UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Arquitectura de interoperabilidad para mejorar la gestión y coordinación de múltiples *UXV* y la 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:
Alberto García García

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

A mi familia, a mi FAVmily y a Esther

gracias por estar siempre.

Resumen

Esta tesis se ha desarrollado dentro del marco de la interoperabilidad de seguridad, enfocándose en la colaboración de los proyectos CAMELOT y PREVISION, financiados por la Comisión Europea dentro del programa Horizonte 2020. Estos proyectos se han ejecutado en el grupo de investigación de Sistemas y Aplicaciones de Tiempo Real Distribuido (SATRD) del Departamento de Comunicaciones de la Universidad Politécnica de Valencia (UPV).

La libre circulación de personas y mercancías en la Unión Europea (UE) y la eliminación progresiva de los controles fronterizos, en virtud del acuerdo de *Schengen*, han presentado desafíos significativos en la seguridad de las fronteras exteriores europeas. Incidentes recientes, incluyendo oleadas de inmigración ilegal, la crisis de refugiados y ataques terroristas, han intensificado la necesidad de un control y vigilancia eficaces.

Esta tesis propone una arquitectura de interoperabilidad genérica, diseñada para integrar sistemas existentes y permitir el intercambio de datos a través de una plataforma unificada. Se ha prestado especial atención a la utilización de adaptadores para la conversión de datos entre los sistemas originales y la plataforma adoptada.

Posteriormente, la implementación de la arquitectura se ha validado en dos contextos distintos: el proyecto CAMELOT, centrado en la mejora de la gestión y control de las fronteras, y el proyecto PREVISION, enfocado en crear un entorno de respuesta rápida para la detección de amenazas como actos terroristas. Ambos proyectos se han validado mediante simulaciones en entornos reales, evaluando situaciones como el contrabando ilegal y la detección de tráfico con inmigrantes ilegales en CAMELOT, y el seguimiento de actividades terroristas en PREVISION. Las demostraciones han mostrado mejoras significativas gracias a las arquitecturas desarrolladas, recibiendo una valoración excelente y destacando su potencial para futuras implementaciones en diversos ámbitos.

RESUMEN

Resum

Aquesta tesi s'ha desenvolupat dins del marc de la interoperabilitat de seguretat, centrant-se en la col·laboració dels projectes CAMELOT i PREVISION, finançats per la Comissió Europea dins del programa Horitzó 2020. Aquests projectes s'han dut a terme en el grup de recerca de Sistemes i Aplicacions de Temps Real Distribuït (SATRD) del Departament de Comunicacions de la Universitat Politècnica de València (UPV).

La lliure circulació de persones i mercaderies a la Unió Europea (UE) i l'eliminació progressiva dels controls fronterers, en virtut de l'acord de Schengen, han presentat desafiaments significatius en la seguretat de les fronteres exteriors europees. Incidents recents, incloent onades d'immigració il·legal, la crisi de refugiats i atacs terroristes, han intensificat la necessitat d'un control i vigilància eficaços.

Aquesta tesi proposa una arquitectura d'interoperabilitat genèrica, dissenyada per integrar sistemes existents i permetre l'intercanvi de dades a través d'una plataforma unificada. S'ha prestat especial atenció a la utilització d'adaptadors per a la conversió de dades entre els sistemes originals i la plataforma adoptada.

Posteriorment, la implementació de l'arquitectura s'ha validat en dos contextos diferents: el projecte CAMELOT, centrat en la millora de la gestió i control de les fronteres, i el projecte PREVISION, enfocat en crear un entorn de resposta ràpida per a la detecció d'amenaces com actes terroristes. Ambdós projectes s'han validat mitjançant simulacions en entorns reals, avaluant situacions com el contraban il·legal i la detecció de tràfic amb immigrants il·legals en CAMELOT, i el seguiment d'activitats terroristes en PREVISION. Les demostracions han mostrat millores significatives gràcies a les arquitectures desenvolupades, rebent una valoració excel·lent i destacant el seu potencial per a futures implementacions en diversos àmbits.

Abstract

This thesis has been developed within the framework of security interoperability, focusing on the collaboration of the CAMELOT and PREVISION projects, funded by the European Commission under the Horizon 2020 program. These projects have been carried out in the research group of Distributed Real-Time Systems and Applications (SATRD) of the Communications Department at the Polytechnic University of Valencia (UPV).

The free movement of people and goods in the European Union (EU) and the gradual elimination of border controls, under the Schengen agreement, have presented significant challenges in the security of Europe's external borders. Recent incidents, including waves of illegal immigration, the refugee crisis, and terrorist attacks, have intensified the need for effective control and surveillance.

This thesis proposes a generic interoperability architecture, designed to integrate existing systems and enable data exchange through a unified platform. Special attention has been given to the use of adapters for the conversion of data between the original systems and the adopted platform.

Subsequently, the implementation of the architecture has been validated in two different contexts: the CAMELOT project, focused on improving border management and control, and the PREVISION project, aimed at creating a rapid response environment for the detection of threats such as terrorist acts. Both projects have been validated through simulations in real environments, evaluating situations such as illegal smuggling and detection of trafficking with illegal immigrants in CAMELOT, and monitoring of terrorist activities in PREVISION. The demonstrations have shown significant improvements thanks to the developed architectures, receiving excellent evaluations and highlighting their potential for future implementations in various fields.

ABSTRACT

Agradecimientos

Agradecimientos

A mi familia, por estar siempre apoyandome y ser uno de mis pilares fundamentales. Gracias por enseñarme a luchar por las cosas que quiero y por darme todo en esta vida.

A mi director, Manuel Esteve, gracias por confiar en mi y darme la oportunidad para que esta aventura haya sido posible.

A mi compañero, amigo y codirector, Francisco Pérez, por ser uno de mis referentes, un espejo en el que mirarse, gracias por tantas cosas, y en general, gracias a la vida por habernos cruzado. Siempre eres un apoyo, la tranquilidad, la paciencia cuando no sale algo y la esperanza de que algo mejor va a llegar. No tengo palabras para describir la admiración que siento por ti.

