS y el resto de módulos.

#### Servicios de Comunicación SAP

El SAP recibe información de varios módulos de ASSISTANCE. Una entrada clave son las mediciones y flujos de vídeo de sensores montados en plataformas móviles o dispositivos portátiles, proporcionados por el SAS a través de suscripciones a WebSocket DDP/NATS en tiempo real o métodos API REST. Además, el SAP recibe datos de la *Chemical Hazard Tool* (CHT), que informa

### 5.3 Arquitectura de ASSISTANCE

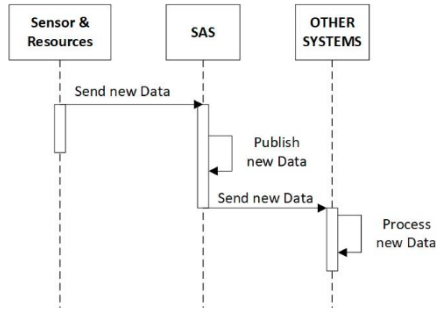


Figura 5.32: Flujo datos SAS

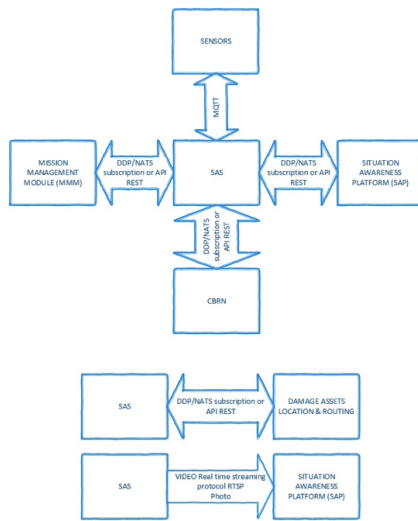


Figura 5.33: Comunicación SAS

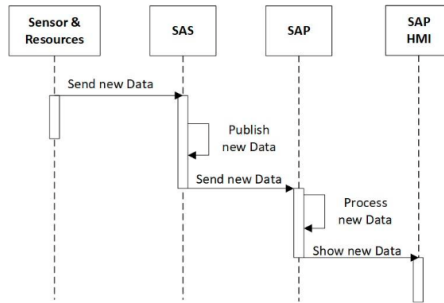
sobre la ubicación y evolución de nubes tóxicas, y del módulo DALR, proporcionando rutas óptimas y evacuaciones seguras.

La información fluye de manera bidireccional, donde los módulos pueden tanto recibir como enviar datos al SAP, permitiendo una interacción dinámica y un flujo de información constante.

## CAPÍTULO 5. CASO 2: ASSISTANCE

---

En la Figura 5.34 se muestra el flujo de datos de la SAP, como se puede observar añade una capa más a la vista en la Figura 5.32. Esta capa es la comunicación entre SAS y SAP tan pronto como se publican nuevos datos.

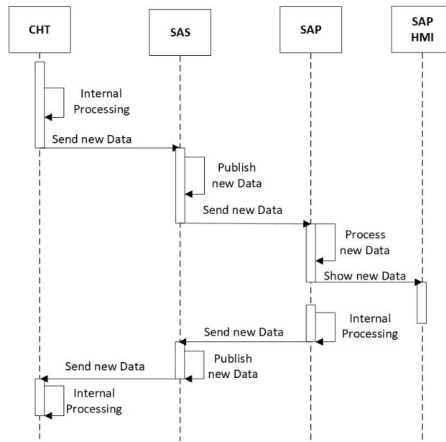


**Figura 5.34:** Comunicación SAP

### Servicios de Comunicación SAP-CHT

El CHT suministra al SAP información sobre la ubicación de nubes tóxicas detectadas, utilizando datos recopilados en el campo por sus operadores (como mediciones de sensores y detalles sobre sustancias tóxicas proporcionados por los FRs). A partir de esta información, el CHT generará alertas y señales de advertencia para los FR que puedan estar en riesgo. Estos datos del CHT se visualizarán en la interfaz de usuario del SAP. A su vez, el SAP enviará al CHT confirmaciones de recepción de estas alertas y, adicionalmente, proporcionará información sobre posibles puntos de interés identificados durante las operaciones, incluyendo su ubicación y descripción, como escuelas o gasolineras. Siguiendo el estándar de intercambio de datos en el sistema ASSISTANCE, toda esta información se transmitirá a través del SAS, asegurando así un medio homogéneo y eficaz para la transferencia de datos entre los diferentes módulos.

En el flujo de datos (Figura 5.35) se puede ver el carácter bidireccional de esta comunicación. Tan pronto como un nuevo dato esté listo en el CHT, se envía al SAS. El SAS publica automáticamente los nuevos datos recibidos y el SAP los recibe y, después de procesarlos, los mostrará a través de su interfaz de usuario principal. De la misma manera, cuando el SAP tenga nuevos datos disponibles para el CHT, se enviarán al SAS y el SAS los publicará automáticamente. El CHT los recibirá para su procesamiento interno.



**Figura 5.35:** Comunicación CHT

### Servicios de Comunicación SAP-DALR

El módulo DALR suministrará a la SAP rutas seguras para que los FRs accedan y evacuen zonas de emergencia. El SAP determina y envía al DALR un punto de origen y un destino, y como respuesta, el DALR calculará y proporcionará una ruta segura entre ambos puntos, incluyendo el tiempo estimado de recorrido. Adicionalmente, el SAP puede indicar al DALR un área específica delimitada por una polilínea. En estos casos, el DALR generará y proporcionará una o varias rutas para la evacuación de la zona indicada, junto con los tiempos estimados para cada una de estas rutas.

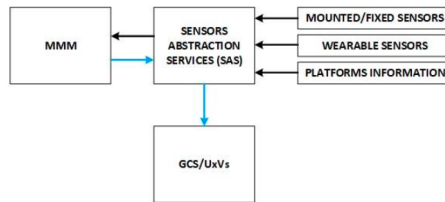
El flujo de datos es similar al de SAP-CHT, mostrado en la Figura 5.35.

### Servicios de Comunicación MMM

El MMM tiene la responsabilidad de diseñar y asignar las misiones y tareas a ser ejecutadas por los distintos UxVs.

Este módulo comunica sus datos e información a las Estaciones de Control Terrestre de los UxVs utilizando el SAS, siguiendo el mismo procedimiento que el resto de los módulos de ASSISTANCE.

Los datos de diferentes tipos de sensores, así como la información proveniente de plataformas no tripuladas, vehículos y personal, se canalizan hacia el SAS a través de interfaces lógicas preestablecidas. Una vez que esta información se encuentra disponible en el SAS y dependiendo de su tipo y características, dis-



**Figura 5.36:** Comunicación MMM

tintos tipos de datos de sensores y recursos se canalizan hacia el MMM (flechas negras Figura 5.36).

Considerando el escenario, los recursos disponibles y la información suministrada por el SAS, el MMM puede diseñar una misión específica y enviarla a los operadores de las GCS a través del SAS (flechas azules Figura 5.36).

### 5.4. Logros de ASSISTANCE

ASSISTANCE se propuso alcanzar un objetivo principal, brindar protección y asistencia a los FRs durante la mitigación de desastres de gran envergadura, ya sean naturales o provocados por el hombre, mediante el desarrollo de nuevas capacidades técnicas. Además, el proyecto se enfocó en mejorar la eficiencia y los tiempos de respuesta de los FRs en tales situaciones de desastre, optimizando así su capacidad para actuar de manera rápida y efectiva.

A lo largo del desarrollo del proyecto, el Consorcio se encontró con varios retos, como la pandemia de COVID-19 y el estallido del conflicto en Ucrania, lo que ocasionó una extensión de tres meses de la duración prevista del proyecto. Al concluir este periodo adicional, el Consorcio logró cumplir con todos los objetivos y desarrollos estipulados en el Acuerdo de Concesión, contribuyendo significativamente a la preparación de los FRs para futuras operaciones de emergencia y mejorando notablemente su seguridad. Los logros principales obtenidos durante el desarrollo de ASSISTANCE son los siguientes:

1. **Integración de UAVs y Robots en la SAP:** La integración de nuevas herramientas como robots y UAVs es crucial para FRs de la UE, especialmente en la era actual, donde la eficiencia y la seguridad son primordiales en la mitigación de desastres, ya sean naturales o provocados por el hombre.

Los UAVs, equipados con una variedad de sensores como cámaras, dispositivos de imágenes térmicas y escáneres LiDAR, no solo ofrecen imágenes



aéreas y monitorización desde posiciones elevadas, sino que también recopilan información crítica en tiempo real. Los robots, por su parte, se utilizan en entornos peligrosos o inaccesibles, equipados con capacidades de sensores remotos y manipulación de objetos. La integración de estos sistemas no tripulados en la SAP permite no solo recopilar datos desde múltiples perspectivas y ubicaciones, sino también visualizar y analizar estos datos en tiempo real a través de la interfaz de usuario de la plataforma.

ASSISTANCE eleva esta integración a un nivel superior, no limitándose a la inclusión de flujos de vídeo y telemetría de UAVs en la plataforma de SA, sino también innovando en el uso de UAVs de maneras que realmente asisten a los FRs. Esto incluye el despliegue de enjambres de UAVs para proporcionar cobertura de red en zonas con baja señal y el uso de UAVs capturadores para neutralizar amenazas aéreas hostiles.

Además, el uso de algoritmos avanzados y técnicas de procesamiento de datos facilita la extracción de conocimiento accionable de los datos recopilados, mejorando así la toma de decisiones y la coordinación de esfuerzos de respuesta.

### Enjambre de UAVs para proporcionar cobertura adicional



**Figura 5.37:** Puntos Acceso wifi integrado en UAVs

A lo largo del proyecto, se efectuó la integración de diversos puntos de acceso wifi en los UAVs y en la red de los FRs que fue desplegada. En las fases de prueba, se formularon y aplicaron varias estrategias para intercambiar UAVs durante las operaciones, garantizando así que los FRs mantuvieran una cobertura constante. Esta habilidad fue exitosamente

## CAPÍTULO 5. CASO 2: ASSISTANCE

---

comprobada en condiciones reales pero controladas, específicamente durante la simulación de un escenario de ataque terrorista, como parte de los pilotos del proyecto. La Figura 5.38 ilustra uno de los UAVs del enjambre (círculo rojo) que provee cobertura de red a una unidad policial en el proceso de seguimiento y captura de un terrorista (círculo azul) durante dicho escenario.



**Figura 5.38:** Operativa Enjambre UAVs

### UAV Captor:

Los UAVs también pueden ser utilizados para actividades criminales, como proporcionar información a terroristas en el campo durante un ataque o llevar explosivos. Los FRs, especialmente las fuerzas policiales, están preocupados por este hecho y la capacidad de captura de UAVs se ha considerado muy útil para su propia seguridad, ya que son posibles objetivos, además de aumentar su eficiencia contra este nuevo vector de ataque.



**Figura 5.39:** Captura UAV en Ejercicio Real

### Integración Robots

Los robots también se integraron en la plataforma de SA para realizar tareas peligrosas como abrir mochilas potencialmente peligrosas o detonar amenazas, así como proporcionar información valiosa a FRs y comandantes de emergencia.

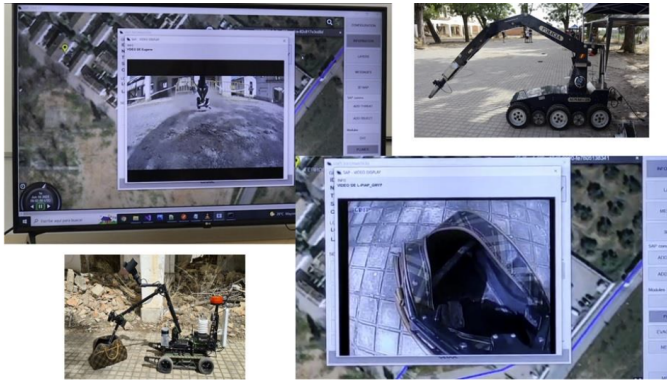


Figura 5.40: Operativa Robots

2. **Mejora de la operativa en campo:** Uno de los logros más destacados ha sido la dotación de tablets ruggedizadas a los diferentes cuerpos de emergencias. Este avance ha significado una mejora sustancial en la SA de los equipos en terreno. Estas tablets, diseñadas para soportar las condiciones más adversas, han permitido a FRs no solo mantener una comunicación fluida y efectiva con el puesto de mando y control, sino también operar con un grado mayor de independencia.

Con estos dispositivos, los equipos en campo tienen acceso directo a información crucial en tiempo real, como la ubicación de las unidades, imágenes de video en vivo y datos críticos del entorno operativo. Además, una funcionalidad clave incorporada en estas tablets es la capacidad de lanzar y controlar misiones de UAVs directamente desde el dispositivo. Esto no solo agiliza la respuesta en situaciones críticas, sino que también potencia la autonomía de los equipos en la toma de decisiones rápidas y fundamentadas. Esta integración tecnológica ha demostrado ser un elemento transformador en la eficiencia y efectividad de las operaciones de emergencia, proporcionando a los FRs una herramienta para la gestión y mitigación de situaciones de crisis.



**Figura 5.41:** Operativa Tablet en Campo

- 3. HMIs inteligentes:** se destaca el desarrollo e implementación de interfaces avanzadas para la interacción con las diversas herramientas y sensores que conforma el sistema ASSISTANCE. Estas interfaces representan un salto cualitativo en términos de SA para los equipos en acción.

La inteligencia de estas interfaces se manifiesta en su capacidad para procesar y presentar información crítica de manera intuitiva, facilitando así una toma de decisiones rápida y fundamentada. Algunas de estas herramientas con sus respectivos interfaces se presentan a continuación:

### **Plumas Tóxicas y medidas de Gas**

Para proporcionar información a los FRs sobre sustancias potencialmente peligrosas en el aire durante operaciones de emergencia, ASSISTANCE integra un módulo capaz de proporcionar nubes tóxicas con información recopilada de sensores en el campo y fuentes externas de información. Estas nubes pueden ser solicitadas por los FRs en el campo a través de sus tablets o desde la sala de control.

Para las medidas de gases tóxicos se integraron sensores de gas en UAVs y robots para proporcionar información en tiempo real a los FRs y comandantes de emergencia sobre la toxicidad del punto caliente. De esta manera, si se detectan valores peligrosos de un gas tóxico, los FRs son informados en tiempo real para permitir su rápida evacuación o el uso del equipo adecuado.

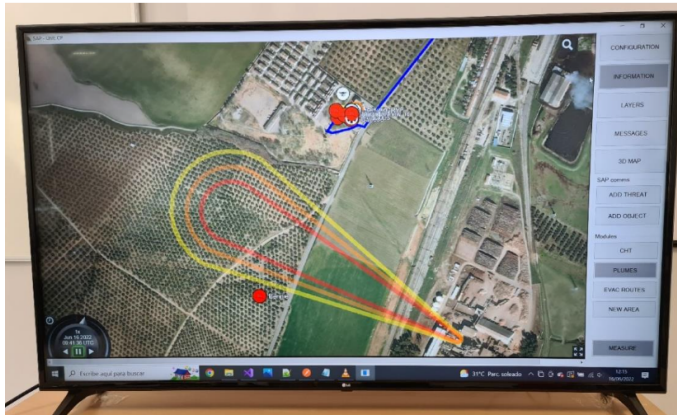


Figura 5.42: Pluma tóxica

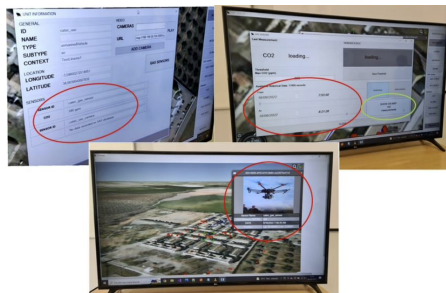


Figura 5.43: Sensores de gas

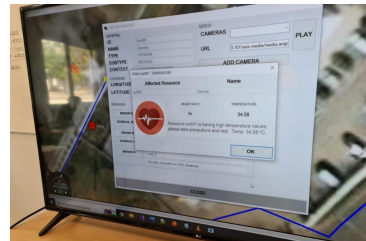
### Integración con Wearables

Los *Wearables* se han integrado en el sistema para proporcionar información en tiempo real sobre la ubicación de los FRs (Figura 5.44), la frecuencia cardíaca, la temperatura corporal y los flujos de vídeo en tiempo real de las cámaras portátiles. En cuanto a las constantes vitales de los FRs, se ha añadido un mecanismo de seguridad adicional, ya que si se superan los umbrales seleccionados para la frecuencia cardíaca o la temperatura, el sistema muestra aviso (Figura 5.45).

## CAPÍTULO 5. CASO 2: ASSISTANCE



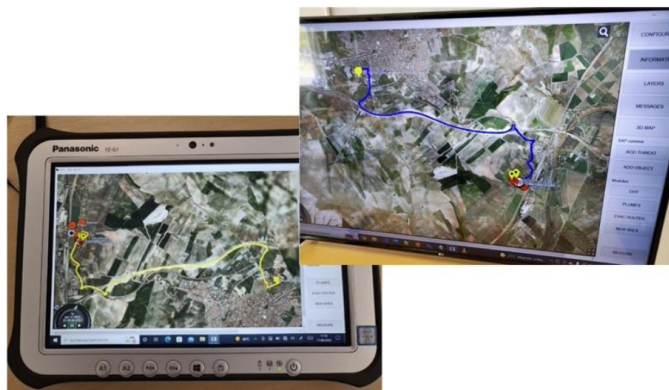
**Figura 5.44:** Posicionamiento Unidades



**Figura 5.45:** Frecuencia Cardiaca Unidad

### Rutas de Evacuación

Los FRs pueden solicitar una ruta segura de evacuación en cualquier momento para evacuar a las víctimas e incluso para evacuar a los FRs del área peligrosa. Estas rutas seguras evitan áreas potencialmente tóxicas o activos dañados, como carreteras o puentes, con el fin de garantizar que la evacuación siga una ruta segura hasta un refugio seguro. Algunas de las rutas solicitadas durante los ejercicios de los pilotos se muestran en la Figura 5.46



**Figura 5.46:** Rutas de Evacuación

4. **Validación de simulaciones de escenarios de emergencia:** un logro significativo ha sido la demostración exitosa de varios casos de uso, los cuales han jugado un papel crucial en la validación y mejora de las herramientas y estrategias desarrolladas. Estos casos de uso, diseñados

para simular situaciones de emergencia reales, han permitido a los equipos de emergencia y a los operadores del sistema de mando y control poner a prueba en condiciones controladas las capacidades operativas y la eficiencia de las soluciones propuestas por ASSISTANCE. Cada caso de uso presentado abarcó distintos escenarios de emergencia, desde desastres naturales hasta situaciones de seguridad pública, como ataques terroristas. Estas simulaciones permitieron no solo evaluar la funcionalidad y la robustez de las herramientas y sistemas desarrollados, sino también la efectividad de los protocolos operativos y los HMIs en diferentes contextos. En el Capítulo 6 se detalla las distintas demostraciones realizadas para cada caso de uso.





## Capítulo 6

# Evaluación

Para verificar la viabilidad de la arquitectura propuesta en el Capítulo 3, se procedió a implementarla dentro del marco de los dos proyectos de investigación descritos en los Capítulos 4 y 5. Tras el diseño y desarrollo detallado en dichos proyectos, el siguiente paso consiste en la rigurosa evaluación de los resultados obtenidos.