A mi compañero y amigo, Víctor Garrido, por ser un apoyo continuo, por estar siempre dispuesto a echar una mano, por remar en la misma dirección, por ser compañero de batalla. Llegaste a mi vida para quedarte, y ahora somos un trío inseparable. Nada podrá con nosotros.

Y por último, también me gustaría agradecer a la persona que me llena de felicidad, Esther Campoó, has llegado a mi vida poniéndola patas arriba, has conseguido que rompa barreras que no creía posible. Me estás enseñando lo que es el amor, la pasión y el ser un equipo. Solo han pasado unos meses y ya sé que eres el amor de mi vida, y que voy a tener todo contigo. Gracias por ser mi motivación, por darme ilusión, por confiar en mí, por darme tranquilidad, gracias por todo.

Muchas gracias a todos.

Alberto García García
Valencia, Diciembre de 2023

AGRADECIMIENTOS

Índice

Índice de figuras

ÍNDICE DE FIGURAS

Índice de tablas

ÍNDICE DE TABLAS

Acrónimos

3D	*3 dimensiones*
AATC	*Automatic Asset Tasking and Control*
API	*Application programming interface*
AUV	*Autonomous Underwater Vehicle*
AIS	*Automatic Identification System*
AR	*Augmented Reality*
AMQP	*Advanced Message Queuing Protocol*
ABD	*Anomalous Behavior Detection*
APP-6A	*Publicación Procedural Aliada*
CAMELOT	*C2 Advanced Multi-domain Environment and Live Observation Technologies*
C2	*Command & Control*
CISE	*Common Information Sharing Environment*
CAL	*CAMELOT adaptor layer*
C4I	*Command, control, communications, computers, intelligence*
CBRN	*Chemical, Biological, Radiological And Nuclear risks*
CRUD	*Create, Read, Update, Delete*
CEP	*Procesador de eventos complejos*
CIDOC CRM	*CIDOC Conceptual Reference Model*
CCTV	*Closed-circuit television*
CI/CD	*Continuous integration and continuous deployment*
CPU	*Central processing unit*

CRM	*Conceptual Reference Model*
DMA	*Data management and analitycs*
DNS	*Domain Name System*
DHCP	*Dynamic Host Configuration Protocol*
EWE	*Early Warning Engine*
ETL	*Extract, transform and load*
ERTZ	*Ertzaintza*
ESXI	*Elastic Sky X integrated*
EXDL	*Extensible data language*
FALCON	*Fight against large-scale corruption and organised crime networks*
GIS	*Geographic Information System*
GCS	*Ground Control Station*
GUI	*Graphical User Interface*
GDPR	*General Data Protection Regulation*
HDFS	*Hadoop Distributed File System*
HMI	*Human Machine Interface*
HMD	*Helmet-mounted display*
HTTP	*Hypertext Transfer Protocol*
ID	*Identificator*
ICOM	*International Council of Museums*
IA	*Inteligencia artificial*
ISO	*International Organization for Standardization*
IoT	*Internet of things*
IP	*Internet Protocol*
JSON	*JavaScript Object Notation*
KLV	*Value-Length-Key*
KML	*Keyhole Markup Language*
KB	*Knowledge base*
KPI	*Key performance indicator*
LEA	*Law Enforcement Agency*
LBS	*Sound based in Location*

LDS	*Conjunto de datos locales*
LOS	*Line of sight*
LETSCROWD	*Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs*
MMKP	*Mind Mapping Knowledgebase Prototyping*
MISB	*Motion imagery standards board*
MLN	*Markov logical network*
MIT	*Massachusetts Institute of Technology*
MPEG4	*Moving Picture Experts Group*
MQTT	*Message Queuing Telemetry Transport*
MOE	*Métricas de Efectividad Operativa*
MSC	*Munich Security Conference*
MR	*Mixed reality*
NoSQL	*Not-Only SQL*
NMEA	*National Marine Electronics Association*
NIEM	*National information exchange model*
OP	*Orientation problem*
OEM	*Original equipment manufacturer*
OTAN	*Organización del Tratado del Atlántico Norte*
OSINT	*Open source intelligence*
PREVISION	*Prediction and Visual Intelligence for Security Information*
PC	*Personal computer*
PVI	*Person and vehicle identification*
PGP	*Pretty Good Privacy*
RF	*Radiofrequency*
REST	*Representation state transfer*
ROV	*Remote Operated Vehicle*
RPC	*Remote Procedure Call*
STANAG	*Standardization Agreement*
SOA	*Service-oriented architecture*
STOMP	*Simple text-oriented messaging protocol*
SMAUG	*Smart Maritime and Underwater Guardian*

SOAP	*Simple object access protocol*
SPARQL	*Language for querying databases stored as RDF*
SSH	*Secure Shell*
TOP	*Team orientation problem*
TV	*Television*
TCP	*Transmission Control Protocol*
UCS	*Unmanned Control System*
UAS	*Unmanned Aerial System*
UxV	*Unmanned vehicles*
UUV	*Unmanned Underwater Vehicles*
USB	*Bus serie universal*
URL	*Uniform Resource Locator*
UGV	*Unmanned ground vehicle*
UAV	*Unmanned Aerial Vehicles*
UPV	*Universidad Politécnica de Valencia*
VPN	*Virtual Private Network*
VR	*Virtual reality*
XML	*eXtensible Markup Language*
xR	*Extended reality*

Capítulo 1

Introducción

1.1. Introducción

Abordando el ámbito de la seguridad transfronteriza, la vigilancia, supervisión y la adaptabilidad a la gestión de cualquier evento con el fin de predecir e interponerse a cualquier suceso, se han realizado diversos análisis que hacen hincapié en la importancia de la adopción de un plan de choque que ayude a generar mejores tomas de decisión.

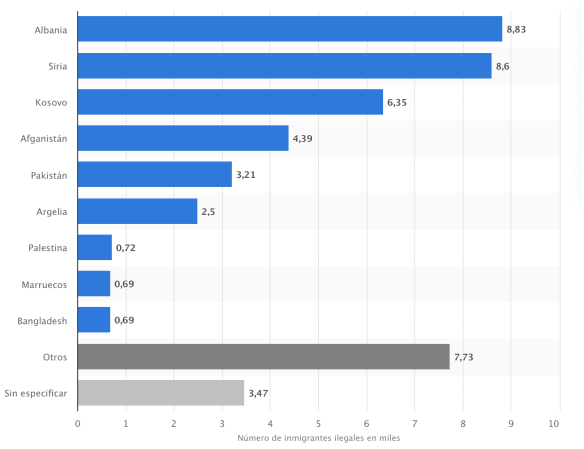

Figura 1.1: Comparativa inmigrantes ilegales diversos países [1]

Según varios estudios que revela la Agencia Europea de la Guardia de Fronteras y Costas, alrededor de 700 millones de personas cruzan las fronteras exteriores de Europa cada año [2]. Esto crea la necesidad de detectar cualquier actividad ilegal sin causar retrasos u obstáculos.

Durante 2018, diversas autoridades nacionales trabajando en colaboración detuvieron más de 15 toneladas de cocaína y 46 toneladas de cannabis en las regiones del Atlántico y el Mediterráneo, según los datos extraídos por el Centro de Análisis y Operaciones Marítimas [3].

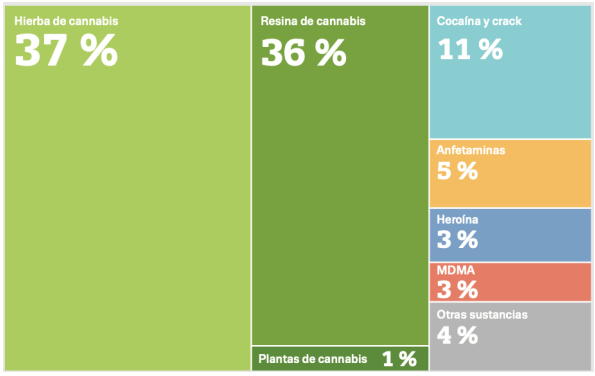

Figura 1.2: Número de incautaciones de drogas notificadas, desglose por drogas, 2019 [4]

Cada Estado miembro y cada profesional de fronteras explotan su propio conjunto de activos por el único objetivo de vigilancia y control. Los Estados han ido realizando importantes inversiones en los activos e infraestructuras necesarias para gestionar y controlar el tránsito en las zonas fronterizas [5].

A medida que los actuales *Command & Control* (C2) envejecen, los profesionales del control fronterizo se enfrentan a un reto cada vez mayor, ya que deben integrar los nuevos activos, para que, deforma coordinada con los antiguos, puedan trabajar de forma coordinada y coherente, sin tener que invertir tiempo extra en construirlo desde cero [6]. Para facilitar esta tarea, se ha diseñado y desarrollado una plataforma distribuida en el marco del proyecto *C2 Advanced Multi-domain Environment and Live Observation Technologies* (CAMELOT) [7], fundado por la Unión Europea.

CAMELOT se basa en los trabajos del segmento de control de sistemas aéreos no tripulados *Unmanned Control System* (UCS) [8] y de *Common Information Sharing Environment* (CISE) 2020 [9].

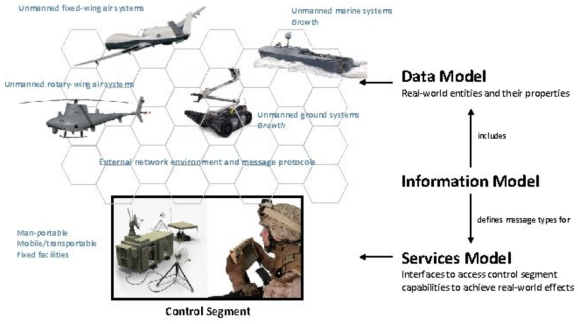

Figura 1.3: Modelo del segmento de control de sistemas aéreos no tripulados.

Por otro lado, las amenazas emergentes causadas por el terrorismo, la delincuencia organizada y la ciberdelincuencia como retos transfronterizos interrelacionados están demostrando hoy en día lo importante que es una respuesta europea conjunta a estas amenazas. Especialmente la protección de los llamados *soft targets* es un reto para las fuerzas de seguridad de toda Europa. En estos casos complejos, los investigadores también se enfrentan cada vez más a enormes cantidades de datos, que deben ser analizados en poco tiempo. La naturaleza heterogénea de estos flujos de datos obliga a las *Law Enforcement Agency* (LEA) a establecer vínculos y prioridades para poder comprenderlos y analizarlos [10].

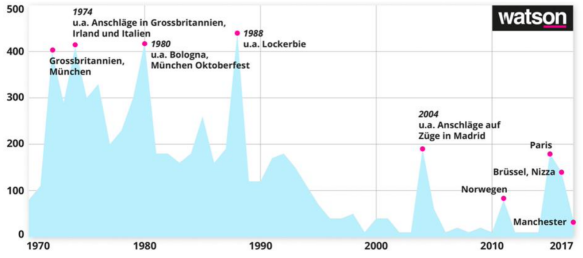

Figura 1.4: Víctimas del terrorismo al oeste de Europa [11]

El proyecto *Prediction and Visual Intelligence for Security Information* (PREVISION) [12] pretende mejorar las capacidades operativas de las LEA proporcionando una plataforma única e innovadora. Y es que es sencillamente imposible lograr una seguridad total. Toda sociedad se enfrenta a comporta-

mientos diferentes y delictivos. La delincuencia es un fenómeno social normal. Sin embargo, todo Estado tiene la obligación de proteger a sus ciudadanos de la delincuencia y las amenazas terroristas. Esto es cada vez más difícil en el contexto de la globalización y el creciente desarrollo tecnológico [13]. Las amenazas deben ser analizadas de forma rápida y objetiva para que las autoridades competentes puedan reaccionar con prontitud ante futuros riesgos sobre la base de previsiones.

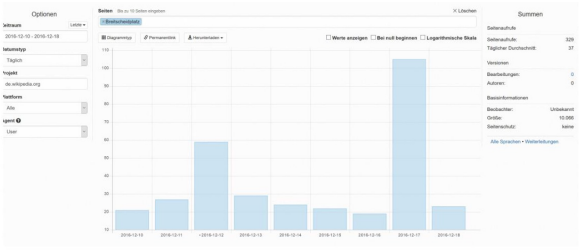

Figura 1.5: Ejemplo de la actividad web en Wikipedia para el artículo "Breitscheidplatz"antes del atentado terrorista en Berlín del 19 de diciembre de 2016.