Durante el capítulo se describirá en las diferentes secciones el contexto y los escenarios específicos en los que se han llevado a cabo las pruebas para cada caso de uso. Posteriormente, se detallará el procedimiento operativo adaptado a las circunstancias de cada escenario. Y finalmente, se analizarán los datos recabados, poniendo especial énfasis en medir la eficiencia y el impacto de las soluciones implementadas.

Cabe destacar que en el caso del proyecto MAGNETO, dedicado a la IC, las evaluaciones se condujeron mediante demostraciones simuladas y ejecutadas de manera remota. Este enfoque fue una respuesta directa a las restricciones impuestas por la pandemia de COVID-19, lo cual planteó el desafío significativo de realizar todas las pruebas sin interacción física. A pesar de estas limitaciones, se pudo garantizar la continuidad y la calidad del proceso de evaluación y se pudo proporcionar una visión global de todas las actividades realizadas a lo largo del proyecto.

Por otro lado, en el proyecto ASSISTANCE, se logró llevar a cabo el despliegue de los desarrollos en entornos controlados y simulados en terreno, lo que permitió una evaluación más tangible y contextualizada de las aplicaciones en situaciones de emergencia. Estos escenarios más realistas facilitaron una valoración integral de la funcionalidad y la operatividad de las herramientas y sistemas desarrollados.

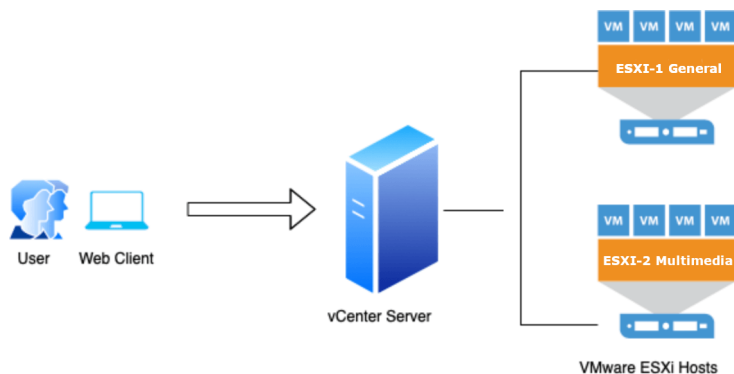
### 6.1. MAGNETO

#### 6.1.1. Escenario de pruebas

La evaluación de la factibilidad y la viabilidad de la plataforma se ha llevado a cabo mediante el prototipo de la arquitectura diseñada en el Capítulo 3 y adaptada al proyecto MAGNETO cuya arquitectura final se ha definido en el Capítulo 4. El escenario seleccionado para las pruebas es un ejercicio de simulación de un ataque extremista a una Infraestructura Crítica en una zona residencial de Múnich, Alemania. Para realizar la demostración, se ha efectuado el despliegue integral de los servicios de MAGNETO en el *CLOUD* proporcionado por la UPV. En este *CLOUD* se establecieron dos nodos clave que permiten a las entidades implicadas en el simulacro compartir y intercambiar información relevante al ataque y las condiciones actuales del entorno, garantizando así una operativa coordinada y una respuesta ágil frente a la situación simulada.

#### Despliegue

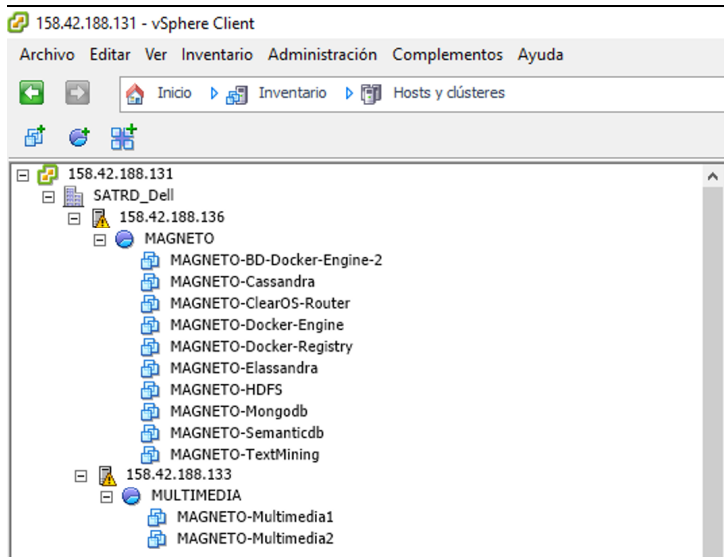
Toda la infraestructura se llevó a cabo dentro de dos servidores alojados en la Universidad y se virtualizaron todas las máquinas y servicios para proporcionar un entorno lo más aislado posible, evitando así cualquier tipo de intrusión o acceso a información restringida que aun siendo simulada contenía modos operandi y datos que podrían considerarse sensibles. La virtualización se llevó a cabo dentro del entorno de VMware vSphere [195] con dos servidores ESXI [196] siguiendo la configuración que se puede observar en la Figura 6.1.



**Figura 6.1:** Entorno de virtualización VMware

Dentro de la configuración propuesta se pueden encontrar dos servidores, el principal (ESXI-1) se dedicó al alojamiento de todos los servicios generales de

la plataforma MAGNETO en el que se desplegaron una serie de máquinas virtuales que veremos con detalle más adelante. Con respecto al segundo servidor (ESXI-2), se dedicó exclusivamente al procesamiento de información multimedia (flujos de vídeo en *streaming* procedentes de CCTV), la división se tuvo que realizar de esta forma, ya que el ESXI-2 disponía de un *Cluster* de *Graphics Processing Unit* (GPU)s que se utilizaban para la ejecución de los diferentes algoritmos de ML dedicados al procesamiento de imágenes y vídeo.



**Figura 6.2:** Detalle de las máquinas virtuales en los servidores

Más en detalle, la Figura 6.2 muestra la distribución de máquinas virtuales que se utilizaron tanto para las últimas actividades de la fase de integración, así como durante las diferentes actividades de validación, *testing* y demostración. En la imagen se puede observar primero que en el servidor .136 se alojaron dentro del espacio de trabajo MAGNETO 10 máquinas virtuales y después en el servidor .133 dentro del espacio de trabajo MULTIMEDIA se alojan 2 máquinas virtuales adicionales.

A continuación se especifican los servicios y recursos asignados a cada una de las máquinas, así como las funcionalidades que pretenden cubrir dentro del piloto de pruebas.

#### Servidor ESXI-1

- **MAGNETO-ClearOS-Router:** Basada en la distribución GNU/Linux ClearOS [197] con raíces en CentOS [198], actúa como un router virtual

avanzado. Su funcionalidad principal es gestionar el tráfico de la red de MAGNETO. Entre sus responsabilidades clave está la asignación dinámica de direcciones IP a través de un servidor *Dynamic Host Configuration Protocol* (DHCP) [199] para las diversas máquinas virtuales hospedadas en los servidores ESXI. Además, facilita la resolución de nombres de dominio para cada servidor mediante un servidor *Domain Name System* (DNS) [200] integrado, asegurando así una navegación fluida y eficiente dentro de la infraestructura de MAGNETO.

- **MAGNETO-Cassandra:** Encapsula el motor de base de datos NoSQL Cassandra, especializado en el manejo de datos tabulares y orientados a columnas. Elegido por su robustez y escalabilidad, Cassandra se adapta perfectamente al almacenamiento y procesamiento de volúmenes masivos de datos. Con su arquitectura basada en el modelo de clave-valor, garantiza un rendimiento excepcional incluso bajo las cargas de trabajo más intensas, siendo una pieza angular para la gestión de datos dentro del ecosistema MAGNETO.
- **MAGNETO-Elassandra:** Combina la potencia del motor de búsqueda y análisis de Elasticsearch con la escalabilidad y resiliencia de Cassandra en una única solución integrada. Elassandra [201] aprovecha la eficiente gestión de datos de Cassandra y la búsqueda flexible y rápida de Elasticsearch para ofrecer una plataforma optimizada para búsquedas complejas y análisis en tiempo real de grandes volúmenes de información, lo que la hace ideal para aplicaciones de análisis forense y de inteligencia en el ámbito de la seguridad pública.
- **MAGNETO-Mongoddb:** Proporciona el motor de base de datos MongoDB, una plataforma NoSQL orientada a documentos que proporciona alta performance, alta disponibilidad y fácil escalabilidad. Con su modelo de datos flexible y su arquitectura basada en documentos, MongoDB es especialmente adecuada para manejar estructuras de datos complejas y heterogéneas, como las que se encuentran en la IC, donde se pueden integrar y consultar rápidamente una variedad de tipos de datos y formatos.
- **MAGNETO-Semanticdb:** Basada en Apache Jena Fuseki, que es un servidor de base de datos semántica que proporciona capacidades avanzadas de almacenamiento y consulta para datos estructurados siguiendo los estándares de la web semántica, incluyendo RDF, SPARQL y OWL. MAGNETO-Semanticdb está diseñado para permitir consultas complejas y razonamiento lógico sobre datos, facilitando la detección de patrones y relaciones ocultas en la información, lo que resulta crucial en la investigación de crímenes y análisis de inteligencia.

- **MAGNETO-HDFS:** Sistema de archivos distribuidos de alta disponibilidad y alta tolerancia a fallos utilizado por Hadoop, conocido como HDFS. En MAGNETO, HDFS se utiliza para almacenar, procesar y analizar grandes conjuntos de datos de manera eficiente en un entorno distribuido. Su arquitectura permite el manejo de grandes volúmenes de información procedentes de diversas fuentes, lo cual es esencial en escenarios de IC donde el volumen de datos puede ser extremadamente grande.
- **MAGNETO-Docker-Registry:** Es el repositorio central para el almacenamiento y la gestión de imágenes de Docker dentro del ecosistema MAGNETO. Actúa como un punto de control clave para la distribución y almacenamiento seguro de contenedores, facilitando el acceso y la reutilización de imágenes de aplicaciones y servicios. En el contexto de MAGNETO, Docker Registry juega un papel crucial en la gestión eficiente de los recursos de la plataforma, asegurando que las imágenes de los contenedores sean fácilmente accesibles y estén correctamente versionadas. Esto contribuye a la eficacia y la eficiencia en el despliegue y la actualización de las aplicaciones de la plataforma.
- **MAGNETO-Docker-Engine:** Primer nodo de la plataforma de contenedores Docker Engine, que facilita la creación y manejo de contenedores de Docker. En el entorno de MAGNETO, Docker Engine [202] es utilizado para encapsular y distribuir aplicaciones y servicios de la plataforma, permitiendo una fácil replicación y escalabilidad. Esto posibilita un despliegue ágil y consistente de las aplicaciones necesarias para la IC, mejorando la interoperabilidad y el intercambio de herramientas entre diferentes entidades y sistemas.
- **MAGNETO-BD-Docker-Engine-2:** Segundo nodo para la creación y manejo de contenedores Docker. Se utiliza dentro de MAGNETO como nodo secundario para correr contenedores y proporcionar alta disponibilidad y balanceo de carga en la ejecución de tareas.
- **MAGNETO-TextMining:** Conjunto de herramientas dedicadas al procesamiento y análisis de texto dentro del ecosistema MAGNETO. Utiliza técnicas avanzadas de minería de texto para extraer información relevante y patrones de grandes conjuntos de datos textuales, como informes de incidentes, comunicaciones interceptadas y bases de datos de inteligencia. Este componente es esencial para identificar tendencias, correlaciones y para ayudar en la construcción de perfiles relacionados con la IC.

Como se puede observar, el servidor ESXI-1 que virtualiza la gran mayoría de los servicios de MAGNETO por lo que disponía de unas especificaciones

## CAPÍTULO 6. EVALUACIÓN

---

técnicas de alto rendimiento para poder llevar a cabo las tareas de las diferentes máquinas virtuales.

- **Equipo:** PowerEdge T640 Server [203]
- **Procesador:** 2x Intel Xeon Gold 5120, 2.2GHZ, 14 núcleos/28 procesos
- **RAM:** 128GB, 2666 MT/s, bloque doble
- **Almacenamiento:** 12TB SAS nearline a 12Gb/s 7,2K rpm

### Servidor ESXI-2

- **MAGNETO-Multimedia1** Esta instancia está especializada en el procesamiento y análisis de flujos de vídeo en tiempo real. Cuenta con una GPU asignada que facilita la ejecución de tareas intensivas de visión por computadora, como la detección y reconocimiento de objetos en secuencias de vídeo procedentes de cámaras de vigilancia CCTV o archivos multimedia. Su capacidad para manejar y analizar vídeo en vivo la hace una herramienta clave para la vigilancia y monitorización.
- **MAGNETO-Multimedia2** De igual forma que Multimedia1, esta máquina virtual se dedica al análisis de flujos de vídeo y también está equipada con una GPU para el procesamiento intensivo de gráficos. Se utiliza para la extracción automatizada de metadatos y análisis de contenido en vídeos, lo que permite identificar patrones, movimientos anómalos y otros elementos de interés que contribuyen significativamente a las investigaciones y respuestas operativas en situaciones críticas.

Para la parte de *streams* de vídeo en tiempo real, el servidor ESXI-2 disponía de dos máquinas virtuales que repartían la carga de procesamiento cada una a una tarjeta gráfica. Para este caso, la configuración del equipo además debía priorizar la escritura en disco, por lo que se utilizaron discos duros de estado sólido de alto rendimiento con las especificaciones que siguen.

- **Equipo:** Fujitsu Primergy TX2560 M2 [204]
- **Procesador:** 2x Intel Xeon E5-2620V4, 2.1GHZ, 8 núcleos/32 procesos
- **RAM:** 128GB, 2666 MT/s, bloque doble
- **Almacenamiento:** Samsung 870 EVO SSD 2.5 4TB 16Gb/s
- **GPU:** 2x Nvidia RTX 2080Ti OC Edition (11GB, GDDR6)

### Actores y Fuentes de datos

En el escenario a cubrir, varios actores juegan un papel crucial en la investigación del ataque a una infraestructura crítica. Estos incluyen testigos, sospechosos y personal de la policía.

Actor	Descripción
Testigos	Personas que presenciaron el incidente y proporcionaron informes clave.
Sospechosos	Individuos identificados o sospechados de estar involucrados en el ataque.
Personal de Policía	Oficiales y detectives a cargo de la investigación del caso.

**Tabla 6.1:** Actores Involucrados en la investigación

Para resolver el caso, se utilizaron varios datasets, incluyendo informes de testigos, registros de vehículos, análisis de CCTV y otros datos relevantes.

Dataset	Descripción
PPM_dataset_01	Informe de testigo (Isabell Gampel).
PPM_dataset_02	Informe de testigo (Desmire Altmann).
PPM_dataset_03	Solicitud de información al Registro Federal de Vehículos.
PPM_dataset_04	Informe de accidente de tráfico.
PPM_dataset_05	Solicitud de información al Registro de Residencia de Múnich.
PPM_dataset_06	Informe de testigo de agente de seguridad privada.
PPM_dataset_07	Material de CCTV.
PPM_dataset_08	Evaluación de teléfono y base de datos policial interna.
PPM_dataset_09	Solicitud de información al Registro de Residencia (Calle Schopenhauer).
PPM_dataset_10	Informe de interrogatorio.
PPM_dataset_11	Informe final de investigación.

**Tabla 6.2:** Datasets Utilizados en la investigación

### Contexto pre-incidente

El escenario propuesto para la evaluación de la plataforma MAGNETO se centra en un ataque extremista hipotético que tiene como objetivo infraestructuras críticas en la ciudad de Múnich, Alemania. Este simulacro está diseñado

## CAPÍTULO 6. EVALUACIÓN

para replicar la complejidad y urgencia de una situación de emergencia real, poniendo a prueba la capacidad de las agencias de respuesta y las tecnologías involucradas para actuar de manera eficaz y coordinada.

El ataque ficticio se describe como una serie de eventos meticulosamente orquestados que desembocan en el sabotaje de un elemento vital de la red de telecomunicaciones. Con el trasfondo de una tranquila mañana de invierno, el estallido de la violencia irrumpe inesperadamente, sacudiendo la rutina diaria de la ciudad. Las fuerzas de seguridad y los equipos de emergencia se ven inmediatamente sumidos en una carrera contra el tiempo, enfrentando el caos que se despliega en las calles y la incertidumbre de posibles ataques secundarios.

En los momentos siguientes al incidente inicial, la ciudad experimenta una cascada de llamadas de emergencia, informes de testigos y alertas de seguridad, cada una añadiendo piezas al rompecabezas de la crisis en curso. La rápida identificación de un vehículo sospechoso y la verificación de pistas sobre posibles complicidades emergen como prioridades en la investigación, revelando la esencia de un desafío que es tanto operativo como analítico.

Este escenario se propone no solo como una prueba de estrés para los sistemas y procesos existentes, sino también como un campo de pruebas para innovaciones en el análisis de datos y la GE, subrayando la importancia de la preparación y la adaptabilidad en un mundo cada vez más conectado y complejo.

### 6.1.2. Caso de uso: Investigación en el ataque de una Infraestructura Crítica

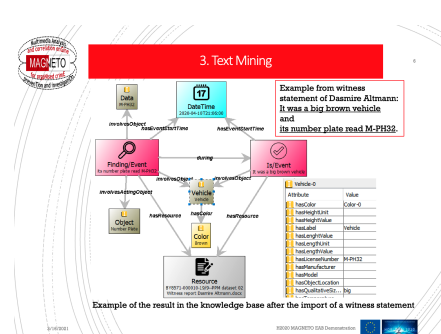


**Figura 6.3:** Caso de uso propuesto por el Departamento de Policía de Múnich



El Departamento de Policía de Múnich se enfrentó a una grave amenaza el viernes por la noche cuando varios testigos informaron de una explosión en el sur de la ciudad. La investigación reveló que un mástil de telecomunicaciones 5G había sido dañado por un pequeño artefacto explosivo. La escena del crimen fue asegurada y se procedió a recopilar pruebas mientras se interrogaba a los testigos con los reportes policiales que se pueden observar en la Figura 6.4.

Un testigo, la Sra. Gampel, estaba paseando a su perro cerca del mástil cuando observó a una persona en sudadera y jeans negros salir del recinto. La atención de la Sra. Gampel se captó debido a que la persona no vestía uniforme oficial y se alejó en un *Sports Utility Vehicle* (SUV) marrón sin cerrar la puerta tras él. Después de la explosión, el hombre huyó del lugar en su vehículo.



**Figura 6.4:** Ejemplo de informes policiales introducidos en el módulo de *TextMining*

**Figura 6.5:** Resultados generados por el módulo *TextMining-Result*

La Sra. Altmann, una segunda testigo, informó haber visto un vehículo BMW marrón a alta velocidad saliendo de la zona de la explosión y pudo identificar las primeras letras y números de la matrícula: M-PH32. Esta información fue crucial para solicitar datos al Registro Federal de Vehículos, que condujo a dos posibles propietarios. Uno fue descartado debido a un accidente de tráfico, mientras que el segundo, Andreas Baader, resultó estar de vacaciones, lo que indicó que su coche fue utilizado sin su consentimiento.