La implementación de la policía predictiva busca optimizar la efectividad y eficiencia de las operaciones policiales. Sin embargo, para lograr su máximo potencial, es imperativo que se integre profundamente y de manera sostenible tanto en los procesos operativos como en la cultura de la autoridad policial [14]. La efectividad de la policía predictiva se ve comprometida si no logra obtener la aceptación de los oficiales que operan en los sistemas pertinentes, especialmente aquellos que deben implementar estas medidas en su rutina operativa diaria.

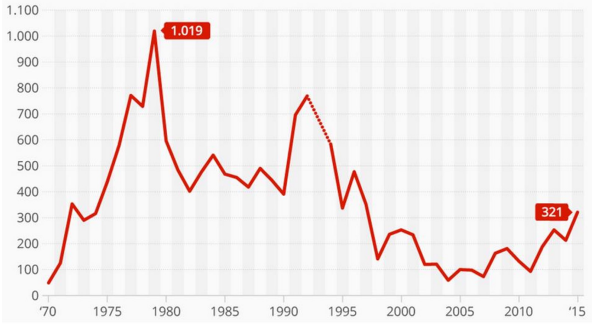

Figura 1.6: Ataques terroristas al oeste de Europa por año [15]

La policía predictiva es todavía una rama bastante joven pero muy dinámica de la investigación criminológica y del trabajo policial. Especialmente en Estados Unidos, pero también cada vez más en países europeos. Además de la lucha contra la delincuencia clásica, la policía predictiva adquiere cada vez más importancia en el ámbito de la lucha contra el terrorismo, no solo para predecir los atentados terroristas, sino también el curso de la radicalización.

1.2. Motivaciones

El desarrollo de esta tesis, abarcando aspectos teóricos y prácticos, se ha situado dentro del ámbito de la defensa y la seguridad, concretándose en dos aplicaciones clave. Se ha llevado a cabo el diseño y ejecución de arquitecturas especializadas para la integración de múltiples fuentes de datos, promoviendo así la interoperabilidad entre dispositivos y plataformas.

Se presentan a continuación las motivaciones principales de esta investigación doctoral:

- **Interoperabilidad**

  Diversas agencias y empresas operan con herramientas específicas para la gestión de incidentes, diseñadas conforme a sus requisitos. La colaboración entre estas entidades, sin embargo, a menudo se ve obstaculizada por la falta de uniformidad. Surge, por tanto, la necesidad de un sistema que pueda consolidar diferentes tipos de datos para una gestión eficiente y ágil de incidentes.

- **Especificación de una Arquitectura Adaptativa**

  La arquitectura propuesta se caracteriza por su versatilidad, adaptándose a diversos escenarios y requerimientos. Esto facilita la incorporación de herramientas de distintas generaciones tecnológicas.

- **Aplicabilidad de la Plataforma**

  La plataforma ha sido diseñada considerando su adaptabilidad a variados entornos y situaciones, con módulos flexibles que permiten el acceso a la información por parte de diferentes herramientas, facilitando su empleo en una amplia gama de contextos.

- **Diseño de un Modelo de Datos Unificado para el Intercambio de Información**

  Mediante adaptadores específicos, la plataforma puede procesar diversas fuentes de datos, transformándolos a un formato estandarizado para garantizar su funcionalidad óptima.

- **Técnicas Avanzadas de Visualización Geoespacial**

  Se han implementado técnicas avanzadas para la visualización y manejo de datos geoespaciales en tiempo real. La plataforma CAMELOT, por ejemplo, gestiona diferentes sistemas aéreos y terrestres no tripulados (UxV) a través de su portal de visualización geoespecial, aportando un valor añadido respecto a otras soluciones del mercado.

- **Eficiencia y Optimización en la Gestión de Incidentes**

  En el proyecto CAMELOT, se pone énfasis en la capacidad de operar en distintos entornos (terrestre, marítimo y aéreo) utilizando una única plataforma para optimizar la gestión de misiones. De manera similar, en el proyecto PREVISION, la incorporación de datos textuales, sonoros y visuales contribuye a mejorar la eficiencia y optimización en la gestión de incidentes.

- **Manejabilidad y Respuesta ante Incidentes**

  Una plataforma eficaz debe ser intuitiva y fácil de manejar. Por ello, se han tomado en cuenta las directrices de los usuarios finales, asegurando que las herramientas desarrolladas sean no solo efectivas, sino también accesibles y amigables para el usuario.

1.3. Objetivos de la tesis

A partir de las motivaciones discutidas anteriormente, se establecen los siguientes objetivos para esta tesis:

- **Análisis del Estado del Arte**: Realizar una evaluación exhaustiva del panorama actual en herramientas de respuesta a incidentes, identificando tanto deficiencias como oportunidades de mejora.

- **Fomentar la Interoperabilidad de Herramientas**: Establecer adaptadores especializados que aseguren la interoperabilidad efectiva entre herramientas existentes y emergentes.

- **Desarrollo de una Arquitectura Integral**: Diseñar una arquitectura sólida y coherente que soporte la interoperabilidad total, basada en los hallazgos y requerimientos surgidos durante la investigación.

- **Validación en Escenarios Reales**: Conducir análisis prácticos para evaluar la funcionalidad de la aplicación en contextos reales, alineándola con los objetivos de los proyectos de investigación asociados.

- **Optimización de la Comunicación**: Desarrollar sistemas de comunicación eficientes para facilitar el acceso a información dispersa en variados entornos y situaciones.

- **Implementación en el Proyecto CAMELOT**: Aplicar y valorar el modelo de datos y la arquitectura en contextos relacionados con CAMELOT, enfocándose en reforzar la seguridad y mejorar la gestión y ejecución de operaciones fronterizas.