Mientras tanto, se recibieron llamadas adicionales sobre intentos de acceso a otro mástil de telecomunicaciones. El sospechoso huyó al ser descubierto, dejando atrás una mochila con materiales explosivos y se informó que escapó en un SUV marrón. El seguimiento de las cámaras de CCTV y las medidas operativas llevadas a cabo por la policía en civil permitieron localizar y arrestar al sospechoso, Hans Fuchs, conocido extremista de izquierda, en su apartamento

## CAPÍTULO 6. EVALUACIÓN

en el norte de Múnich. La Figura 6.6 muestra las capacidades de la plataforma y un ejemplo de detección en un flujo CCTV.



Figura 6.6: Ejemplo de detección por medio del módulo *FaceRecognition*

El análisis del teléfono del sospechoso, junto con la búsqueda en su apartamento, reveló contactos con otros extremistas y evidencia financiera y digital que vinculaba a Fuchs con los ataques. Los resultados del análisis se pueden observar de forma gráfica en la Figura 6.7

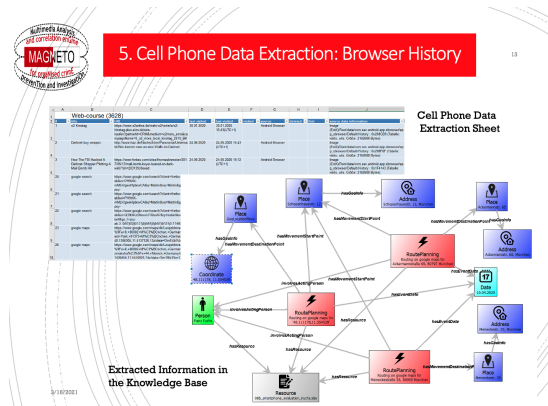


Figura 6.7: Resultados del módulo de extracción de datos de *Smartphones*

A pesar de su falta de cooperación durante los interrogatorios, la acumulación de pruebas que se pueden observar en la representación gráfica de la

ontología generada en la Figura 6.8 y los resultados obtenidos del módulo de razonamiento semántico fueron suficientes para confirmar su culpabilidad.

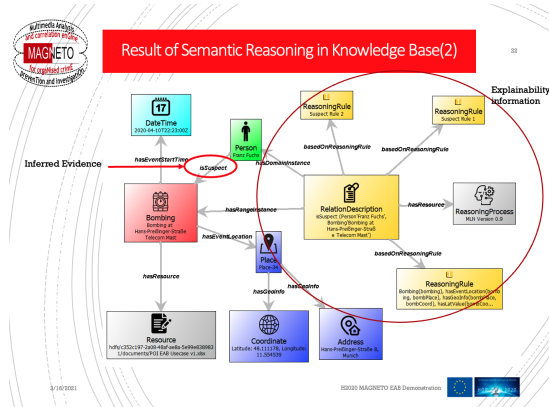


Figura 6.8: Resultados del módulo de análisis semántico

### Metodología en la Investigación

- **Recopilación de Testimonios:** Se recopilaron informes de testigos y se procesaron en la plataforma MAGNETO.
- **Análisis de Texto:** Se empleó la minería de texto para extraer datos clave de los informes de testigos y solicitudes de registro.
- **Reconocimiento de Matrículas:** Se analizaron las grabaciones de CCTV para identificar el vehículo del sospechoso.
- **Evaluación de Datos de Teléfono Móvil:** Se examinó el teléfono del sospechoso para corroborar su presencia en la escena del crimen y sus comunicaciones.
- **Fusión de Datos:** Se integraron diversas fuentes de datos para rastrear los movimientos del sospechoso.
- **Razonamiento Semántico:** Se aplicaron reglas semánticas para formular hipótesis y llegar a conclusiones basadas en la evidencia recopilada.

A través de estos métodos, la plataforma MAGNETO demostró su capacidad para facilitar una investigación eficiente y efectiva, subrayando la importancia de una integración tecnológica avanzada en la respuesta policial moderna.

## CAPÍTULO 6. EVALUACIÓN

### 6.1.3. Demostraciones

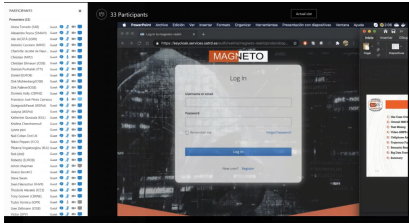
Durante la primera mitad del año 2021 y para demostrar el correcto funcionamiento de la plataforma MAGNETO se realizaron diferentes demostraciones para evaluar primero la plataforma de forma interna por los usuarios finales que formaban parte del consorcio MAGNETO. Una vez ajustados los escenarios y las diferentes historias a contar durante las demostraciones, se atendieron una serie de eventos, entre los cuales cabe destacar la demostración final realizada a la Comisión Europea, así como a las demostraciones realizadas a los *External Advisory Boards*, la *UN Office of Counter-Terrorism* [205], el *i-LEAD Research Day* [206] o el *The Internet Investigation Online Event* del European Network of Law Enforcement Technology Services (ENLETS) [207], entre otros. La Figura 6.9 muestra algunos de los eventos mencionados.



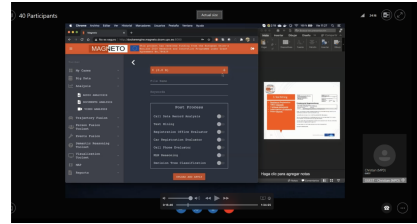
**Figura 6.9:** Eventos en los que se demostró la plataforma MAGNETO

En estas demostraciones 100% remotas, se revisaron las funcionalidades principales de la plataforma, así como su estabilidad y capacidad a la hora de ingestar grandes cantidades de datos. Además, se pudo comprobar como diferentes investigadores podían estar conectados a la plataforma MAGNETO se les permitía el acceso a casos de investigación específicos, con roles que permitían realizar unas actividades u otras. Las Figuras 6.10 y 6.11 muestran el acceso a la plataforma y los diferentes tipos de análisis que se podían realizar.

Otra de las funcionalidades de la plataforma que más interés generaron durante las demostraciones fueron la capacidad de identificación de matrículas a

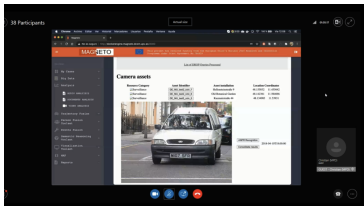


**Figura 6.10:** Pantalla de acceso a la plataforma

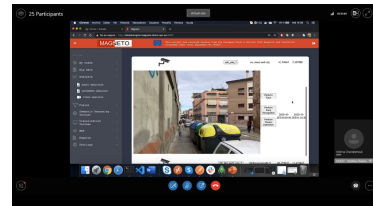


**Figura 6.11:** Lista de análisis a ejecutar

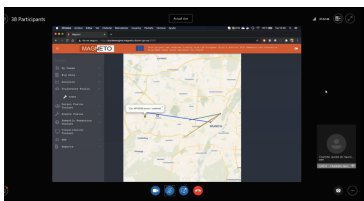
través de flujos de vídeo de CCTVs como se puede observar en la Figura 6.12, La identificación de personas también de flujos de vídeo de CCTVs como se muestra en la Figura 6.13, o el resultado de los análisis de fusión de trayectorias en la Figura 6.14, y la generación de puntos calientes identificados tras la ejecución de análisis de TextMining como vemos en la Figura 6.15.



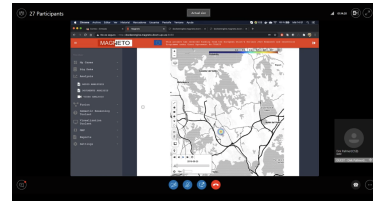
**Figura 6.12:** Análisis de reconocimiento de matrículas



**Figura 6.13:** Análisis de detección de personas



**Figura 6.14:** Análisis de fusión de trayectorias



**Figura 6.15:** Representación de resultados de *hotspots*

Estos son solo algunos de los ejemplos de los diferentes análisis y funcionalidades que se abordaron a lo largo de las diferentes demostraciones realizadas a los cuerpos de seguridad e investigadores policiales para validar las capacidades de la plataforma MAGNETO.

### 6.2. Valoración de los usuarios finales

La sección de valoración de los usuarios finales reveló una perspectiva generalmente positiva hacia las funcionalidades del sistema MAGNETO, destacando particularmente la utilidad del aprendizaje automático continuo y las capacidades analíticas del sistema. A continuación, se presenta la tabla de valoración actualizada que incluye una columna de valoración neutral, tal como se solicitó:

Funcionalidad	Valoración Positiva	Valoración Neutral
Aprendizaje continuo de IA	X	-
Evaluación de riesgos	X	-
Análisis de texto	X	-
Reconocimiento de imágenes	X	-
Análisis de vídeo	-	X
Dashboard para análisis	X	-

**Tabla 6.3:** Tabla de valoración de los usuarios finales

Esta tabla refleja un análisis más matizado de las opiniones de los usuarios, permitiendo un margen para aquellos aspectos del sistema que quizás no fueron calificados de forma tan polarizada como ‘positiva’ o ‘negativa’, sino que se sitúan en un término medio, indicativo de un potencial de mejora o de un rendimiento que cumple las expectativas, pero no las supera notablemente.

Se observó que la herramienta de análisis de vídeo requería mejoras, sugiriendo también la necesidad de anonimización de rostros en imágenes y vídeos para cumplir con la protección de datos. Los usuarios apreciaron la capacidad de integración de datos estructurados con otras aplicaciones utilizadas en el análisis, aunque se mencionó que las herramientas de visualización requerían de mayor claridad.

En resumen, el sistema MAGNETO ha demostrado ser prometedor y, aunque se encuentra en una etapa inicial y requiere de mejoras continuas al tratarse de un prototipo que has salido de un proyecto de I+D, tiene el potencial de reforzar significativamente el trabajo de las agencias encargadas en actividades de IC.

### 6.3. ASSISTANCE

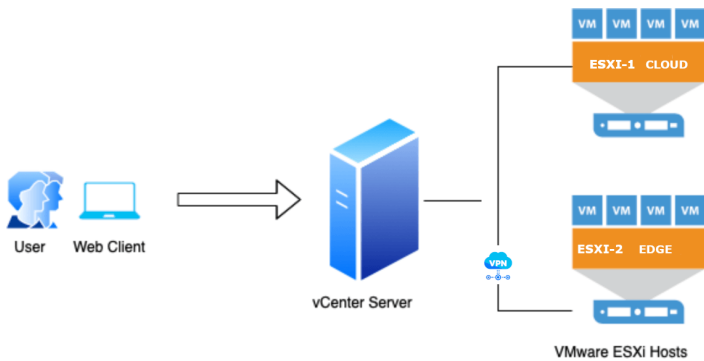
#### 6.3.1. Escenario de pruebas

Al igual que durante la última fase del proyecto MAGNETO en ASSISTANCE se realizó la evaluación de la factibilidad y la viabilidad de la

plataforma a través del prototipo de arquitectura diseñado en el Capítulo 3 y adaptado al proyecto ASSISTANCE cuya arquitectura final se ha definido en el Capítulo 5. En este caso, debido a la diversidad de escenarios en los que se puede utilizar el prototipo desarrollado, se diseñaron 3 escenarios de pruebas en los que demostrar todas las capacidades que la plataforma ofrece. El primero en la ciudad de **Izmir** en Turquía, donde se realizó la simulación de las actividades de respuesta tras un terremoto de primer grado con víctimas en diferentes estados. El segundo en la ciudad de **Róterdam**, en los Países Bajos, en el que se simuló un incendio dentro de una planta petroquímica donde se manejan infinidad de sustancias perjudiciales para la salud. Por último, el tercero en la ciudad de **Linares**, en España, donde se simula un incidente terrorista con varios implicados aprovechando que son días festivos y hay miles de turistas.

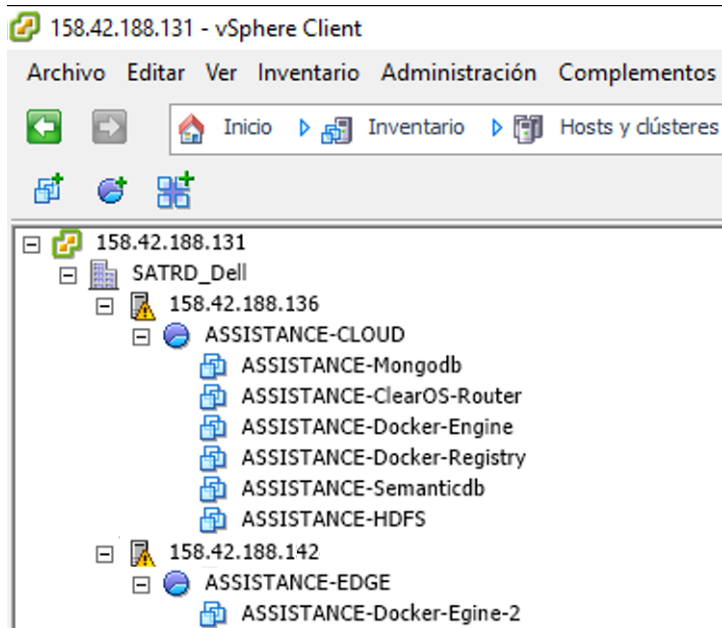
### Despliegue

En contraposición al despliegue que se hizo en MAGNETO donde el 100 % de los servicios se alojaban virtualizados dentro de una serie de servidores en la infraestructura de la Universidad, en este caso se optó por una solución híbrida donde parte de los servicios de ASSISTANCE (los menos críticos y pesados) se alojaban en la infraestructura *CLOUD* proporcionada por la Universidad y el resto (necesarios durante la operativa local) se desplegaron en otro servidor que actuó como nodo *EDGE* para ofrecer los servicios en el terreno.



**Figura 6.16:** Entorno híbrido CLOUD-EDGE VMware

Tanto para los servicios alojados en el *CLOUD* como para los alojados en el *EDGE*, se optó por virtualizarlos dentro del entorno VMware vSphere con dos servidores ESXI siguiendo la configuración que se observa en la Figura 6.16 y conectados a través de una red protegida por VPN para garantizar la seguridad y privacidad de los datos.



**Figura 6.17:** Detalle de las máquinas virtuales en los servidores

Más en detalle, la Figura 6.17 muestra la distribución de máquinas virtuales que se utilizaron en las diferentes demostraciones realizadas, así como durante las actividades de desarrollo, testeo, y validación. En la imagen se puede observar primero que en el servidor .136 se alojan dentro del espacio de trabajo ASSISTANCE-CLOUD 6 máquinas virtuales y después en el servidor .142 del espacio de trabajo ASSISTANCE-EDGE se aloja una máquina virtual adicional. A continuación se especifican los servicios y los recursos asignados a cada una de las máquinas así como las funcionalidades que pretenden cubrir dentro de los diferentes escenarios de pruebas.

### Servidor ESXI-1 CLOUD

- **ASSISTANCE-ClearOS-Router:** Basada en la distribución GNU/Linux ClearOS con raíces en CentOS, actúa como un router virtual avanzado. Su funcionalidad principal es gestionar el tráfico de la red de ASSISTANCE. Entre sus responsabilidades clave está la asignación dinámica de direcciones IP a través de un servidor DHCP para las diversas máquinas virtuales hospedadas en los servidores ESXI. Además, facilita la resolución de nombres de dominio para cada servidor median-



te un servidor DNS integrado, asegurando así una navegación fluida y eficiente dentro de la infraestructura de ASSISTANCE.

- **ASSISTANCE-Mongodb:** Proporciona el motor de base de datos MongoDB, una plataforma NoSQL orientada a documentos que proporciona alta performance, alta disponibilidad y fácil escalabilidad. Con su modelo de datos flexible y su arquitectura basada en documentos, MongoDB es especialmente adecuada para manejar estructuras de datos complejas y heterogéneas, como las que se encuentran en la IC, donde se pueden integrar y consultar rápidamente una variedad de tipos de datos y formatos.
- **ASSISTANCE-Semanticdb:** Basada en Apache Jena Fuseki, que es un servidor de base de datos semántica que proporciona capacidades avanzadas de almacenamiento y consulta para datos estructurados siguiendo los estándares de la web semántica, incluyendo RDF, SPARQL y OWL. ASSISTANCE-Semanticdb está diseñado para permitir consultas complejas y razonamiento lógico sobre datos, facilitando la fusión de datos dentro de las diferentes operativas de GE.
- **ASSISTANCE-HDFS:** Sistema de archivos distribuidos de alta disponibilidad y alta tolerancia a fallos utilizado por Hadoop, conocido como HDFS. En ASSISTANCE, HDFS se utiliza para almacenar, procesar y analizar grandes conjuntos de datos de manera eficiente en un entorno distribuido. Su arquitectura permite el manejo de grandes volúmenes de información procedentes de diversas fuentes, lo cual es esencial en escenarios de GE donde el volumen y heterogeneidad de los datos puede ser complejo.
- **ASSISTANCE-Docker-Registry:** Es el repositorio central para el almacenamiento y la gestión de imágenes de Docker dentro del ecosistema ASSISTANCE. Actúa como un punto de control clave para la distribución y almacenamiento seguro de contenedores, facilitando el acceso y la reutilización de imágenes de aplicaciones y servicios. En el contexto de ASSISTANCE, Docker Registry juega un papel crucial en la gestión eficiente de los recursos de la plataforma, asegurando que las imágenes de los contenedores sean fácilmente accesibles y estén correctamente versionadas. Esto contribuye a la eficacia y la eficiencia en el despliegue y la actualización de las aplicaciones de la plataforma.
- **ASSISTANCE-Docker-Engine:** Primer nodo de la plataforma de contenedores Docker Engine, que facilita la creación y manejo de contenedores de Docker. En el entorno de ASSISTANCE, Docker Engine es utili-

zado para encapsular y distribuir aplicaciones y servicios de la plataforma, permitiendo una fácil replicación y escalabilidad. Esto posibilita un despliegue ágil y consistente de las aplicaciones necesarias para la GE, mejorando la interoperabilidad y el intercambio de herramientas entre diferentes entidades y sistemas.

Como se puede observar, el servidor ESXI-1 *CLOUD* virtualiza la mayoría de los servicios que requieren de mayor capacidad de almacenamiento y cómputo de ASSISTANCE por lo que sus especificaciones técnicas son de alto rendimiento para poder llevar a cabo las tareas de las diferentes máquinas virtuales.

- **Equipo:** PowerEdge T640 Server
- **Procesador:** 2x Intel Xeon Gold 5120, 2.2GHz, 14 núcleos/28 procesos
- **RAM:** 128GB, 2666 MT/s, bloque doble
- **Almacenamiento:** 12TB SAS nearline a 12Gb/s 7,2K rpm

### Servidor ESXI-2 *EDGE*

- **ASSISTANCE-Docker-Engine-2:** Segundo nodo para la creación y manejo de contenedores Docker. Se utiliza dentro de ASSISTANCE como nodo secundario para correr contenedores de servicios prioritarios y proporcionar alta disponibilidad y balanceo de carga en la ejecución de tareas en el entorno *EDGE* (en el terreno).

Para los servicios que tienen que proporcionar alta disponibilidad en el terreno se hace uso del servidor ESXI-2 *EDGE*, se trata de un servidor portátil que permite conectarse de forma inmediata en cualquier red proporcionando servicios locales a cualquier herramienta o dispositivo que se encuentre en el terreno y tenga acceso a la red local. Se le ha dotado de una gran capacidad en memoria RAM, así como discos duros de estado sólido para que las tareas tengan la mínima latencia posible.

- **Equipo:** Intel NUC, NUC11PAHi7 [208]
- **Procesador:** Core i7-1165G7, 4.7GHz, 4 núcleos/8 procesos
- **RAM:** 64GB, LPDDR4x-4267
- **Almacenamiento:** Samsung 870 EVO SSD 2.5 4TB 16Gb/s

### Actores y Fuentes de datos

En el escenario de **Izmir**, diversos actores juegan un papel crucial en la gestión de la emergencia provocada por el terremoto. Estos actores incluyen equipos de respuesta, comandantes de incidentes y operadores en el centro de mando, entre otros. La siguiente tabla resume los roles y los actores.

Actor	Descripción
FRs	Responden a emergencias y realizan rescates
Comandantes de Incidentes	Evalúan y toman decisiones críticas en el sitio
Operadores en el Centro de Mando	Monitorizan y coordinan las operaciones
Personal de <i>Acil Afet Ambulans Hekimleri Derneği</i> (AAHD)	Proporcionan apoyo y asesoramiento técnico
Personal de VIASAT	Encargados de las comunicaciones
Voluntarios como víctimas	Simulan ser víctimas en el entrenamiento
Personal de IYDEM	Facilitan el entrenamiento en el centro

**Tabla 6.4:** Actores Involucrados en el Terremoto de Izmir

Además, durante las actividades realizadas, se utilizaron varios datasets y fuentes de datos para mejorar la gestión de la emergencia y la toma de decisiones. Estos incluyen datos provenientes de sensores, UAVs, y otros sistemas. La siguiente tabla detalla estas fuentes de datos y su relevancia en el escenario.

Dataset/Fuente	Descripción
Sensores (vitales, GPS, cámaras)	Recopilan datos de las condiciones y ubicaciones
Datos de UAVs	Proporcionan imágenes y reconocimiento aéreo
Datos de UGVs	Información desde el terreno en tiempo real
Llamadas a los servicios de emergencias	llamadas de voz y texto

**Tabla 6.5:** Datasets y Fuentes de Datos del Escenario del Terremoto

En el incidente en un área petroquímica de **Róterdam** involucra varios actores clave, cada uno con un rol específico en la gestión y respuesta al incidente. Esta tabla resume los actores principales y sus funciones en el escenario.

Actor	Descripción
FRs	Responsables de la respuesta inicial en el lugar del incidente
Personal del C2	Coordinan la operación y toman decisiones estratégicas
Autoridades locales	Informadas sobre la evolución del incidente para tomar medidas
Equipos de bomberos ( <i>Gemeentelijke Brandweer</i> (GB) y <i>Söderstra Brandförsvarsförband Fire Brigade</i> (SBFF))	Luchan contra el fuego y realizan tareas de rescate
Equipos de rescate ( <i>Ministerio del Interior - Policía Nacional</i> (MIR-PN) y <i>Orhótnicka Stráž Požarna w Gdarowie Mazowieckim</i> (OSPOM))	Asisten en la búsqueda y rescate de víctimas
Equipos médicos (AAHD y <i>Scientific and Research Centre for Fire Protection</i> (CNBOP))	Proporcionan atención médica y asistencia a las víctimas

**Tabla 6.6:** Actores Involucrados en el Incidente Petroquímico de Rotterdam

Durante la gestión del incidente petroquímico, se emplearon diversos datasets y herramientas para facilitar la respuesta y la toma de decisiones. La siguiente tabla detalla los datasets y fuentes de datos utilizados en el escenario.

En el escenario terrorista simulado de **Sevilla** que se desarrolla en las instalaciones de la policía nacional en Linares se involucra una serie de actores

## CAPÍTULO 6. EVALUACIÓN

Dataset	Descripción
Datos de sensores CO	Detectan la presencia de monóxido de carbono
Cámara IR montada en UxV	Proporciona imágenes térmicas para la evaluación de la situación
Cámaras de vídeo en UxV	Capturan imágenes en tiempo real del lugar del incidente
Cámaras y sensores portátiles	Recogen datos ambientales y visuales desde la perspectiva de los FRs
GPS	Permite el seguimiento de la ubicación de los equipos y recursos
Sensores de constantes vitales	Monitorizan las condiciones de salud de los FRs
Sensores de velocidad del viento	Información meteorológica clave para la gestión del incidente

**Tabla 6.7:** Datasets y Fuentes de Datos del Escenario Petroquímico

clave, cada uno desempeñando un papel crucial en el desarrollo y respuesta al incidente. Esta tabla resume los actores y sus funciones en el escenario.

Actor	Descripción
Terroristas	Ejecutan el ataque en la ciudad
Policía	Responde al ataque y coordina la seguridad
Bomberos	Controla incendios y asiste en rescates
Equipos Médicos	Proporciona atención médica a los heridos
Civiles (Turistas y Locales)	Víctimas y testigos del ataque
Operadores de UAV (Policía)	Utiliza tecnología de UAVs para rastrear terroristas
Unidad Técnico Especialista en Desactivación de Artefactos Explosivos (TEDAX)	Especializada en desactivación de explosivos

**Tabla 6.8:** Actores Involucrados del Ataque Terrorista en Sevilla

Durante la simulación, se utilizaron varios datasets y tecnologías para manejar eficazmente la crisis y facilitar la toma de decisiones. La siguiente tabla detalla los principales datasets y fuentes de datos utilizados y su relevancia.

Dataset	Descripción
Flujos de vídeo de UAVs	Imágenes aéreas del ataque y la respuesta
Comunicaciones de Emergencia	Comunicación entre los servicios de emergencia
Datos de Localización GPS	Ubicación de los equipos de emergencia y terroristas
Informes de Incidentes	Registros detallados de los acontecimientos
Datos de Sensores de Signos Vitales	Monitorización de la salud de los equipos de respuesta
Registros de Respuesta de Emergencia	Actividades y movimientos de los equipos de emergencia
Información de Rastreo de Explosivos	Datos sobre la localización y desactivación de explosivos

**Tabla 6.9:** Datasets y fuentes de datos del Ataque Terrorista en Sevilla

### Contexto pre-incidente

- **Izmir:** Un estado de pánico se apoderó del centro de Izmir tras un terremoto de magnitud 6.2 en la escala de Richter, que duró 45 segundos. El sismo, que se sintió con mayor intensidad por las personas que viven cerca de la costa, causó el colapso de algunos edificios, grietas en otros y la rotura de numerosas ventanas. El centro de llamadas de emergencia

112 recibió información sobre un incendio en un almacén en el puerto y el colapso completo de algunos edificios cercanos al puerto. Un estado de pánico se apoderó del centro de Izmir tras un terremoto de magnitud 6.2 en la escala de Richter, que duró 45 segundos. El sismo, que se sintió con mayor intensidad por las personas que viven cerca de la costa, causó el colapso de algunos edificios, grietas en otros y la rotura de numerosas ventanas. El centro de llamadas de emergencia 112 recibió información sobre un incendio en un almacén en el puerto y el colapso completo de algunos edificios cercanos al puerto.

- **Róterdam:** El 29 de julio, alrededor de las 23:00, ocurre un incidente en un área petroquímica de 5,3 km<sup>2</sup>. Hay un pequeño incendio en un transformador. Minutos después de la llegada de los primeros camiones de bomberos y mientras los bomberos investigan el lugar, se produce una explosión. Un gran destello sale del transformador. Todo queda repentinamente oscuro, el Apagado de Emergencia se activa. El Flare funciona y grandes llamas de unos 50 a 60 metros se elevan sobre él. Hay mucho humo negro. Además, se sospecha una fuga de gas SF<sub>6</sub> (hexafluoruro de azufre), que se descompone en los gases altamente peligrosos SO<sub>2</sub> (dióxido de azufre) y HF (fluoruro de hidrógeno); esto haría peligrosa la investigación de los FRs, además de una posible distribución del gas a las áreas habitadas cercanas. El escenario se llevará a cabo en el área de entrenamiento de GB. GB RDM [209] tiene varias áreas de entrenamiento, por ejemplo, para evacuación de propiedades, entrenamiento en materiales peligrosos y simulacros de incendio, que se pueden usar dentro del proyecto ASSISTANCE. Las imágenes a continuación muestran las áreas de entrenamiento para accidentes industriales y entrenamiento en materiales peligrosos.
- **Linares:** Es un sábado de abril en Sevilla, y la ciudad está llena de vida y actividad mientras se prepara para sus fiestas patronales. En un apartamento cercano al centro, un grupo de terroristas bien entrenados está ultimando los preparativos de un ataque coordinado. Armados con chaquetas explosivas y armas, y con la ayuda de un UAV equipado con una cámara, planean sembrar el terror en las calles repletas de gente. El ataque se desata abruptamente en medio de la multitud desprevenida. En las calles, lo que comenzó como una tarde festiva se convierte rápidamente en una escena de caos y desesperación. Los servicios de emergencia, compuestos por la policía, bomberos y equipos médicos, responden con urgencia. Mientras los equipos de rescate trabajan en el terreno, la policía utiliza tecnología avanzada para rastrear y detener a los atacantes. Esta simulación de un ataque terrorista se lleva a cabo en el centro de

## CAPÍTULO 6. EVALUACIÓN

---

entrenamiento de la policía nacional en Linares donde se pone a prueba la preparación y respuesta de FRs ante emergencias, destacando la importancia de la coordinación efectiva entre los diferentes servicios de emergencia y el uso de tecnología en situaciones de crisis.

### 6.3.2. Caso de uso 1: Terremoto en Izmir

#### 9:30 am. Comienza la demostración

La acción del ejercicio comienza unos minutos después de un gran terremoto en la zona de Izmir. En el centro de mando se reciben llamadas describiendo una situación caótica en la zona de la ciudad: edificios colapsados, muchas personas heridas en la calle, personas atrapadas en edificios derrumbados. Un gran almacén, que podría contener sustancias peligrosas, también se ha visto gravemente afectado.

Esta situación ha sido completamente simulada en el primer ejercicio de demostración del piloto realizado en el Centro de Entrenamiento de Incendios y Desastres Naturales de Izmir **IYDEM** [210] como se indica en la Figura 6.18. Esta parte inicial del ejercicio está compuesta por varios voluntarios actuando como víctimas (indicados como puntos rojos en las Figuras 6.10 – 6.16), en la calle y atrapados en los edificios colapsados, y un edificio de tres pisos que simula el almacén dañado.



**Figura 6.18:** Estado inicial del ejercicio

Las herramientas de ASSISTANCE están instaladas en la sala de mando para intercambiar información con las unidades y sensores desplegados en el campo. Estas aumentan la SA de los operadores y gerentes del ejercicio (descritos como comandantes en este texto, mientras que AAHD [211] y otros usuarios finales actúan como asesores u observadores). Los comandantes están listos para comenzar las actividades de rescate.

### 9:45 am. Los equipos de FRs llegan al área y comienzan las tareas de rescate

Se da una orden desde el puesto de mando a todas las unidades de FRs para que vayan al punto caliente. Después de esto, la primera orden desde la sala de mando es enviar tres mensajes indicando el área de rescate para cada equipo.

El equipo de FRs 1 (AAHD (líder del equipo + 1 FR), GB (2 FRs)) es asignado por los comandantes al almacén de 3 pisos a través de un mensaje de texto, que se recibe en la tablet, lo lee el líder del equipo y lo transmite al resto de los FRs del equipo 1. No hay escaleras en el edificio de 3 pisos. Pero AAHD puede proporcionar equipo y personal para rescatar a una víctima. El Departamento de Bomberos de Izmir puede rescatar al paciente y AAHD y GB hacen intervenciones. También es posible utilizar un maniquí de víctima.

El equipo de FRs 2 (SBFF [212] (líder del equipo + 1 FR) y SBFF (2 FRs)) es asignado por los comandantes a un edificio colapsado a través de un mensaje de texto, que se recibe en la tablet, lo lee el líder del equipo y lo transmite al resto de los FRs. El piloto del UAV está en este equipo y volará el UAV lo antes posible para hacer un reconocimiento general del área con el fin de aumentar la SA para los equipos de FRs y los comandantes.

El equipo de FRs 3 (GB (líder del equipo + 1 FR) y CNBOP [213] (1 FR)) es asignado por los comandantes a un tercer edificio con habitaciones colapsadas a través de un mensaje de texto, que se recibe en la tablet, lo lee el líder del equipo y lo transmite al resto de los FRs.

Cuando los diferentes equipos llegan a sus objetivos, los líderes de equipo darán las órdenes y los FRs comenzarán la evaluación preliminar de seguridad del área antes de comenzar las operaciones de rescate, mientras esperan órdenes específicas de la sala de mando.

En la sala de mando comienza a llegar la primera información del campo (por ejemplo, imágenes de cámaras portátiles, vídeos de cámaras de UAVs, signos vitales constantes de los FRs, ubicaciones de las unidades, etc.).

Un mensaje del equipo 1 se envía a la sala de mando solicitando una misión de UAV para revisar las columnas y vigas del almacén con el fin de decidir si el edificio es lo suficientemente seguro para llevar a cabo operaciones de reconocimiento y rescate, si es necesario.

Los comandantes verifican los vídeos iniciales del almacén desde el UAV y las cámaras portátiles y piden al piloto del UAV que realice una misión manual para examinar el estado del edificio (principalmente algunas columnas y vigas).

Tras visualizar los vídeos de UAVs en la sala de mando por los comandantes de la operación y el operador del módulo DALR, se declara seguro el almacén y se localiza una nueva víctima en el techo del almacén dañado. La ubicación

## CAPÍTULO 6. EVALUACIÓN

---



**Figura 6.19:** Primera misión a los UAVs

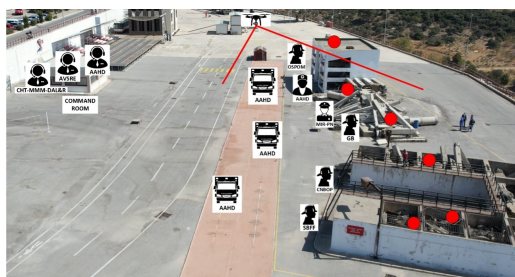
de la víctima se introduce en la SAP por los comandantes y los FRs del Equipo 1 en el campo son informados sobre esta situación a través de un mensaje pidiéndoles que inicien el rescate.

Los FRs del Equipo 1 pueden comenzar el rescate de la víctima en el techo. Una vez localizada la víctima, AAHD y el Departamento de Bomberos de Izmir gestionarán las acciones de rescate de esta víctima. La víctima será simulada por un maniquí de cuerpo completo proporcionado por AAHD.

Después de rescatar a la víctima en el techo, se dan las siguientes órdenes a los operadores de las herramientas ASSISTANCE en la sala de mando:

Verificación (simulada) de la información de los sensores presentados en el módulo CHT y realizar una evaluación de la pluma tóxica potencial en el área.

Esta primera fase del ejercicio se describe en la Figura 6.20.



**Figura 6.20:** Los FRs y los comandantes comienzan los rescates

### 10:15 Primera evaluación de la situación

Desde la sala de mando se establecen diferentes áreas y zonas para ayudar a los FRs a hacer su trabajo. A través de la evaluación de los vídeos de los UAVs y las cámaras portátiles, los comandantes establecen una zona de seguridad



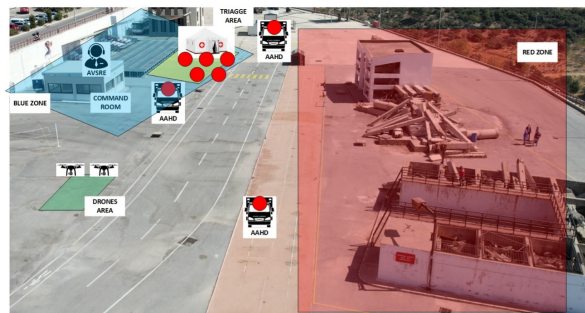
(roja) que cubre las tres partes del escenario y una zona de triaje (amarilla) en un área segura. Esta situación se describe en la siguiente figura.

La ubicación de estas áreas es insertada por los comandantes en la plataforma SA y visualizada en la HMI de la plataforma. Esta información se replica automáticamente en las tablets de los líderes de los equipos de FRs (por ejemplo, las zonas y áreas establecidas se visualizan en las tablets). Además, los comandantes en la sala de control envían la orden al equipo 1 para que coloquen la carpa de triaje en el área segura indicada en el mapa y los miembros del equipo 1 de AAHD realizan la acción. Esta acción se realizará en alrededor de 15 minutos en una ubicación segura seleccionada por el equipo de AAHD.

También, durante esta fase, los FRs establecerán algunas áreas desde sus tablets, que se replicarán en la sala de mando. Las áreas establecidas por los FRs se describen a continuación.

El líder del equipo 3 establecerá un área de comando que cubra la sala de mando (zona azul) y el líder del equipo 2 establecerá un área de aterrizaje de UAVs (zona verde) cerca del punto caliente en un área segura.

Esta situación se describe en la Figura 6.21.



**Figura 6.21:** Evolución de la situación debido al uso de las herramientas ASSISTANCE

Cuando las víctimas hayan sido rescatadas por los equipos de FRs, los miembros de AAHD las llevarán a la carpa de triaje en ambulancia o en camilla (dependiendo de su condición). Por lo tanto, a partir de este momento se realizarán varios traslados de víctimas hasta que todas las víctimas hayan sido llevadas al área de triaje.

## CAPÍTULO 6. EVALUACIÓN

---

### **10:45 Los FRs y los comandantes utilizarán diferentes capacidades de ASSISTANCE durante el ejercicio**

El equipo 3 está evaluando la posibilidad de transportar a una víctima sin ayuda adicional, midiendo la distancia entre su ubicación y el área de triaje. Esta medición se realiza en la tablet. Los comandantes están preparando misiones de UAVs utilizando la capacidad de terreno 3D, en la que se pueden visualizar las características geográficas del área de Izmir.

Los equipos 1 y 2 verificarán simultáneamente las capacidades de personalización de la HMI para probar que ambas HMIs ofrecen información diferente según las necesidades actuales de cada equipo.

Desde el CHT se creará una pluma tóxica simulada y algunos de los FRs estarán dentro de ella. Luego, se enviarán mensajes automáticos para los FRs en peligro por el módulo CHT y el mensaje aparecerá en las tablets y la HMI de la plataforma SA en la sala de mando para tomar las acciones necesarias para informar a estos FRs sobre el peligro y moverlos a un área segura fuera de la pluma tóxica.

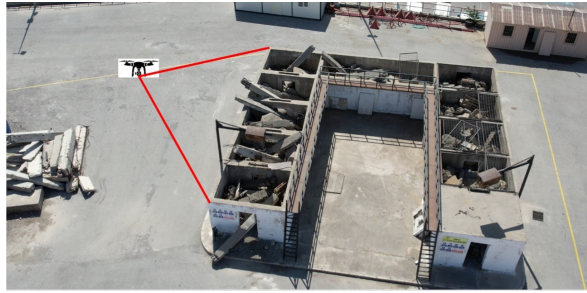
### **11:00 Se realiza la Misión Automática para UAVs**

El equipo 3 solicita una misión de UAV para verificar la seguridad de la parte trasera de su edificio a través de un mensaje de texto/radio.

Después de recibir este mensaje, los comandantes en la sala de control piden al operador MMM una misión de UAV automática.