- **Implementación en el Proyecto PREVISION**: Aplicar y testar el modelo de datos y la arquitectura en escenarios del proyecto PREVISION, buscando anticipar y responder de manera proactiva a incidentes potenciales.

- **Estudio de las Mejoras Alcanzadas**: Investigar y valorar los beneficios y mejoras logradas con la implementación del modelo y la arquitectura en ambos proyectos, identificando recomendaciones y áreas de mejora para futuras aplicaciones.

1.4. Principales aportaciones

1.4.1. Artículos

- **García-García, Alberto**; Pérez-Carrasco, Francisco José; Garrido-Peñalver, Víctor Javier; Zambrano-Vizuete, Oscar Marcelo; Rafal Kozik; Michal Choras ... Wilmuth Müller. (2021) *Multimedia analysis platform for crime prevention and investigation. Multimedia Tools and Applications* - . 10.1007/s11042-020-10206-y

- **García-García, Alberto**; Pérez-Carrasco, Francisco José; Garrido-Peñalver, Víctor Javier; Esteve Domingo, Manuel; Zambrano-Vizuete, Oscar Marcelo. (2021) *C2 Advanced Multi-domain Environment and Live Observation Technologies. International Journal of Computers Communications & Control*, 6 (16), - . 10.15837/ijccc.2021.6.4251

1.4.2. Congresos y Jornadas

- **García-García, Alberto** (2021). Proyectos europeos H2020: CAMELOT. Día Nacional de las Telecomunicaciones 2021. Online.

- **García-García, Alberto** (2021). Encuentro de Investigación Tecnológica (RITAM 2021) - PREVISION. EN II Encuentro de Investigación Tecnológica (RITAM 2021). Online.
- **García-García, Alberto** (2021). European project H2020: PREVISION. EN II International Congress of Research and Innovation (CI3 2021). Sangolquí, Ecuador.
- **García-García, Alberto**; Pérez-Carrasco, Francisco José; Garrido-Peñalver, Víctor Javier; Zambrano-Vizuete, Oscar Marcelo; Rafal Kozik; Michal Choras ... Wilmuth Müller (2019). Multimedia Analysis and correlation engine for organised crime prevention and investigation. EN 1st International Conference on Applied Technologies (ICAT 2019). (1 - 15). Quito, Ecuador: Springer.
- Pérez-Carrasco, Francisco José; **García-García, Alberto**; Garrido-Peñalver, Víctor Javier; Zambrano-Vizuete, Oscar Marcelo (2019). C2 Advanced Multi-domain Environment and Live Observation Technologies. EN 1st International Conference on Applied Technologies (ICAT 2019). (1 - 12). Quito, Ecuador: Springer.

1.4.3. Proyectos de investigación

- Proyecto CAMELOT:
  - **WP.2 Requisitos de usuario**. En este paquete, se recopilaron y analizaron las necesidades y requisitos específicos de los usuarios finales para el desarrollo y funcionamiento del sistema.
  - **WP.3 Arquitectura del sistema**. Se diseñó la estructura y las especificaciones del sistema, tomando en cuenta la interoperabilidad y la eficiencia en la integración de las distintas herramientas.
  - **WP.4 Recogida de datos y correlación**. Se establecieron métodos para la recopilación de datos de distintas fuentes y se desarrollaron algoritmos para la correlación de esta información.
  - **WP.5 Visualización**. Se trabajó en la creación de interfaces gráficas intuitivas y efectivas para la representación y análisis de datos.
  - **WP.6 Integración y prototipado**. Se llevó a cabo la fase de integración de los diferentes componentes del sistema y se desarrollaron prototipos para pruebas iniciales.
  - **WP.7 Evaluación y validación del sistema**. Una vez finalizado el prototipo, se sometió a diferentes pruebas para evaluar su funcionalidad y garantizar su correcta operación.

- Proyecto PREVISION:
  - **WP.3 Requisitos de los usuarios y escenarios de riesgo**. Se recogieron las necesidades de los usuarios y se diseñaron escenarios de riesgo para anticipar posibles incidentes.
  - **WP.4 Conciencia de la situación de la ciberseguridad**. Se abordaron temas de ciberseguridad, estableciendo mecanismos de alerta y respuesta a amenazas en el ámbito digital.
  - **WP.5 Conciencia de la situación física**. Se trabajó en la detección y respuesta a amenazas en el ámbito físico, como la seguridad de infraestructuras.
  - **WP.6 Conocimiento de la situación híbrida**. Este paquete abordó la integración de las alertas y respuestas tanto en el ámbito digital como físico.
  - **WP.7 Comunicación con el público e interoperabilidad**. Se establecieron protocolos de comunicación con el público y se trabajó en la interoperabilidad de las herramientas y sistemas utilizados.
  - **WP.8 Demostración y validación del sistema**. Se presentaron demostraciones del sistema y se realizaron pruebas de validación para garantizar su correcta funcionalidad.

1.4.4. Desarrollo software

En el marco de los proyectos CAMELOT y PREVISION, mi aportación ha sido destacada en el ámbito del desarrollo de software, con énfasis en las siguientes áreas:

- **Adaptadores de Interoperabilidad**: Estos elementos son clave para asegurar la colaboración efectiva entre diversas herramientas y sistemas. He diseñado y desarrollado software que sirve como conexión entre distintos entornos y plataformas, facilitando la transformación y transferencia eficiente de datos. Estos adaptadores son vitales para la comunicación fluida y el intercambio de datos entre todos los componentes implicados en los proyectos.
- **Módulos Centrales de la Plataforma**: Constituyen la base de ambos proyectos, siendo fundamentales para las operaciones principales de las plataformas. Mi labor se ha enfocado en desarrollar módulos robustos y escalables capaces de procesar, analizar y manejar grandes volúmenes de datos en tiempo real. Estos módulos aseguran que la plataforma pueda

reaccionar con prontitud ante incidentes y brindar información crucial a los usuarios.

- **Componente Principal o Interfaz Hombre-Máquina (HMI)**: Un elemento crítico en cualquier sistema es la manera en que los usuarios interactúan con él. La HMI es la interfaz que facilita esta interacción. He contribuido al diseño y desarrollo de interfaces intuitivas y accesibles que ofrecen una visión clara y permiten tomar decisiones informadas de manera rápida. Este componente también ha sido optimizado para asegurar que la presentación de datos sea clara y comprensible, especialmente bajo condiciones de alta presión.