La segunda misión enviada al UAV es revisar a fondo el lado trasero de un edificio colapsado para tratar de localizar nuevas víctimas o posibles peligros para los FRs. Una nueva víctima es detectada por el flujo de vídeo del UAV y el equipo FRs 3 ingresa la ubicación utilizando las capacidades de la tablet (se crea un nuevo objeto en la ubicación de la víctima). Esta segunda misión se describe en la siguiente figura. Desde la sala de mando se contacta al equipo FRs 2 por mensajes de radio/texto y se les informa que se muevan a esta sección para ayudar al equipo FRs 3 a rescatar a la nueva víctima.

La información sobre los signos vitales de los FRs y las cámaras portátiles sigue llegando a la sala de mando durante esta fase y los comandantes deciden retirar a dos FRs de la línea del frente, ya que sus signos vitales son alarmantemente altos debido a la alta situación de estrés físico. Los comandantes notifican al líder del equipo de FRs a través de un mensaje de texto o radio y él/ella tomará las acciones necesarias para retirar a los FRs en cuestión.

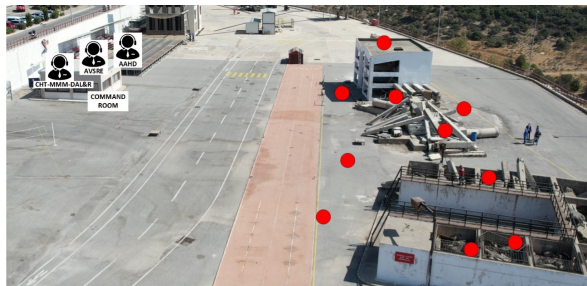


**Figura 6.22:** Segunda misión a los UAVs

### 11:30 Todas las víctimas están siendo rescatadas y llevadas al área de triaje

En este momento, las últimas víctimas son llevadas al área de triaje con las ambulancias o con las camillas por los FRs de AAHD para ser estabilizadas y transportadas a los hospitales de manera más segura. Los FRs de AAHD pedirán a los comandantes rutas seguras de evacuación y los comandantes utilizarán el módulo DALR para obtener información sobre rutas seguras a hospitales reales (las carreteras dañadas y los atascos de tráfico se simulan en el módulo durante esta acción).

Estas rutas se enviarán a la versión móvil de la SAP instalada en las tablets.



**Figura 6.23:** Fin del ejercicio

### 11:30 Fin del ejercicio

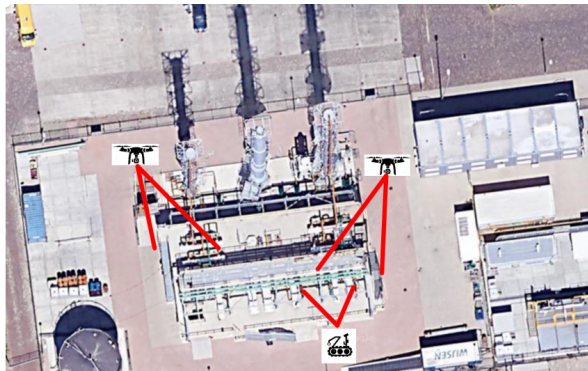
Todas las víctimas han sido estabilizadas y las que necesitan atención hospitalaria han sido transportadas en ambulancia de manera simulada a otro punto de las instalaciones de AADH.

### 6.3.3. Caso de uso 2: Incendio en una petroquímica de Rotterdam

#### 9:30: Los FRs llegan al incidente

comienza la evaluación del área antes de enviar unidades para extinguir los incendios y rescatar posibles víctimas en la planta. Los diferentes equipos de FRs están compuestos por los siguientes usuarios finales:

El equipo de FRs 1 (GB y SBFF) El equipo de FRs 2 (MIR-PN [214] y OSPOM) El equipo de FRs 3 (AAHD y CNBOP) La primera orden enviada desde la SAP es realizar dos misiones diferentes para los UAVs para volar alrededor de la planta a diferentes altitudes para la evaluación de seguridad del escenario. Los UAVs reciben las misiones y despegan para comenzar a recopilar datos de los sensores. El UAV 1 enviará flujos de vídeo de la planta para visualizar el área e intentar localizar posibles víctimas. El UAV 2 enviará flujos de vídeo IR para verificar la temperatura de algunas tuberías y tanques y localizar todos los focos de incendio en la planta. Ambos UAVs estarán equipados con sensores de gas para enviar datos sobre la calidad del aire y detectar posibles sustancias tóxicas en el aire. Todos los flujos de vídeo y datos de sensores serán visualizados desde la SAP y en las tablets en campo. Además, desde la SAP también se ordena realizar una misión para el robot para verificar la temperatura de alguna puerta o tanque y también para tomar mediciones de gas desde el campo. El robot también informará sobre la presencia de posibles campos electromagnéticos peligrosos cerca de un transformador eléctrico.



**Figura 6.24:** Primera misión de UAVs y robots

Toda esta información se visualiza y analiza desde la SAP y desde las tablets.

### 10:00 La SAP pide a CHT información sobre posibles plumas tóxicas

Se realiza una petición de plumas tóxicas en el área y se detecta una pluma tóxica que está afectando un vecindario en el área sureste de la planta. Después de verificar la evolución de la pluma desde la SAP, se decide informar a las autoridades locales sobre este hecho para tomar las medidas oportunas.

### 10:20 Verificaciones de flujos de vídeo

Después de verificar los vídeos enviados por el UAV y los robots en la SAP, se han detectado varios focos de incendio y posibles víctimas, y se colocan en el mapa como objetos con la etiqueta víctima y como amenazas de incendio.



**Figura 6.25:** Localización de fuegos y víctimas

Por otro lado, desde la SAP se establecen varias áreas en el mapa para ayudar a los FRs en campo. Se dibuja un área segura para llevar a las víctimas en la parte oeste de la planta (área verde). Además, la parte de la planta donde se han detectado los incendios se incluye en un área roja para alertar a los FRs de que esta es un área muy peligrosa.



**Figura 6.26:** Definición de perímetros de peligro y zonas seguras

## CAPÍTULO 6. EVALUACIÓN

---

### 10:35 Verificación de datos de sensores

Después de verificar los datos de los sensores, los expertos en la SAP declaran segura el área y se envía un mensaje de inicio de actividades a los equipos en campo. En el mensaje del equipo 1 se incluye la tarea de extinguir el fuego y los equipos 2 y 3 están designados para rescatar a las víctimas localizadas.

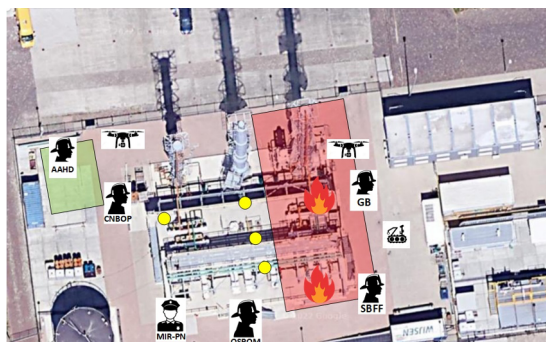


Figura 6.27: Localización de los FRs en el terreno

### 10:45 Monitorización de FRs

Desde el puesto de mando también se monitoriza el estado de los FRs y los flujos de vídeo de las cámaras portátiles para verificar cómo van las operaciones de rescate. Algunas víctimas son rescatadas por los bomberos del Equipo 2 y estabilizadas y evacuadas por los FRs médicos del Equipo 3. Se detecta una alarma de los sensores de signos vitales y se informa al líder del equipo para retirar/ayudar a la unidad afectada. Una vez que las víctimas llegan al área segura (área verde), el líder del equipo 2 solicitará rutas seguras de evacuación teniendo en cuenta las plumas tóxicas como áreas restringidas.

### 6.3.4. Caso de uso 3: Ataque terrorista en Sevilla

9:00 a.m.

Es sábado por la tarde en abril, y en un apartamento cerca del centro de Sevilla, un comando terrorista compuesto por tres terroristas bien entrenados está terminando de ajustar sus chaquetas explosivas y cargando todos los cargadores que pueden para sus ametralladoras AK47. Además, uno de ellos está revisando el nivel de las baterías de un UAV y también comprobando la recepción de vídeo en el GCS (Sistema de Control en Tierra).

### 9:30 a.m.

En la calle, muchas personas pasean, ya que mañana comienza el principal festival de la ciudad de Sevilla y miles de turistas y visitantes están en la ciudad dispuestos a asistir a todos los eventos relacionados con este festival. Todas las terrazas de los bares también están llenas de gente.

### 9:45 a.m.

Dos de los tres terroristas están ahora en la calle y el otro está en el techo de un edificio con el UAV listo para volar. Este terrorista inicia una llamada telefónica con los demás y da la orden de comenzar el ataque. El UAV comienza a volar y el terrorista en el techo recibe imágenes de una gran calle comercial llena de gente caminando y sentada en las terrazas de los bares. A través del teléfono indica el nombre del bar que será el objetivo. (Quizás usemos un autobús si está disponible para ser el objetivo)

### 10:00 a.m.

Uno de los terroristas se dirige al objetivo seleccionado y comienza a disparar alrededor, muchas personas resultan heridas o muertas y de repente activa la chaqueta y se produce una gran explosión. Muchas personas están en el suelo llorando y pidiendo ayuda. Además, hay algunos vehículos en llamas y también un edificio se ve afectado por las llamas.

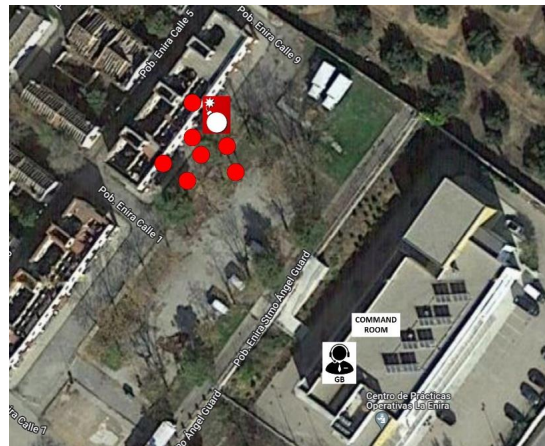


Figura 6.28: Estado inicial del escenario

## CAPÍTULO 6. EVALUACIÓN

---

**10:15 a.m.**

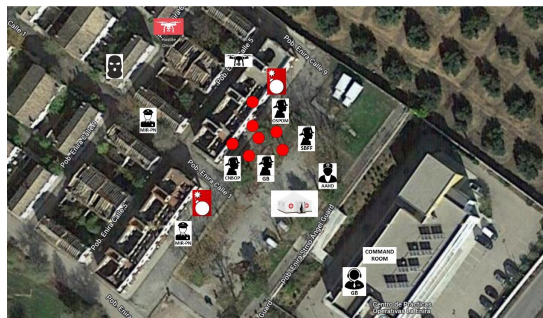
El terrorista en el techo revisa la escena a través de la cámara del UAV. En un par de minutos llegan varias unidades de policía al área, así como una brigada de bomberos y una ambulancia. La policía establece un perímetro de seguridad y solicita al módulo CHT un análisis de una posible pluma tóxica en el área. Una vez que CHT muestra que el área está limpia de sustancias tóxicas, los FRs comienzan las extinciones y los rescates. De repente, cerca del punto caliente, el segundo terrorista es descubierto y comienza a disparar.

**10:30 a.m.**

El terrorista en el techo le indica a dónde ir, ya que la policía se está acercando. La policía intenta localizar al tirador, pero es dirigido a través del teléfono y continúa disparando fuera del alcance de la policía.

**10:45 a.m.**

Para detectar al terrorista, la policía vuela su propio UAV y comienza a recibir el flujo de vídeo en el puesto de mando avanzado cerca del punto caliente y en sus tablets en el campo. Se solicita una misión desde la SAP al MMM para volar cubriendo el área cerca del punto caliente. En algunos minutos, el UAV localiza al terrorista y todos los líderes de equipo de la policía pueden verlo corriendo por las calles. Se envían algunos mensajes desde la SAP a las unidades para que vayan a una ubicación (objeto) para cortar las rutas de escape del terrorista. Desde la sala de mando se activa la fusión de vídeo avanzada para una ubicación precisa del terrorista en el mapa y, así, se marcan el resto de los puntos de escape para el terrorista y estos puntos se reciben en las tablets en el campo y las unidades de policía bloquean todas las rutas de escape potenciales.



**Figura 6.29:** Primera misión de los UAVs



**11:00 a.m.**

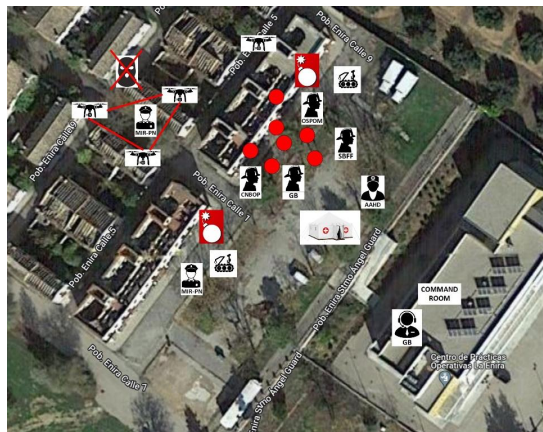
El terrorista en el techo le ordena que detone su chaqueta, ya que informa que la ametralladora está bloqueada. Localiza un grupo de personas y corre, pero el mecanismo de detonación de la chaqueta falla. El terrorista lanza su chaqueta dentro de un bar y comienza a correr mientras el otro terrorista lo guía con la ayuda del UAV malévolo.

**11:15 a.m.**

Las unidades en el campo marcan la chaqueta como una amenaza explosiva y esta información se visualiza en la sala de mando y se pasa esta información a la brigada TEDAX para que acuda rápidamente a esta ubicación. Allí, la unidad TEDAX despliega su robot para comenzar la desactivación de la chaqueta.

**11:30 a.m.**

Se reciben algunos mensajes en la SAP de los FRs en el punto caliente sobre la presencia de una mochila sospechosa en el área. Además, una alerta de los sensores de signos vitales llega a la SAP indicando que una unidad está altamente estresada. La unidad es retirada de la acción. El segundo robot (PIAP) se despliega y comienza a manipular la segunda mochila, mientras se revisan los flujos de vídeo para las unidades TEDAX también en la sala de control. Finalmente, esta segunda mochila resulta ser una falsa alarma y la amenaza se elimina.



**Figura 6.30:** El enjambre de robots y UAVs trabajan en el escenario

## CAPÍTULO 6. EVALUACIÓN

---

**11:45 a.m.**

En este punto, la policía está al tanto de la presencia de un UAV desconocido y comienza a buscar al piloto con su propio UAV y también lanza un UAV captor para neutralizar el UAV hostil. El terrorista en el techo es localizado y se detecta que está guiando al otro terrorista por calles muy estrechas donde las unidades policiales no tienen cobertura de red. En este momento, se activa un enjambre de UAVs por parte de la policía para proporcionar conectividad a las unidades que buscan al terrorista con baja conectividad.

El UAV captor comienza la captura mientras el UAV hostil intenta continuar tomando vídeo para ayudar al otro terrorista, pero en algunos segundos el UAV hostil es capturado en el aire y llevado a una zona segura marcada en el mapa desde la sala de control.



**Figura 6.31:** UAV hostil y piloto terrorista neutralizados

**12:00 p.m.**

En el campo, los FRs están evacuando a los heridos y atendiéndolos en el hospital portátil. Además, el fuego se extingue y los bomberos también evacúan a las víctimas junto con el personal sanitario. Las víctimas se ubican en una zona segura también marcada desde la SAP y los FRs en el campo incluyen a todas las víctimas rescatadas en el sistema a través de objetos para informar a la SAP sobre el número de víctimas rescatadas. También, desde el campo se solicitan rutas de evacuación seguras, evitando algunos atascos de tráfico detectados por el UAV de la policía para una evacuación rápida y segura de las víctimas.

12:15 p.m.

Paralelamente, la brigada TEDAX está desactivando la chaqueta explosiva ubicada en la entrada de un bar cerca del punto inicial caliente. Finalmente, el terrorista en el techo que ha intentado escapar también ha sido capturado por la policía, ya que su ubicación e imágenes estaban disponibles en las tablets.

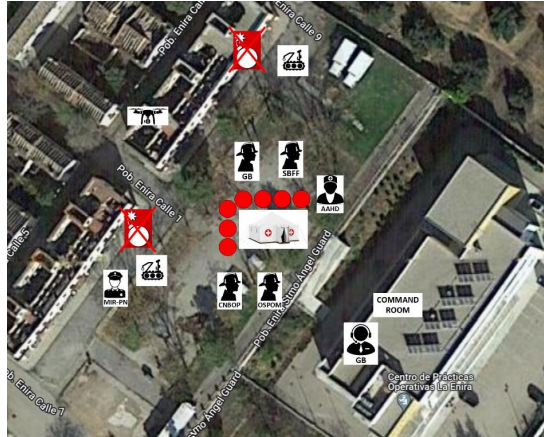


Figura 6.32: Explosivo desactivado y víctimas rescatadas

### 6.3.5. Demostraciones

Durante los últimos meses del proyecto y para demostrar el correcto funcionamiento de la plataforma de ASSISTANCE se realizaron 3 demostraciones para evaluar con usuarios finales el correcto funcionamiento de los sistemas en entornos operacionales simulados bajo operativas reales.

**La primera demostración** se desarrolló del 24-28 de enero de 2022 en la ciudad de Izmir en Turquía, más concretamente en el centro de entrenamiento de incendios y desastres naturales **IYDEM**. Durante estos días se realizaron una serie de entrenamientos previos al simulacro para comprobar que todos los sistemas y herramientas funcionarían de forma correcta durante la demostración. Durante este caso de uso se consiguieron testear los siguientes componentes:

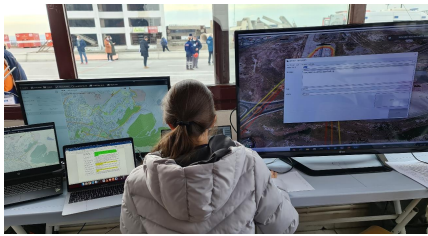
- El despliegue de sensores y plataformas móviles.
- La gestión y manejo de las comunicaciones a todos los niveles

## CAPÍTULO 6. EVALUACIÓN

---

- La recepción de información procedente de sensores por el SAS y poner los datos a disposición de la herramienta de SA
- La generación de rutas rápidas y seguras para operaciones de los FRs
- La monitorización de los FRs por medio de sensores de estado

Durante la operativa también se pudo comprobar el correcto funcionamiento del sistema de intercambio de información entre las unidades móviles y el centro de mando y control, como se puede ver en las Figuras 6.33 y 6.34.



**Figura 6.33:** Envío de mensajes y operativas desde el puesto de mando y control

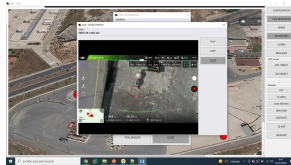


**Figura 6.34:** Recepción de mensajes en el terreno

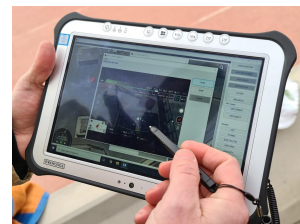
La integración de diferentes UAVs y cámaras con la plataforma para intercambiar flujos de vídeo con el puesto de mando y control y los FRs que se encontraban en el terreno tal y como se aprecia en las Figuras 6.35, 6.36 y 6.37.