Estos desarrollos representan no solo la creación de software funcional, sino también la garantía de que este sea seguro, fiable y cumpla con los estrictos requerimientos de los campos de defensa y seguridad. Mis contribuciones reflejan mi habilidad y compromiso para desarrollar soluciones tecnológicas avanzadas que enfrentan los retos actuales en el ámbito de la seguridad y la defensa.

1.5. Organización de la memoria

La estructura de la tesis se ha organizado de la siguiente manera:

- El capítulo 2 ofrece un análisis del estado del arte en la gestión de la vigilancia y la prevención de incidencias. Se enfoca en la importancia de soluciones colaborativas para el intercambio de información y procedimientos entre diferentes agencias en situaciones de crisis, así como en la evaluación del estado actual de las herramientas y mecanismos de interoperabilidad en la gestión de misiones e incidencias.

- En el capítulo 3, se presenta la arquitectura general propuesta, incluyendo una descripción de alto nivel de sus distintos módulos y las configuraciones posibles.

- El capítulo 4 detalla la implementación de la arquitectura en el caso de uso de CAMELOT. Se describen los módulos principales, los servicios compartidos por las herramientas de terceros a través del HMI desarrollado, y los logros alcanzados al finalizar el proyecto.

- El capítulo 5 se centra en la aplicación de la arquitectura en el caso de uso de PREVISION. Incluye una descripción del funcionamiento de los módulos principales, los servicios de herramientas de terceros integrados en el HMI y los resultados obtenidos tras la finalización del proyecto.

- En el capítulo 6, se realiza la evaluación de los sistemas diseñados para el proyecto CAMELOT. Este capítulo incluye los escenarios de prueba usados para validar el proyecto y los resultados obtenidos de una encuesta.
- El capítulo 6, dedicado a la evaluación de los sistemas en el proyecto PREVISION, describe los escenarios de prueba y los hallazgos de una encuesta realizada para validar el proyecto.
- El capítulo 7 aborda las conclusiones derivadas de la investigación y propone futuras líneas de investigación.
- Finalmente, se incluyen las referencias bibliográficas citadas en la tesis.

En resumen, esta memoria guía al lector en un viaje desde el reconocimiento de los problemas existentes y las necesidades en el sector, a través del diseño y la aplicación de soluciones innovadoras, hasta la evaluación y reflexión sobre los resultados y posibles futuros desarrollos. Este documento es un reflejo del esfuerzo y la dedicación invertidos en la investigación y el desarrollo en el campo de la defensa y seguridad.

Capítulo 2

Estado del arte

2.1. Introducción

En el dinámico panorama de la seguridad global, la cooperación entre agencias de control de fronteras y de investigación criminal juega un papel crucial. Este capítulo se enfoca en el análisis del estado actual de esta colaboración, poniendo especial énfasis en las necesidades y desafíos que enfrentan estas agencias, tanto en contextos nacionales como internacionales. La interacción eficiente y efectiva entre estas entidades es esencial para enfrentar y resolver casos complejos con repercusiones a nivel global.

Las agencias de control de fronteras tienen la responsabilidad de gestionar y supervisar el movimiento transfronterizo de personas y bienes, desempeñando un papel clave en la prevención de actividades ilícitas como el tráfico de drogas, la trata de personas y el contrabando. La eficacia de estas agencias depende de su capacidad para recolectar, procesar y compartir información de forma rápida y segura.

Por otro lado, las agencias dedicadas a la investigación criminal se centran en una amplia gama de delitos que pueden tener implicaciones internacionales. Estas agencias se enfrentan a desafíos únicos relacionados con la coordinación y cooperación entre diferentes jurisdicciones y países. Su trabajo implica no solo la investigación y prevención de delitos dentro de las fronteras nacionales, sino también el manejo de casos que requieren colaboración internacional, como el terrorismo, la ciberdelincuencia y los delitos financieros transnacionales.

Ambas entidades se enfrentan a retos comunes, entre los que se incluyen la necesidad de gestionar grandes volúmenes de datos, la integración de tecnologías avanzadas para el procesamiento y análisis de esta información, y la

implementación de sistemas seguros y eficientes para el intercambio de datos entre diversas agencias y países [16].

Este capítulo tiene como objetivo profundizar en la comprensión de cómo las agencias de control de fronteras y de investigación criminal pueden colaborar de manera más efectiva. Se explorarán las tecnologías modernas y las prácticas operativas que pueden ayudar a superar los obstáculos actuales y mejorar la seguridad y la eficacia en la lucha contra el crimen y la protección de las fronteras.

2.2. Cooperación entre agencias en la actualidad

2.2.1. Acceso y recolección de datos

El acceso y la recolección de datos constituyen un pilar crítico en las operaciones de las agencias de control de fronteras y de investigación criminal. A pesar de su importancia, las metodologías y herramientas empleadas a menudo se basan en tecnologías más rudimentarias, presentando así varios retos en términos de eficacia y eficiencia [17][18].

Herramientas y Tecnologías Predominantes

- **Cámaras de Circuito Cerrado de Televisión (CCTV):** Estas cámaras son ubicuas en las operaciones de seguridad, pero a menudo sufren de limitaciones como baja resolución, campos de visión restringidos y la necesidad de monitoreo humano constante.
- **Radares y Sensores:** Usados extensamente en zonas fronterizas, los radares y sensores son eficaces para la vigilancia de áreas amplias. Sin embargo, su eficiencia puede verse comprometida por condiciones ambientales adversas o tácticas de evasión avanzadas.
- **Bases de Datos Tradicionales:** Estas bases de datos a menudo enfrentan desafíos en términos de interconectividad, actualizaciones y accesibilidad, lo que limita el análisis en tiempo real y la capacidad de respuesta rápida.
- **Equipos de Vigilancia Manual:** Muchas operaciones todavía dependen en gran medida del monitoreo manual, lo que no solo es intensivo en recursos humanos, sino también propenso a errores y limitaciones humanas.