**Figura 6.35:** Preparación de los UAVs y las cámaras



**Figura 6.36:** Vídeos en la SAP



**Figura 6.37:** Vídeos en las tablets

Y la coordinación de todos en la operativa, así como la ejecución de todos los rescates planeados de forma eficiente y evitando cualquier tipo de riesgo para la seguridad de los FRs. La Figura 6.38 muestra algunos de los rescates efectuados.



**Figura 6.38:** Rescates de víctimas

Por último, la demostración no se podría haber realizado de forma satisfactoria sin el trabajo y esfuerzo tanto de los técnicos que desarrollaron las herramientas como los FRs que las usaron y los voluntarios que hicieron de víctimas. La Figura 6.39 muestra el equipo al completo.



**Figura 6.39:** Equipo implicado en la demostración

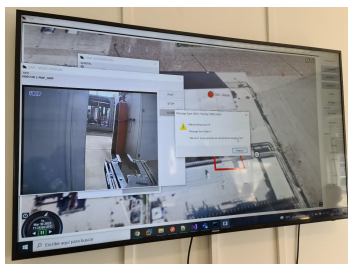
## CAPÍTULO 6. EVALUACIÓN

---

La **segunda demostración** se desarrolló la última semana de marzo de 2022 en la ciudad de Róterdam, más concretamente el *Deltalinqs Trainingplant* de GB. Durante esos días se realizaron una serie de *tests* y entrenamientos previos al simulacro del incendio en la planta petroquímica para comprobar que todos los sistemas y herramientas funcionarían de forma correcta durante la demostración final. Además, durante este caso de uso se consiguieron testear los siguientes elementos:

- El despliegue de sensores y plataformas móviles.
- La gestión y manejo de las comunicaciones a todos los niveles
- La recepción de información procedente de sensores por el SAS y poner los datos a disposición de la herramienta de SA filtrados de acuerdo al tipo de FR
- La generación de rutas rápidas y seguras para operaciones de los FRs
- La monitorización de los FRs por medio de sensores de estado
- El despliegue y rendimiento del módulo CBRN

Durante la operativa pudo comprobar el intercambio de información entre el puesto de mando y control y los FRs en otro entorno, como vemos en las Figuras 6.40 y 6.41



**Figura 6.40:** Envío de mensajes y operativas desde la SAP

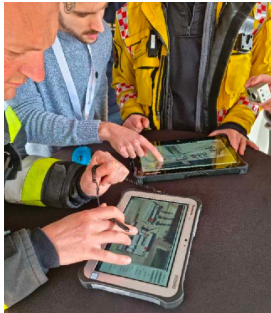


**Figura 6.41:** Recepción de mensajes en el terreno

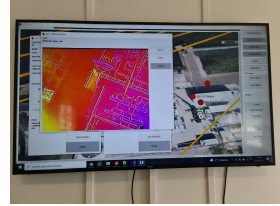
Nuevas integraciones de sensores en los UAVs de GB así como la integración de sus datos en la plataforma de ASSISTANCE para su correcta visualización desde los puestos de mando y control, así como en las tablets de los FRs que operan sobre el terreno tal y como se aprecia en las figuras 6.42, 6.43 y 6.44



**Figura 6.42:**  
Preparación de los UAVs y las cámaras

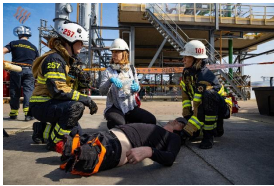


**Figura 6.43:** Vídeos y sensores en las tablets



**Figura 6.44:** Flujos de vídeo y sensores en la SAP

De igual forma que en la demostración anterior, toda la operativa fue perfectamente coordinada a través de la plataforma y la ejecución de todos los rescates se realizó de forma eficiente, evitando cualquier tipo de riesgo para la seguridad de las víctimas y los FRs. La Figura 6.45 muestra algunos de los rescates efectuados



**Figura 6.45:** Rescates de víctimas

Destacar en esta demostración la gran implicación de tanto actores como FRs y técnicos, sin los que la actividad realizada no hubiese alcanzado el éxito obtenido. La Figura 6.46 muestra el equipo al completo.



**Figura 6.46:** Equipo implicado en la demostración

**La tercera y última demostración** se desarrolló la semana del 13 al 17 de junio de 2022 en la ciudad de Linares, más concretamente en el centro operativo y de entrenamiento **La Enira** de la Policía Nacional.

Durante esos días se realizaron una serie de *tests* y entrenamientos previos al simulacro del incendio en la planta petroquímica para comprobar que todos los sistemas y herramientas funcionarían de forma correcta durante la demostración final. Además, durante este caso de uso se consiguieron testear los siguientes elementos:

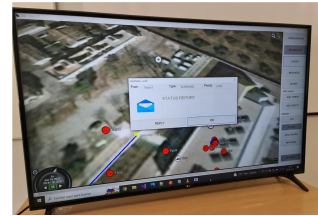
- El despliegue de sensores y plataformas móviles.
- La gestión y manejo de las comunicaciones a todos los niveles
- La recepción de información procedente de sensores por el SAS y poner los datos a disposición de la herramienta de SA filtrados de acuerdo al tipo de FR
- La generación de rutas rápidas y seguras para operaciones de los FRs
- La monitorización de los FRs por medio de sensores de estado
- La neutralización de UAVs potencialmente hostiles
- El despliegue de una red ad hoc montada en un enjambre de UAVs para mejorar la cobertura de las comunicaciones



Durante la operativa se comprobaron las últimas mejoras en el intercambio de mensajes entre el puesto de mando y control y los FRs permitiendo el envío de mensajes automatizados desde el terreno y revisar el histórico de los mismos en el puesto de mando como se ve en las Figuras 6.47 y 6.48



**Figura 6.47:** Envío de mensajes pre-generados desde el terreno



**Figura 6.48:** Recepción de mensajes en la SAP

Integración nuevas funcionalidades en los UAVs, como la red de comunicaciones extendida o el dispositivo de captura para UAVs hostiles, todo ello gestionado por el sistema de mando y control de ASSISTANCE como se muestra en las Figuras 6.49, 6.50 y 6.51



**Figura 6.49:** Enjambre de UAVs para mejora de cobertura



**Figura 6.50:** UAV captor con la red de captura instalada



**Figura 6.51:** Captura de UAV hostil en vuelo por el UAV captor

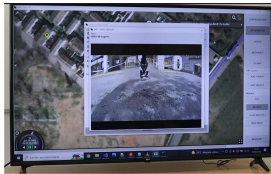
## CAPÍTULO 6. EVALUACIÓN

---

Inclusión de cámaras y sensores en los robots de tierra utilizados por los TEDAX [215] para la identificación y neutralización de los objetos marcados de forma georreferenciada en la plataforma de ASSISTANCE como sospechosos y distribuida a los equipos de campo como se puede observar en las Figuras 6.52, 6.53 y 6.54



**Figura 6.52:** Robot de los TEDAX acercándose al objeto sospechoso



**Figura 6.53:** Robot acercándose al objetivo



**Figura 6.54:** Inspección del objetivo

Por otro lado, del mismo modo que en las demostraciones anteriores, la operativa fue perfectamente coordinada a través de la plataforma ASSISTANCE y la ejecución de todos los rescates se realizó de forma eficiente, evitando cualquier tipo de riesgo para la seguridad de las víctimas y los FRs involucrados en la demostración. La Figura 6.55 muestra algunos de los rescates efectuados.



**Figura 6.55:** Rescates de víctimas

Durante esta última demostración cabe destacar la increíble coordinación por parte de los FRs, técnicos y actores involucrados en la ejecución de las pruebas. La Figura 6.56 muestra la gran cantidad de personal que se movilizó para comprobar los resultados obtenidos en el proyecto.



**Figura 6.56:** Equipo implicado en la demostración

### 6.4. Valoración de los usuarios finales

Durante las tres pruebas piloto del proyecto ASSISTANCE, los usuarios finales proporcionaron comentarios interesantes sobre la usabilidad y efectividad de la plataforma. Estos comentarios son cruciales para refinar ASSISTANCE y satisfacer las necesidades reales de los FRs.

Los usuarios finales enfrentaron varios desafíos de usabilidad al interactuar con la interfaz de la tablet en situaciones de emergencia. Los problemas clave incluyeron:

- Dificultad para navegar en la tablet, especialmente con cuadros de texto y menús desplegados pequeños.
- Proceso lento para escribir mensajes utilizando un lápiz.
- Desafíos al insertar información sobre áreas seguras en la tablet.
- Mecanismos pobres captando la atención en advertencias y mensajes.
- Sobrecarga de información sin distinciones en datos relevantes.

La plataforma ASSISTANCE demostró su potencial para mejorar la SA entre los FRs. Sin embargo, se sugirieron algunas mejoras:

## CAPÍTULO 6. EVALUACIÓN

---

- Necesidad de un intercambio de información más rápido y confiable.
- Mejora en la coordinación entre tareas y claridad en las responsabilidades de los equipos.
- Integración de capacidades para compartir imágenes para ayudar en una mejor evaluación y toma de decisiones.

La tabla a continuación resume los comentarios y las puntuaciones en la Escala de Usabilidad del Sistema de las tres pruebas piloto:

<b>Aspecto</b>	<b>Piloto 1</b>	<b>Piloto 2</b>	<b>Piloto 3</b>
Puntuación de Usabilidad	6.3	7.1	7.8
Efectividad en SA	Alta	Moderada	Moderada
Navegación GUI	Pobre	Regular	Mejorada
Gestión de Información	Adecuada	Necesita Mejora	Adecuada
Soporte de Coordinación	Bueno	Moderado	Moderado

**Tabla 6.10:** Resumen de Comentarios y Puntuaciones de las Pruebas Piloto

Como conclusión, indicar que los comentarios de las pruebas piloto subrayan la importancia del diseño centrado en el usuario en los sistemas de respuesta a emergencias. El refinamiento continuo basado en la retroalimentación de los usuarios fue esencial para garantizar la usabilidad y efectividad del sistema en escenarios del mundo real.

## Capítulo 7

# Conclusiones y líneas de trabajo futuras

### 7.1. Conclusiones finales

Esta tesis ha abordado de manera exhaustiva los retos y dificultades inherentes a la IC y la GE, especialmente en contextos donde se requiere una colaboración estrecha entre diversas agencias. A partir de un análisis detallado de estos problemas, se ha desarrollado una arquitectura innovadora general que se ha adaptado y puesto en práctica para superar los desafíos de la falta de coordinación interagencial tanto durante la IC como en la actuación en campo durante la GE. Estas arquitecturas han sido evaluadas en dos casos de uso distintos, el proyecto MAGNETO y el proyecto ASSISTANCE donde se han realizado demostraciones en diferentes escenarios, lo que ha permitido obtener una serie de conclusiones y aprendizajes clave. A continuación, se presentan las conclusiones finales extraídas de este trabajo de investigación.

#### 7.1.1. Conclusiones generales

##### Estado del arte

- **Gestión de la información en la era digital:** La proliferación de contenido digital y la generación masiva de datos presentan desafíos significativos para la gestión eficiente de la información. Esto es especialmente crítico en campos como la IC y la GE, donde el manejo efectivo de datos es esencial para operaciones exitosas.

## CAPÍTULO 7. CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

---

- **Tecnologías BD y sus desafíos:** La adopción de tecnologías de BD promete mejoras significativas en el análisis de información heterogénea. Sin embargo, su implementación efectiva y manejo requieren superar retos complejos relacionados con la integración, seguridad y análisis de datos.
- **Respuesta ágil en emergencias:** La necesidad de una respuesta rápida y coordinada en situaciones de emergencia subraya la importancia de una colaboración efectiva entre agencias. Este desafío se agrava por la diversidad en procedimientos y tecnologías utilizadas por diferentes entidades.
- **Interoperabilidad y colaboración entre agencias:** El intercambio fluido y constante de información entre agencias es crucial, pero se ve obstaculizado por la diversidad de sistemas y herramientas, lo que dificulta la colaboración efectiva.
- **Desafíos tecnológicos en sistemas complejos:** Integrar y manejar tecnologías emergentes en sistemas cada vez más complejos presenta retos técnicos significativos, que requieren enfoques innovadores y soluciones adaptativas.
- **Gestión de datos heterogéneos:** El manejo de datos extremadamente grandes y variados, especialmente en la lucha contra el crimen organizado y delitos económicos, presenta desafíos únicos en términos de almacenamiento, procesamiento y análisis.
- **Limitaciones en recursos y capacitación:** La escasez de recursos, infraestructuras tecnológicas obsoletas y la falta de capacitación en tecnologías avanzadas constituyen barreras significativas que impiden una respuesta eficaz en situaciones críticas.
- **Desafíos del volumen y complejidad de datos:** El manejo efectivo de grandes volúmenes de datos, especialmente en tiempo real, requiere soluciones más avanzadas que las tecnologías tradicionales, lo que plantea desafíos en términos de escalabilidad y rendimiento.
- **Silos de datos y problemas de integración:** La existencia de silos de datos y la falta de integración efectiva entre sistemas limitan la capacidad de obtener una visión comprensiva y actualizada, esencial en la IC y la GE.
- **Evolución y desafíos de las herramientas de análisis y visualización:** A pesar de los avances en herramientas de análisis y visualización de datos, persisten desafíos en adaptar y aplicar estas tecnologías para satisfacer las necesidades específicas y dinámicas de distintos escenarios operativos.

### Especificación de la arquitectura

- **Superación de limitaciones de sistemas tradicionales:** La arquitectura propuesta aborda los desafíos de eficiencia e interoperabilidad de los sistemas actuales en la prevención y resolución de crímenes, así como en la GE, con el fin de integrar y compartir información de manera efectiva entre diferentes agencias y organismos.
- **Abordaje integral de los requisitos del usuario:** La propuesta tiene en cuenta los requisitos específicos de los usuarios finales de los proyectos MAGNETO y ASSISTANCE, adaptando la arquitectura a sus necesidades particulares.
- **Innovación en estructura y versatilidad:** Se plantea una estructura innovadora y detallada, aplicable en diferentes entornos, desde oficinas hasta situaciones de emergencia en campo, con un énfasis especial en la interoperabilidad y la optimización de la comunicación y colaboración interagencial.
- **Integración eficiente de componentes software:** La arquitectura busca aprovechar la experiencia y conocimientos complementarios mediante la integración de componentes software diversos, utilizando tecnologías como RMI, SOAP, REST, y JMS para superar los problemas de los "silos" de software.
- **Preferencia por microservicios y API Gateway:** Se destaca la transición hacia arquitecturas basadas en microservicios, utilizando un API Gateway para mejorar la modularidad, escalabilidad, rendimiento y flexibilidad en la elección de tecnologías.
- **Enfrentando la complejidad del software:** La arquitectura aborda la complejidad inherente en los sistemas integrados, poniendo énfasis en la integración de diversas tecnologías para manejar grandes volúmenes de datos y garantizar la heterogeneidad, escalabilidad, flexibilidad y eficiencia.
- **Evolución en la adquisición de datos:** Se desarrolla una infraestructura robusta para la adquisición y almacenamiento de datos, utilizando tecnologías avanzadas como Apache Kafka y sistemas de bases de datos especializados, permitiendo una gestión eficiente de los datos.
- **Innovación en la fusión de datos:** Se transforman los datos brutos en formatos máquina-legibles utilizando ontologías y una KB, lo que permite una organización y acceso eficiente a la información y la evolución constante del conocimiento almacenado.

## CAPÍTULO 7. CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

---

- **Profundización en análisis de datos:** La plataforma permite una amplia gama de análisis de datos, implementados como microservicios documentados y gestionados por el Postprocess-Manager, para optimizar la utilización de recursos y la escalabilidad.
- **Visualización intuitiva y operativa de datos:** Se enfatiza la importancia de transformar los resultados del análisis en visualizaciones claras y comprensibles, utilizando técnicas de visualización adaptadas a la naturaleza de los datos y consolidadas en un único dashboard.
- **Personalización y adaptabilidad en la representación de datos:** La arquitectura contempla diversas interfaces hombre-máquina y técnicas de visualización, adaptándose a las necesidades específicas de cada tipo de dato y situación operativa, y asegurando una comunicación eficiente entre el *Frontend* y el *Backend*.
- **Enfoque en seguridad y resiliencia:** La propuesta destaca la necesidad de una arquitectura que refuerce la seguridad y resiliencia en situaciones críticas, mediante una comunicación y análisis de datos mejorados.
- **Facilitación de la toma de decisiones basada en datos:** La arquitectura busca optimizar la capacidad de análisis de información y toma de decisiones, a través de una integración efectiva de datos y una representación clara de la información.
- **Flexibilidad y escalabilidad en la implementación:** La arquitectura diseñada permite adaptarse a diferentes escenarios y entornos, ofreciendo flexibilidad en su implementación y posibilitando su escalabilidad según las necesidades del proyecto.
- **Mejora en la gestión de emergencias:** La arquitectura apunta a una gestión más eficiente en la respuesta ante emergencias, permitiendo una mejor coordinación de recursos y una capacidad de respuesta rápida y efectiva.

### 7.1.2. MAGNETO

- **Innovación en la lucha contra el crimen digitalizado:** MAGNETO surge como respuesta al creciente desafío de la criminalidad en la era digital. Su objetivo es integrar y analizar datos multimedia de diversas fuentes, proporcionando una herramienta avanzada para las Agencias de Aplicación de la Ley. Esta integración de datos facilita la identificación de patrones ocultos y la generación de inteligencia en la lucha contra el crimen organizado y el terrorismo.



- **Plataforma unificada para análisis criminal:** MAGNETO consolida datos de audio, vídeo, redes sociales y bases de datos policiales en una única plataforma. Esta centralización permite un análisis más profundo y una interpretación más eficaz de la información, crucial para investigaciones complejas y la toma de decisiones estratégicas.
- **Potenciación de la capacidad predictiva y cognitiva:** La plataforma se distingue por su enfoque en la anticipación de tendencias delictivas y amenazas. Utiliza modelos de datos avanzados y procesamiento semántico para construir una base sólida para el razonamiento y la cognición, permitiendo una mejor preparación y respuesta proactiva frente a situaciones emergentes.
- **Objetivos alcanzados con metodología S.M.A.R.T.:** Los objetivos de MAGNETO, tanto científico-técnicos como operativos, se han definido y medido utilizando el enfoque S.M.A.R.T., asegurando resultados claros y concretos. La implementación de Indicadores Clave de Desempeño ha permitido monitorear el progreso y el éxito de cada objetivo, garantizando así la efectividad general del proyecto.
- **Desarrollo de interfaces intuitivas para usuarios:** MAGNETO ha enfocado gran parte de su desarrollo en la creación de interfaces hombre-máquina centradas en el usuario. Estas interfaces mejoran significativamente la SA y la capacidad operativa de los agentes, facilitando la interacción con la plataforma y agilizando las rutinas de trabajo.
- **Arquitectura modular y escalable:** La plataforma MAGNETO se ha construido con una arquitectura modular, lo que permite una flexibilidad y escalabilidad sin precedentes. Esta arquitectura facilita la adaptación a diferentes escenarios operativos y permite la incorporación de nuevas tecnologías y componentes según sea necesario, asegurando la relevancia y la efectividad a largo plazo de la plataforma.
- **Integración y seguridad de tecnologías de vanguardia:** La integración de tecnologías avanzadas como procesamiento de lenguaje natural y aprendizaje automático en MAGNETO ha enriquecido las capacidades de análisis y de toma de decisiones, proporcionando una herramienta poderosa y segura en el contexto de seguridad y emergencia.
- **Visualización avanzada para análisis de datos:** MAGNETO ha implementado herramientas sofisticadas para el análisis y la visualización de datos. Estas herramientas permiten un análisis detallado y una interpretación precisa de una amplia variedad de datos, desde textos hasta

## CAPÍTULO 7. CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

---

contenido multimedia, mejorando la inteligencia operativa y la toma de decisiones.