Desafíos en la Recolección de Datos

- **Limitaciones en la Integración de Datos:** La recolección de datos se ve frecuentemente obstaculizada por la falta de sistemas interoperables y la ausencia de estándares unificados para el intercambio de datos.
- **Dependencia de la Vigilancia Manual:** La escasez de tecnologías avanzadas de análisis conlleva una dependencia excesiva del análisis manual, aumentando la probabilidad de errores y reduciendo la eficiencia operativa.
- **Incapacidad para Manejar Grandes Volúmenes de Datos:** Las herramientas convencionales no están equipadas para procesar ni analizar de manera efectiva el creciente volumen de datos generados, lo que resulta en una significativa pérdida de información potencialmente valiosa.
- **Reticencia a la Adopción de Nuevas Tecnologías:** A menudo existe una resistencia institucional a la implementación de nuevas tecnologías, lo que puede ser un obstáculo para la modernización de los procesos de recolección de datos.
- **Problemas de Privacidad y Ética:** El uso de tecnologías de vigilancia plantea cuestiones de privacidad y ética, especialmente cuando se trata de la recolección y almacenamiento de datos personales.

Estos retos destacan la necesidad urgente de modernización en el área de recolección de datos para las agencias de control de fronteras y de investigación criminal, con el objetivo de incrementar la eficiencia, precisión y capacidad de respuesta ante amenazas de seguridad.

2.2.2. Análisis y extracción de inteligencia

El análisis y la extracción de inteligencia en las agencias de control de fronteras y de investigación criminal a menudo se caracterizan por enfoques rudimentarios, que limitan significativamente la eficacia y profundidad del análisis de inteligencia [19][20].

Enfoques y Metodologías Predominantes

- **Análisis Manual de Datos:** La mayoría de las operaciones se basan en la interpretación manual de datos, lo que no solo es laborioso y consume tiempo, sino que también está sujeto a sesgos y errores humanos.

- **Uso Limitado de Herramientas Analíticas:** Las herramientas analíticas disponibles son a menudo básicas, careciendo de la capacidad para realizar análisis complejos o extraer patrones significativos de grandes conjuntos de datos.
- **Dependencia de Informes Estáticos:** Se tiende a depender de informes estáticos y análisis retrospectivos que no capturan dinámicas en tiempo real ni permiten la anticipación proactiva de amenazas.
- **Falta de Integración y Análisis Interconectado:** Existe una carencia significativa en la capacidad de integrar y analizar datos de múltiples fuentes, lo que limita la comprensión holística de situaciones complejas.

Desafíos en el Análisis y Extracción de Inteligencia

- **Incapacidad para Manejar la Diversidad de Datos:** Las herramientas rudimentarias actuales no están equipadas para analizar efectivamente la variedad y complejidad de datos disponibles, desde comunicaciones digitales hasta señales de inteligencia geoespacial.
- **Dificultades en la Identificación de Patrones y Conexiones:** La falta de tecnologías analíticas avanzadas impide la identificación eficiente de patrones ocultos y conexiones entre diferentes fragmentos de datos.
- **Retrasos en la Extracción de Inteligencia Accionable:** El enfoque manual y las herramientas básicas conducen a retrasos significativos en la extracción de inteligencia accionable, lo que puede ser crítico en situaciones de seguridad.
- **Falta de Capacidades Predictivas:** Actualmente, hay una capacidad limitada para realizar análisis predictivos, lo que reduce la capacidad de las agencias para anticipar y prevenir actividades delictivas o amenazas a la seguridad.
- **Barreras para la Adopción de Tecnologías Innovadoras:** Existe una resistencia institucional y desafíos logísticos en la adopción de nuevas tecnologías analíticas, lo que frena la modernización del análisis de inteligencia.

Estos desafíos destacan la necesidad crítica de mejorar las capacidades analíticas en las agencias de control de fronteras y de investigación criminal, adoptando tecnologías avanzadas y metodologías innovadoras para un análisis y una extracción de inteligencia más efectivos y eficientes.

2.2.3. Intercambio de información

El intercambio de información entre agencias de control de fronteras y de investigación criminal es un pilar fundamental en la lucha contra el crimen y la protección de la seguridad nacional e internacional [21]. Sin embargo, actualmente este proceso enfrenta serias limitaciones debido a la falta de interoperabilidad y a métodos y protocolos obsoletos, lo que representa un desafío considerable para la eficacia operativa de las agencias involucradas [22].

Desafíos y Limitaciones en el Intercambio de Información

- **Incompatibilidad Técnica:** La diversidad de sistemas de información y la ausencia de estándares técnicos comunes impiden un intercambio de datos fluido y automático entre las distintas agencias.
- **Problemas de Comunicación y Coordinación:** La falta de un marco común para la comunicación y la coordinación interagencial obstaculiza la colaboración efectiva, especialmente en operaciones conjuntas o en la respuesta a incidentes transfronterizos.
- **Dificultades en la Gestión de Datos Sensibles:** La gestión de datos sensibles y clasificados se ve complicada por la falta de protocolos de seguridad unificados, lo que incrementa el riesgo de fugas de información y mal uso de los datos.
- **Retrasos en la Toma de Decisiones:** La dependencia de procesos manuales y la falta de automatización en el intercambio de información conllevan retrasos significativos en la toma de decisiones operativas y estratégicas.
- **Barreras Jurisdiccionales y Normativas:** Las diferencias en las regulaciones y leyes nacionales e internacionales generan barreras adicionales para el intercambio efectivo de información entre países.

Consecuencias Operativas de los Desafíos en el Intercambio de Información

- **Ineficiencia en Respuestas a Crisis:** La ineficacia en el intercambio de información crucial puede llevar a respuestas tardías o inadecuadas en situaciones de crisis o emergencias de seguridad.
- **Redundancia de Datos y Esfuerzos:** La falta de un sistema de intercambio eficiente a menudo resulta en la recopilación y procesamiento redundante de datos, desperdiciando recursos valiosos y tiempo.