- **Contribución a la gestión eficiente en investigaciones:** La plataforma MAGNETO ha demostrado ser una herramienta crucial en la mejora de la obtención de patrones y elaboración de pruebas forenses en ICs. Permite una mejor coordinación de recursos y una capacidad de respuesta rápida y efectiva, facilitando la toma de decisiones críticas en situaciones de alta presión.
- **Validación y satisfacción de usuarios:** La implementación de MAGNETO ha sido validada a través de demostraciones y ejercicios prácticos con agencias de aplicación de la ley. La retroalimentación obtenida ha sido ampliamente positiva, reflejando la eficacia y la utilidad de la plataforma en entornos operativos reales.

### 7.1.3. ASSISTANCE

- **Integración de nuevas tecnologías:** El proyecto ha demostrado con éxito la integración de tecnologías avanzadas, incluyendo UAVs, robots, y sistemas de realidad virtual y aumentada, lo cual ha revolucionado la manera en que los FRs abordan las situaciones de emergencia. Esta integración ha permitido una evaluación más precisa y segura de las zonas afectadas, mejorando significativamente la eficiencia y seguridad de las operaciones.
- **Eficacia de la plataforma de SA:** La implementación de la SAP en ASSISTANCE ha demostrado ser un avance significativo en la mejora de la SA de los FRs. La plataforma ha proporcionado una interfaz unificada e intuitiva para la visualización y gestión de datos críticos durante emergencias, incluyendo flujos de video en tiempo real, datos de sensores y ubicaciones GPS. La SAP ha facilitado la toma de decisiones rápida y basada en datos, mejorando la coordinación entre los FRs y el mando y control. Su capacidad para integrar y procesar datos de múltiples fuentes en una sola interfaz ha sido fundamental para proporcionar una visión completa y en tiempo real del entorno operativo, lo que da como resultado una respuesta más eficaz y coordinada durante situaciones de emergencia. Esta plataforma ha establecido un nuevo estándar en la operativa de respuesta a emergencias, destacando la importancia de la tecnología avanzada en la mejora de las capacidades de los FRs.
- **Innovación en la integración de sensores a través del servicio de Abstracción de Sensores):** Un componente clave del éxito de

ASSISTANCE ha sido el desarrollo y la implementación del SAS, una plataforma avanzada que ha permitido una integración eficaz y eficiente de una amplia gama de sensores y fuentes de datos. El SAS ha jugado un papel crucial en la estandarización y normalización de los datos procedentes de sensores heterogéneos, lo que ha facilitado su integración en la plataforma de SA. Esta capacidad ha permitido una recopilación y análisis de datos más robustos y confiables, mejorando significativamente la toma de decisiones en tiempo real durante emergencias. El SAS ha demostrado ser una herramienta esencial para la gestión de datos complejos y ha contribuido a una mayor eficiencia operativa, tanto en la recopilación de datos como en su análisis y presentación en la SAP.

- **Conectividad y comunicación robustas:** La implementación de una red de comunicaciones segura y fiable ha sido esencial para asegurar una coordinación efectiva y una respuesta rápida en situaciones críticas. La infraestructura de red ha permitido mantener la conectividad incluso en condiciones adversas, mejorando la coordinación entre los FRs y los centros de mando.
- **Evaluación integral del proyecto:** Las pruebas realizadas en entornos controlados y las evaluaciones de impacto social han permitido validar la efectividad de las soluciones desarrolladas. Además, se han identificado y abordado desafíos legales y éticos, asegurando que el proyecto cumpla con los estándares de protección de datos y privacidad.
- **Desarrollo HMIs:** Las HMIs avanzadas e inteligentes desarrolladas han mejorado significativamente la interacción con el sistema, permitiendo a los usuarios acceder y procesar información crítica de manera más eficiente. Esto ha mejorado la toma de decisiones y ha facilitado la operación de diversas herramientas y sensores en situaciones de emergencia.
- **Simulaciones realistas de escenarios de emergencia:** Las simulaciones y demostraciones de casos de uso han sido fundamentales para probar y mejorar las herramientas y estrategias desarrolladas. Estas simulaciones han proporcionado oportunidades valiosas para que los FRs practiquen y se familiaricen con las nuevas tecnologías y procedimientos en un entorno controlado.
- **Mejoras en la operativa en campo:** La dotación de tablets ruggedizadas a los FRs ha mejorado la operativa en el campo, proporcionando una herramienta poderosa para la gestión y mitigación de situaciones de crisis. Estos dispositivos han permitido acceder a información crucial en

## CAPÍTULO 7. CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

---

tiempo real, mejorando la autonomía y eficiencia de los equipos en el terreno.

- **Uso de wearables para monitoreo en tiempo real:** La integración de dispositivos wearables ha proporcionado una herramienta valiosa para la monitorización en tiempo real de las condiciones de los FRs, aumentando su seguridad y eficacia en operaciones.
- **Compromiso con la seguridad y la conformidad Legal:** El proyecto ha mantenido un enfoque firme en la seguridad, la protección de datos y la conformidad con los valores sociales europeos. Esto ha asegurado que todas las soluciones desarrolladas se alineen con los derechos fundamentales y las regulaciones de protección de datos.
- **Fortalecimiento de la capacitación:** ASSISTANCE ha establecido una infraestructura de formación avanzada, utilizando metodologías innovadoras como la realidad virtual, mixta y aumentada. Estos programas han contribuido significativamente a mejorar las habilidades y capacidades de los FRs, preparándolos mejor para enfrentar emergencias complejas.

### 7.2. Líneas futuras

Tras el desarrollo de esta tesis, se han identificado diversas oportunidades para expandir la investigación en múltiples direcciones. Hemos observado la relevancia de herramientas BD y la interoperabilidad en la GE, así como su potencial aplicación en una variedad de contextos más allá de la IC. La plataforma MAGNETO, con su capacidad para manejar grandes volúmenes de datos, podría adaptarse fácilmente a diferentes entornos con mínimas modificaciones. Esto abre posibilidades para su aplicación en nuevos escenarios, como los contemplados en el proyecto PREVISION [216] en el que la UPV participa como socio, proporcionando el conocimiento obtenido durante el proyecto MAGNETO así como los módulos y herramientas desarrollados.

En el ámbito de interoperabilidad, la plataforma podría ser útil en muchos otros contextos más allá de los estudiados en MAGNETO y ASSISTANCE. Aunque los adaptadores específicos pueden no ser directamente aplicables a otras herramientas, las funcionalidades internas de la plataforma general diseñada en esta tesis podrían de utilidad en diversos entornos. Una línea de investigación futura podría incluir la adaptación de la plataforma a nuevas bases de datos distribuidas y modelos de IA que permitan mejorar el rendimiento en el almacenado, indexación y análisis de la información que se maneja en cualquier ámbito, no solo dentro de la IC o la GE.

Otra área de interés es la barrera del idioma en la interoperabilidad, especialmente cuando se trata de compartir información entre agencias de diferentes países. Implementar módulos de traducción autónomos y *offline* basados en modelos del lenguaje de inteligencia artificial sería una línea de investigación emergente importante. Adicionalmente, sería beneficioso explorar la incorporación de nuevos escenarios en casos de uso como los que se abordaron en ASSISTANCE, con el fin de cubrir un espectro más amplio de emergencias. La integración de diferentes servicios de imágenes por satélite, además de COPERNICUS [217], y la exploración de nuevas tecnologías como la realidad aumentada y el IoT, podrían enriquecer significativamente la gestión y respuesta ante emergencias. Esto se ha tenido en consideración durante la redacción de una nueva propuesta que coordina la UPV para el programa HE. La propuesta IMPRESSIVE trata de ser un *follow up* del proyecto ASSISTANCE en el que además de mejorar las capacidades de los FRs por medio de plataformas no tripuladas UxVs, se hará uso de nuevas tecnologías de realidad aumentada para mejorar la visión de los FRs en situaciones de baja visibilidad.

Finalmente, la integración de sistemas de mensajería modernos, comunicaciones 5G y la conexión con una amplia gama de sensores IoT podrían proporcionar a la plataforma una herramienta aún más potente y versátil tanto en la IC como en la GE.

## **CAPÍTULO 7. CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS**

---

# Referencias

- [1] Europol report on terrorism in the EU. Europol. [Online]. Available: <https://datagraver.com/europol-terrorism-data/#more-605>
- [2] C. E. Á. Calderón and C. A. R. Beltrán, “Ecosistemas criminales,” *Revista Científica General José María Córdova*, 2018.
- [3] S. Pisabarro, “Fortalezas y debilidades de la unión europea en la lucha antiterrorista desde 2015,” 2020.
- [4] The human cost of disasters: an overview of the last 20 years (2000-2019). United Nations Office for Disaster Risk Reduction. [Online]. Available: <http://www.undrr.org/quick/50922>
- [5] E. Shittu, G. G. Parker, and N. B. Mock, “Improving communication resilience for effective disaster relief operations,” *Environment Systems and Decisions*, vol. 38, pp. 379–397, 2018.
- [6] Multinational interoperability council. [Online]. Available: <https://usac.army.mil/sites/default/files/publications/16-18.pdf>
- [7] Global disaster alert and coordination system. [Online]. Available: <https://gdacs.org/>
- [8] Virtual on site operations coordination center. [Online]. Available: <https://vosocc.unocha.org/>
- [9] M. E. Bonfanti and F. Capone, “Fostering a comprehensive security approach: An exploratory case study of cbrn crisis management frameworks in eleven european countries,” *Information & Security: An International Journal*, vol. 33, p. 55, 2015.
- [10] A. Bjerre-Nielsen, V. Kassarnig, D. D. Lassen, and S. Lehmann, “Task-specific information outperforms surveillance-style big data in predictive

## REFERENCIAS

---

- analytics.” *Proceedings of the National Academy of Sciences of the United States of America*, 2021.
- [11] Multimedia analysis and correlation engine for organised crime prevention and investigation. [Online]. Available: <https://cordis.europa.eu/project/id/786629/es>
- [12] Assistance. [Online]. Available: <https://assistance-project.eu/>
- [13] J. Kolbitsch and H. A. Maurer, “The transformation of the web: How emerging communities shape the information we consume,” *J. Univers. Comput. Sci.*, vol. 12, pp. 187–213, 2006.
- [14] S. Brayne, “The criminal law and law enforcement implications of big data,” *Annual Review of Law and Social Science*, 2018.
- [15] T. Simona, T. Taupo, and P. M. Antunes, “A scoping review on agency collaboration in emergency management based on the 3c model,” *Information Systems Frontiers*, vol. 25, pp. 291–302, 2021.
- [16] B. Vitoriano, J. Montero, and D. Ruan, “Decision aid models for disaster management and emergencies,” in *Atlantis Computational Intelligence Systems*, 2013.
- [17] A. M. Razip *et al.*, “A mobile visual analytics approach for law enforcement situation awareness,” *2014 IEEE Pacific Visualization Symposium*, pp. 169–176, 2014.
- [18] Q. Liao *et al.*, “A secure end-to-end cloud computing solution for emergency management with uavs,” *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, 2018.
- [19] A. K. Dogra and TanujWala, “A review paper on data mining techniques and algorithms,” 2015.
- [20] W. Müller, A. Kuwertz, D. Mühlenberg, and J. Sander, “Semantic information fusion to enhance situational awareness in surveillance scenarios,” *2017 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI)*, pp. 397–402, 2017.
- [21] Une-en iso 22311:2014 protección y seguridad de los ciudadanos. [Online]. Available: <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0054093>
- [22] Niem. [Online]. Available: <https://www.niem.gov/>



- [23] Emergency data exchange language (edxl) distribution element version 2.0. [Online]. Available: <https://docs.oasis-open.org/emergency/edxld/v2.0/edxld-v2.0.html>
- [24] Oasis open. [Online]. Available: <https://www.oasis-open.org/>
- [25] Common alerting protocol. [Online]. Available: <https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>
- [26] Geography markup language - open geospatial consortium. [Online]. Available: <https://www.ogc.org/standard/gml/>
- [27] Learn about hl7 international. [Online]. Available: <https://info.hl7.org/learn-more>
- [28] Ieee sa - ieee 1512-2006. [Online]. Available: <https://standards.ieee.org/ieee/1512/3522/>
- [29] Iso/iec 27001:2022 - information security, cybersecurity and privacy protection. [Online]. Available: <https://www.iso.org/standard/27001>
- [30] Its standards – intelligent transport systems. [Online]. Available: <https://www.itsstandards.eu/>
- [31] W3c. [Online]. Available: <https://www.w3.org/>
- [32] Jc3iedm. [Online]. Available: <https://brainsciencesjournal.org/2007.JC3IEDM.pdf>
- [33] Manchester bomber salman abedi murdered 22 in suicide attack, coroner rules - bbc news. [Online]. Available: <https://www.bbc.com/news/uk-england-manchester-67143958>
- [34] Inquests arising from the deaths in the westminster terror attack of 22 march 2017. [Online]. Available: <https://www.judiciary.uk/wp-content/uploads/2018/12/Westminster-Terror-Attack-2018-0304.pdf>
- [35] Atentado en la rambla de barcelona. [Online]. Available: <https://www.lavanguardia.com/sucesos/20170817/43611025471/atentado-barcelona-rambla.html>
- [36] L. Alawneh, M. Said, and Z. Al-Sharif, “Towards hierarchical cooperative analytics architecture in law enforcement agencies,” in *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 2017, pp. 1–6.

## REFERENCIAS

---

- [37] M. Karyda and L. Mitrou, “Internet forensics: Legal and technical issues,” *International Workshop on Digital Forensics and Incident Analysis*, 2007.
- [38] F. Alamdar, M. Kalantari, and A. Rajabifard, “Towards multi-agency sensor information integration for disaster management,” *Comput. Environ. Urban Syst.*, vol. 56, pp. 68–85, 2016.
- [39] H. Yu and C. Hu, “A police big data analytics platform: Framework and implications,” in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, 2016, pp. 323–328.
- [40] Mysql. [Online]. Available: <https://www.mysql.com/>
- [41] Oracle — aplicaciones y plataforma en la nube. [Online]. Available: <https://www.oracle.com/es/>
- [42] Opentext encase forensic. [Online]. Available: <https://www.opentext.com/products/encase-forensic>
- [43] Ftk® forensic toolkit - exterro. [Online]. Available: <https://www.exterro.com/forensic-toolkit>
- [44] Arcgis. [Online]. Available: <https://www.arcgis.com/index.html>
- [45] Software de análisis e inteligencia de negocios — tableau. [Online]. Available: <https://www.tableau.com/es-es>
- [46] M. Miljković, “Challenges in the work of intelligence services in the information age,” 2020.
- [47] W. V. Pelfrey, “Emergency manager perceptions of the effectiveness and limitations of mass notification systems: A mixed method study,” *Journal of Homeland Security and Emergency Management*, vol. 18, pp. 49 – 65, 2020.
- [48] H. Watson, R. L. Finn, and K. Wadhwa, “Organizational and societal impacts of big data in crisis management,” *ERN: Knowledge Management & Innovation (Topic)*, 2017.
- [49] D. V. Puyvelde, S. Coulthart, and M. S. Hossain, “Beyond the buzzword: big data and national security decision-making,” *International Affairs*, vol. 93, pp. 1397–1416, 2017.
- [50] P. K. Khobragade and L. G. Malik, “Data generation and analysis for digital forensic application using data mining,” *2014 Fourth International Conference on Communication Systems and Network Technologies*, pp. 458–462, 2014.

- [51] N. G. Khan and V. B. Bhagat, "Effective data mining approach for crime-terrorpattern detection using clustering algorithm technique," *International journal of engineering research and technology*, vol. 2, 2013.
- [52] M. Feng *et al.*, "Big data analytics and mining for effective visualization and trends forecasting of crime data," *IEEE Access*, vol. 7, pp. 106 111–106 123, 2019.
- [53] K. M. Richmond, "Ai, machine learning, and international criminal investigations: The lessons from forensic science," *Social Science Research Network*, 2020.
- [54] A. H. Lone and R. N. Mir, "Forensic-chain: Ethereum blockchain based digital forensics chain of custody," 2017.
- [55] J. Wang *et al.*, "Virtual reality and integrated crime scene scanning for immersive and heterogeneous crime scene reconstruction." *Forensic science international*, vol. 303, p. 109943, 2019.
- [56] J. R. Blum, A. Eichhorn, S. Smith, M. Sterle-Contala, and J. R. Coopers-tock, "Real-time emergency response: improved management of real-time information during crisis situations," *Journal on Multimodal User Inter-faces*, vol. 8, pp. 161 – 173, 2013.
- [57] N. Stylianou, J. Young, C. J. Peden, and C. Vasilakis, "Developing and validating a predictive model for future emergency hospital admissions," *Health Informatics Journal*, vol. 28, 2022.
- [58] J. Qadir *et al.*, "Crisis analytics: big data-driven crisis response," *Journal of International Humanitarian Action*, vol. 1, 2016.
- [59] H. Gwalani, A. R. Mikler, S. Ramisetty-Mikler, and M. O'Neill, "Collec-tion and integration of multi-spatial and multi-type data for vulnerability analysis in emergency response plans," in *International Conference on Informatics for Environmental Protection*, 2016.
- [60] H. Watson and R. Rodrigues, "Bringing privacy into the fold: Consider-ations for the use of social media in crisis management," *POL: Other Change Management Strategy (Topic)*, 2018.
- [61] Y. Tao, "Application of big data technology in national emergency ma-nagement system," 2020.

## REFERENCIAS

---

- [62] G. Trecarichi, V. Rizzi, M. Marchese, L. Vaccari, and P. Besana, “Enabling information gathering patterns for emergency response with the openknowledge system.” *Computing and Informatics*, vol. 29, pp. 537–555, 01 2010.
- [63] Fema.gov. [Online]. Available: <https://www.fema.gov/>
- [64] S. Šubik, S. Rohde, T. Weber, and C. Wietfeld, “Spider: Enabling interoperable information sharing between public institutions for efficient disaster recovery and response,” 12 2010, pp. 190 – 196.
- [65] Servicios web - documentación de ibm. [Online]. Available: <https://www.ibm.com/docs/es/was/9.0.5?topic=services-web>
- [66] Xml - explicación del lenguaje de marcado extensible (xml) - aws. [Online]. Available: <https://aws.amazon.com/es/what-is/xml/>
- [67] Soap - documentación de ibm. [Online]. Available: <https://www.ibm.com/docs/es/radfw/9.6.1?topic=standards-soap>
- [68] Wsdl (web services description language) - documentación de ibm. [Online]. Available: <https://www.ibm.com/docs/es/rsas/7.5.0?topic=standards-web-services-description-language-wsdl>
- [69] Uddi (universal description, discovery, and integration) - documentación de ibm. [Online]. Available: <https://www.ibm.com/docs/es/rsas/7.5.0?topic=standards-universal-description-discovery-integration-uddi>
- [70] Json. [Online]. Available: <https://www.json.org/json-es.html>
- [71] J. Tekli, E. Damiani, and R. Chbeir, “Differential soap multicasting,” in *2011 IEEE International Conference on Web Services*, 2011, pp. 1–8.
- [72] J. C. Pickering and A. M. Fox, “Enabling collaboration and communication across law enforcement jurisdictions: Data sharing in a multiagency partnership,” *Criminal Justice Policy Review*, vol. 33, pp. 732 – 755, 2021.
- [73] P. Hewett, J. Mitrani, W. C. Metz, and J. J. Vercellone, “Coordinating, integrating, and synchronizing disaster response: Use of an emergency response synchronization matrix in emergency planning, exercises, and operations,” *International Journal of Mass Emergencies & Disasters*, vol. 19, pp. 1 – 12, 2001.
- [74] Rest — codecademy. [Online]. Available: <https://www.codecademy.com/article/what-is-rest>

- [75] J. S. Spaulding and K. B. Morris, “Integration of dna, fingerprint, and firearm databases into forensic intelligence networks for a real-time case assessment model,” *Journal of Policing, Intelligence and Counter Terrorism*, vol. 14, pp. 39 – 61, 2019.
- [76] A. Dilo and S. Zlatanova, “Data modelling for emergency response,” 2010.
- [77] Data interoperability solution at stakeholders emergencies reaction — disaster. [Online]. Available: <https://cordis.europa.eu/project/id/285069>
- [78] Aftermath crisis management system-of-systems demonstration — acrimas —. [Online]. Available: <https://cordis.europa.eu/project/id/261669>
- [79] The driver project for crisis management. [Online]. Available: <https://www.driver-project.eu/>
- [80] Sql server 2022 — microsoft. [Online]. Available: <https://www.microsoft.com/es-es/sql-server/sql-server-2022>
- [81] Postgresql. [Online]. Available: <https://www.postgresql.org/>
- [82] Nosql databases explained. [Online]. Available: <https://www.mongodb.com/es/nosql-explained>
- [83] Data lakes ibm. [Online]. Available: <https://www.ibm.com/es-es/topics/data-lake>
- [84] Mongodb. [Online]. Available: <https://www.mongodb.com/es>
- [85] Apache cassandra documentation. [Online]. Available: [https://cassandra.apache.org/\\_/index.html](https://cassandra.apache.org/_/index.html)
- [86] Neo4j graph database & analytics. [Online]. Available: <https://neo4j.com/>
- [87] Apache hbase. [Online]. Available: <https://hbase.apache.org/>
- [88] Bigquery. [Online]. Available: <https://cloud.google.com/bigquery?hl=es>
- [89] Hdfs apache hadoop — ibm. [Online]. Available: <https://www.ibm.com/es-es/topics/hdfs>
- [90] Minio — high performance, kubernetes native object storage. [Online]. Available: <https://min.io/>

## REFERENCIAS

---

- [91] Aws — almacenamiento de datos seguro en la nube (s3). [Online]. Available: <https://aws.amazon.com/es/s3/>
- [92] Apache kafka. [Online]. Available: <https://kafka.apache.org/>
- [93] Apache spark™. [Online]. Available: <https://spark.apache.org/>
- [94] Apache hive. [Online]. Available: <https://hive.apache.org/>
- [95] Superset. [Online]. Available: <https://superset.apache.org/>
- [96] C. H. Ku, J. H. Nguyen, and G. Leroy, “Tasc - crime report visualization for investigative analysis: A case study,” *IEEE International Conference on Information Reuse and Integration*, 2012.
- [97] i2 analyst’s notebook. [Online]. Available: <https://i2group.com/i2-analysts-notebook>
- [98] Visualización de datos — microsoft power bi. [Online]. Available: <https://powerbi.microsoft.com/es-es/>
- [99] Gis. [Online]. Available: <https://www.qgis.org/es/site/>
- [100] Cesium. [Online]. Available: <https://cesium.com/>
- [101] Tensorflow. [Online]. Available: <https://www.tensorflow.org/?hl=es-419>
- [102] Pytorch. [Online]. Available: <https://pytorch.org/>
- [103] Maltego. [Online]. Available: <https://www.maltego.com/>
- [104] Google earth. [Online]. Available: <https://www.google.es/intl/es/earth/index.html>
- [105] Ushahidi. [Online]. Available: <https://www.ushahidi.com/>
- [106] Splunk. [Online]. Available: <https://www.splunk.com/>
- [107] Zabbix. [Online]. Available: <https://www.zabbix.com/>
- [108] Docker. [Online]. Available: <https://www.docker.com/>
- [109] Kubernetes. [Online]. Available: <https://kubernetes.io/es/docs/concepts/overview/what-is-kubernetes/>
- [110] Ansible. [Online]. Available: <https://www.ansible.com/>
- [111] Terraform by hashicorp. [Online]. Available: <https://www.terraform.io/>

- [112] Kong inc. [Online]. Available: <https://konghq.com/>
- [113] Netflix/zuul: Zuul is a gateway service that provides dynamic routing, monitoring, resiliency, security, and more. [Online]. Available: <https://github.com/Netflix/zuul>
- [114] Istio. [Online]. Available: <https://istio.io/>
- [115] Consul by hashicorp. [Online]. Available: <https://www.consul.io/>
- [116] Rabbitmq. [Online]. Available: <https://www.rabbitmq.com/>
- [117] Aws — cloud computing. [Online]. Available: <https://aws.amazon.com/es/>
- [118] Ecs. [Online]. Available: <https://aws.amazon.com/es/ecs/>
- [119] Azure kubernetes service (aks) — microsoft azure. [Online]. Available: <https://azure.microsoft.com/es-es/products/kubernetes-service>
- [120] Remote method invocation (rmi). [Online]. Available: <https://www.javatpoint.com/RMI>
- [121] Java message service (jms). [Online]. Available: <https://www.oracle.com/java/technologies/java-message-service.html>
- [122] J. Bogner and A. Zimmermann, “Towards integrating microservices with adaptable enterprise architecture,” *2016 IEEE 20th International Enterprise Distributed Object Computing Workshop (EDOCW)*, pp. 1–6, 2016.
- [123] ¿qué es un esb (bus de servicio empresarial)? — ibm. [Online]. Available: <https://www.ibm.com/es-es/topics/esb>
- [124] A. Akbulut and H. G. Perros, “Software versioning with microservices through the api gateway design pattern,” in *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, 2019, pp. 289–292.
- [125] L. Weerasinghe and I. Perera, “An exploratory evaluation of replacing esb with microservices in service-oriented architecture,” *2021 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, vol. 4, pp. 137–144, 2021.
- [126] Http. [Online]. Available: <https://developer.mozilla.org/es/docs/Web/HTTP>

## REFERENCIAS

---

- [127] Uri. [Online]. Available: <https://developer.mozilla.org/es/docs/Glossary/URI>
- [128] Amqp. [Online]. Available: <https://www.amqp.org/>
- [129] Haproxy - the reliable, high perf. tcp/http load balancer. [Online]. Available: <https://www.haproxy.org/>
- [130] Advanced load balancer, web server, & reverse proxy - nginx. [Online]. Available: <https://www.nginx.com/>
- [131] Tornado web server. [Online]. Available: <https://www.tornadoweb.org/en/stable/index.html>
- [132] R. Kozik *et al.*, “Common representational model and ontologies for effective law enforcement solutions,” *Vietnam Journal of Computer Science*, vol. 07, no. 01, pp. 1–18, 2020.
- [133] Z. Zlatev, G. Veres, and Z. Sabeur, “Agile data fusion and knowledge base architecture for critical decision support,” *International Journal of Decision Support System Technology*, 2013.
- [134] E.-J. Behmer *et al.*, “Ontology population framework of magneto for instantiating heterogeneous forensic data modalities,” *null*, 2019.
- [135] Osint — incibe. [Online]. Available: <https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder>
- [136] Ubuntu 18.04.6 lts (bionic beaver). [Online]. Available: <https://releases.ubuntu.com/18.04/>
- [137] Webhdfs rest api. [Online]. Available: <https://hadoop.apache.org/docs/r1.0.4/webhdfs.html>
- [138] Python. [Online]. Available: <https://www.python.org/>
- [139] Cassandrarestfulapi. [Online]. Available: <https://github.com/rohitsakala/CassandraRestfulAPI>
- [140] Elasticsearch: Motor de búsqueda y analítica distribuido oficial. [Online]. Available: <https://www.elastic.co/es/elasticsearch>
- [141] Moses. [Online]. Available: <https://www2.statmt.org/moses/>
- [142] Treetagger. [Online]. Available: <https://www.cis.uni-muenchen.de/~schmid/tools/TreeTagger/>



- [143] Nltk :: Natural language toolkit. [Online]. Available: <https://www.nltk.org/>
- [144] Opencv - open computer vision library. [Online]. Available: <https://opencv.org/>
- [145] Ffmpeg. [Online]. Available: <https://ffmpeg.org/>
- [146] C. Szegedy, A. Toshev, and D. Erhan, “Deep neural networks for object detection,” *Advances in neural information processing systems*, vol. 26, 2013.
- [147] Speech-to-text: reconocimiento de voz automático. [Online]. Available: <https://cloud.google.com/speech-to-text>
- [148] Wit.ai. [Online]. Available: <https://wit.ai/>
- [149] Speech to text – audio to text translation — microsoft azure. [Online]. Available: <https://azure.microsoft.com/en-us/products/ai-services/speech-to-text>
- [150] Speech to text - ibm cloud. [Online]. Available: <https://cloud.ibm.com/catalog/services/speech-to-text>
- [151] Cmusphinx open source speech recognition. [Online]. Available: <https://cmusphinx.github.io/>
- [152] pyaudioanalysis: Python audio analysis library: Feature extraction, classification, segmentation and applications. [Online]. Available: <https://github.com/tyiannak/pyAudioAnalysis>
- [153] M. Richardson and P. Domingos, “Markov logic networks,” *Machine learning*, vol. 62, pp. 107–136, 2006.
- [154] F. J. M. Pérez *et al.*, “Multimedia analysis platform for crime prevention and investigation,” *Multimedia Tools and Applications*, 2021.
- [155] Tuffy: A scalable markov logic inference engine. [Online]. Available: <http://i.stanford.edu/hazy/tuffy/>
- [156] Apache jena fuseki. [Online]. Available: <https://jena.apache.org/documentation/fuseki2/>
- [157] Owl - semantic web standards. [Online]. Available: <https://www.w3.org/OWL/>

## REFERENCIAS

---

- [158] R. Segers *et al.*, “The event and implied situation ontology (ESO): Application and evaluation,” in *Proceedings of the Tenth International Conference on Language Resources and Evaluation (LREC’16)*. European Language Resources Association (ELRA), May 2016, pp. 1463–1470.
- [159] A. Pease, I. Niles, and J. Li, “The suggested upper merged ontology: A large ontology for the semantic web and its applications,” in *Working notes of the AAAI-2002 workshop on ontologies and the semantic web*, vol. 28, 2002, pp. 7–10.
- [160] Url (uniform resource locator). [Online]. Available: [https://www.techtarget.com/searchnetworking/definition/URL#:~:text=A%20URL%20\(Uniform%20Resource%20Locator\)%20is%20a%20unique%20identifier%20used,where%20to%20retrieve%20a%20resource](https://www.techtarget.com/searchnetworking/definition/URL#:~:text=A%20URL%20(Uniform%20Resource%20Locator)%20is%20a%20unique%20identifier%20used,where%20to%20retrieve%20a%20resource).
- [161] Microsoft word: software de procesamiento de textos. [Online]. Available: <https://www.microsoft.com/es-es/microsoft-365/word>
- [162] Apache tika. [Online]. Available: <https://tika.apache.org/>
- [163] Software de hojas de cálculo microsoft excel. [Online]. Available: <https://www.microsoft.com/es-es/microsoft-365/excel>
- [164] Oculus rift: Gafas de juegos de realidad. [Online]. Available: [https://www.oculus.com/rift-s/?locale=es\\_ES](https://www.oculus.com/rift-s/?locale=es_ES)
- [165] Luciad developer platform. [Online]. Available: <https://dev.luciad.com/portal/welcome/>
- [166] Vue.js. [Online]. Available: <https://vuejs.org/guide/introduction.html#what-is-vue>
- [167] Axios. [Online]. Available: <https://axios-http.com/es/docs/intro>
- [168] Expressjs. [Online]. Available: <https://expressjs.com/es/>
- [169] Node.js. [Online]. Available: <https://nodejs.org/en>
- [170] Socket.io. [Online]. Available: <https://socket.io/>
- [171] Ultraleap. [Online]. Available: <https://www.ultraleap.com/>
- [172] Keycloak. [Online]. Available: <https://www.keycloak.org/>
- [173] D. R. Perez, M. E. Domingo, I. Pérez-Llopis, and F. J. C. Rodrigo, “System and architecture of an adapted situation awareness tool for first responders.” in *ISCRAM*, 2020, pp. 928–936.

- [174] M. Esteve, I. Pérez-Llopis, L. Hernández-Blanco, A. Climente, and C. E. Palau, “Simacet-fft: Spanish army friendly force tracking system,” in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, 2009, pp. 1–7.
- [175] Upv universitat politècnica de valència. [Online]. Available: <https://www.upv.es/>
- [176] Mqtt - the standard for iot messaging. [Online]. Available: <https://mqtt.org/>
- [177] Nats docs. [Online]. Available: <https://docs.nats.io/>
- [178] Datagram delivery protocol (ddp). [Online]. Available: <https://www.geeksforgeeks.org/datagram-delivery-protocol-ddp/>
- [179] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: Vision and challenges,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.
- [180] Matrice dji enterprise. [Online]. Available: <https://enterprise.dji.com/es/matrice-300>
- [181] T. Mioch, R. Sterkenburg, T. Beuker, and M. A. Neerincx, “Actionable situation awareness: Supporting team decisions in hazardous situations.” in *ISCRAM*, 2021, pp. 62–70.
- [182] J. González-Villa, A. Cuesta, D. Alvear, and A. Balboa, “Evacuation management system for major disasters,” *Applied Sciences*, vol. 12, no. 15, 2022.
- [183] Rtsp: Real-time streaming protocol. [Online]. Available: <https://developer.mozilla.org/en-US/docs/Glossary/RTSP>
- [184] Sieć badawcza Łukasiewicz – przemysłowy instytut automatyki i pomiarów piap - strona sieci badawczej Łukasiewicz – przemysłowy instytut automatyki i pomiarów piap. [Online]. Available: <https://piap.lukasiewicz.gov.pl/en/>
- [185] Piap gryf). [Online]. Available: <https://www.antyterroryzm.com/wp-content/uploads/gryf.pdf>
- [186] Openjaus. [Online]. Available: <https://openjaus.com/understanding-jaus/>
- [187] Eclipse mosquito. [Online]. Available: <https://mosquitto.org/>

## REFERENCIAS

---

- [188] Webrtc. [Online]. Available: <https://webrtc.org/?hl=es-419>
- [189] cosinuss° two – cosinuss gmbh. [Online]. Available: <https://store.cosinuss.com/products/cosinuss-two?variant=32175832924242>
- [190] Bluetooth low energy protocol stack. [Online]. Available: [https://software-dl.ti.com/lprf/simplelink\\_cc2640r2\\_sdk/1.00.00.22/exports/docs/blestack/html/ble-stack/index.html](https://software-dl.ti.com/lprf/simplelink_cc2640r2_sdk/1.00.00.22/exports/docs/blestack/html/ble-stack/index.html)
- [191] Axis m1045-lw network camera. [Online]. Available: <https://www.axis.com/es-es/products/axis-m1045-lw/support>
- [192] Gps tracking software - traccar. [Online]. Available: <https://www.traccar.org/>
- [193] U. Srilakshmi *et al.*, “An improved hybrid secure multipath routing protocol for manet,” *IEEE Access*, vol. 9, pp. 163 043–163 053, 2021.
- [194] S. Sesia, S. Sesia, I. Toufik, M. Baker, and M. Baker, “Lte - the umts long term evolution: From theory to practice,” 2011.
- [195] Vmware vsphere. [Online]. Available: <https://www.vmware.com/es/products/vsphere.html>
- [196] Esxi— hipervisor bare metal. [Online]. Available: <https://www.vmware.com/es/products/esxi-and-esx.html>
- [197] Clearos. [Online]. Available: <https://www.clearos.com/>
- [198] The centos project. [Online]. Available: <https://www.centos.org/>
- [199] Protocolo de configuración dinámica de host (dhcp). [Online]. Available: <https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>
- [200] Dns. [Online]. Available: <https://aws.amazon.com/es/route53/what-is-dns/>
- [201] Elasticsearch documentation — elasticsearch 6.8.4.13. [Online]. Available: <https://elasticsearch.readthedocs.io/en/latest/#>
- [202] Docker engine overview — docker docs. [Online]. Available: <https://docs.docker.com/engine/>
- [203] Servidor de torre poweredge t640 — dell españa. [Online]. Available: <https://www.dell.com/es-es/shop/ipovw/poweredge-t640>

- [204] ds-py-tx2560-m2.pdf. [Online]. Available: <https://sp.ts.fujitsu.com/dmsp/Publications/public/ds-py-tx2560-m2.pdf>
- [205] Office of counter-terrorism —. [Online]. Available: <https://www.un.org/counterterrorism/>
- [206] I-lead — project — cordis — european commission. [Online]. Available: <https://cordis.europa.eu/project/id/740685/es>
- [207] Enlets. [Online]. Available: <https://enlets.eu/>
- [208] Kit intel® nuc 11 performance: Nuc11pahi7. [Online]. Available: <https://www.intel.la/content/www/xl/es/products/sku/205073/intel-nuc-11-performance-kit-nuc11pahi7/specifications.html>
- [209] Gezamenlijke brandweer. [Online]. Available: <https://www.gezamenlijke-brandweer.nl/>
- [210] İzmir İtfaiye dairesi başkanlığı. [Online]. Available: <https://itfaiye.izmir.bel.tr/en/about-training-center/1070/1180?AspxAutoDetectCookieSupport=1>
- [211] Acil afet ambulans hekimleri derneği – www.aahd.org.tr. [Online]. Available: <https://www.aahd.org.tr/>
- [212] Södertörns branförsvarsförbund fire brigade. [Online]. Available: <https://www.sbff.se/>
- [213] Cnbop. [Online]. Available: <https://www.cnbop.pl/en>
- [214] Portal web de la policía nacional española. [Online]. Available: [https://policia.es/\\_es/index.php](https://policia.es/_es/index.php)
- [215] Tedax-nrbq; policía nacional. [Online]. Available: [https://www.policia.es/\\_es/tupolicia\\_conocenos\\_estructura\\_dao\\_cginformacion\\_especialidades\\_tedax.php](https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cginformacion_especialidades_tedax.php)
- [216] Prevision – prediction and visual intelligence for security information. [Online]. Available: <http://www.prevision-h2020.eu/>
- [217] Copernicus. [Online]. Available: <https://www.copernicus.eu/en>