- **Riesgos de Seguridad Nacional:** La incapacidad para compartir información de manera rápida y eficiente puede comprometer la seguridad nacional y la protección contra amenazas transnacionales.
- **Desafíos en la Lucha Contra el Crimen Organizado:** Los obstáculos en el intercambio de información dificultan el seguimiento y la desarticulación de redes criminales organizadas que operan a través de fronteras nacionales.
- **Limitaciones en Análisis Predictivo y Preventivo:** La falta de intercambio fluido de datos limita la capacidad de las agencias para realizar análisis predictivos y preventivos, clave en la lucha contra el crimen y el terrorismo.

Para superar estos desafíos, se requiere una transformación significativa en la manera en que las agencias de control de fronteras y de investigación criminal intercambian información. Es imperativo desarrollar e implementar soluciones tecnológicas avanzadas y estandarizadas que permitan un intercambio de datos seguro, rápido y eficiente. Esto incluye la adopción de protocolos de seguridad robustos, la estandarización de formatos de datos y la mejora en la interoperabilidad de los sistemas de información. Además, es crucial trabajar hacia una mayor armonización de las regulaciones y políticas a nivel internacional para facilitar un intercambio de información más fluido y efectivo entre agencias de diferentes países.

2.3. Problemas y desafíos identificados

2.3.1. Heterogeneidad en fuentes de datos y protocolos

Continuando con el análisis de los desafíos identificados en la cooperación entre agencias de control de fronteras y de investigación criminal, un aspecto fundamental es la heterogeneidad en las fuentes de datos y protocolos utilizados. Esta heterogeneidad no solo se manifiesta en la diversidad de plataformas y formatos, sino también en la utilización de tecnologías específicas como los *Unmanned vehicles* (UxV)s, que incluyen drones y otros sistemas autónomos [23].

Diversidad de Fuentes de Datos

- **Variedad de Plataformas y Formatos:** Las agencias utilizan una amplia gama de plataformas de datos, cada una con sus propios formatos y estándares. Esto incluye sistemas de información geográfica, bases de

datos de inteligencia, registros de vigilancia, y más, ocasionando una falta de uniformidad.

- **Datos No Estructurados y Estructurados:** Se manejan tanto datos estructurados (como registros y bases de datos) como no estructurados (como comunicaciones interceptadas y vídeos de vigilancia), complicando la integración y análisis de los mismos.
- **Fuentes de Datos Dispersas:** Los datos provienen de múltiples fuentes, incluyendo sensores, cámaras de *Closed-circuit television* (CCTV), bases de datos nacionales e internacionales, y plataformas en línea, dificultando su recolección y análisis centralizado.

Incompatibilidad de Protocolos

- **Falta de Estándares Comunes:** La ausencia de protocolos estandarizados entre diferentes agencias y países conduce a incompatibilidades que obstaculizan la colaboración y el intercambio de datos.
- **Diferentes Niveles de Acceso y Seguridad:** Cada agencia puede tener diferentes niveles de seguridad y protocolos de acceso para sus datos, restringiendo el intercambio eficiente y seguro de información.
- **Dificultades en la Interoperabilidad:** La variedad en los sistemas y protocolos de comunicación impide la interoperabilidad efectiva entre las distintas plataformas y herramientas utilizadas por las agencias.

Consecuencias de la Heterogeneidad

- **Retrasos en la Respuesta Operativa:** La heterogeneidad en datos y protocolos puede causar retrasos significativos en la respuesta a situaciones críticas, debido a la necesidad de convertir o adaptar datos para su análisis y uso.
- **Costes Operativos Incrementados:** La necesidad de mantener múltiples sistemas y convertir datos entre diferentes formatos incrementa los costes operativos y de mantenimiento.
- **Riesgos de Pérdida de Datos:** La manipulación de datos entre diferentes sistemas aumenta el riesgo de pérdida o corrupción de información vital.
- **Limitaciones en la Analítica de Datos:** La diversidad en los tipos y formatos de datos dificulta el uso de herramientas analíticas avanzadas,

limitando la capacidad de las agencias para realizar análisis profundos y predictivos.

Para mitigar estos problemas, es imperativo desarrollar e implementar estrategias de estandarización de datos y protocolos, así como explorar soluciones integradoras para sistemas de UxVs. Además, la adopción de plataformas y herramientas que puedan manejar eficientemente la diversidad de datos y sistemas contribuirá significativamente a mejorar la cooperación entre las distintas agencias, reduciendo los costes operativos y aumentando la eficiencia y efectividad de las operaciones de seguridad.

2.3.2. Almacenamiento de datos heredado y su ineficiencia

Las agencias de control de fronteras y de investigación criminal enfrentan desafíos significativos debido al uso continuado de sistemas de almacenamiento de datos heredados. Estos sistemas, a menudo creados con tecnologías obsoletas, no están equipados para manejar las demandas de un entorno de seguridad en constante evolución y presentan una serie de problemas que afectan la operatividad y la eficiencia [24].

Problemas Asociados con Sistemas Heredados

- **Capacidad y Rendimiento Limitados:** Muchos sistemas heredados tienen capacidades restringidas para almacenar y procesar la cantidad masiva de datos generados en las operaciones modernas, lo que resulta en un rendimiento lento y una eficiencia reducida.
- **Escalabilidad y Adaptabilidad Inadecuadas:** Estos sistemas a menudo carecen de la flexibilidad necesaria para adaptarse a las cambiantes necesidades tecnológicas y operativas, limitando la capacidad de las agencias para expandir o actualizar sus capacidades de almacenamiento de datos.
- **Mantenimiento y Soporte Técnicos Costosos:** Los sistemas heredados generalmente requieren un mantenimiento especializado y soporte técnico, lo que puede ocasionar costes operativos significativos y la necesidad de mantener personal con habilidades específicas.

Implicaciones Operativas y de Eficiencia

- **Retos en la Gestión de Datos:** La recuperación y manejo de información almacenada en sistemas obsoletos puede ser un proceso lento y

complicado, lo que afecta negativamente la rapidez y la eficacia de las respuestas en situaciones críticas.

- **Barreras para la Integración de Datos Modernos:** Integrar datos provenientes de tecnologías avanzadas con sistemas de almacenamiento antiguos presenta desafíos considerables, lo que puede ocasionar incompatibilidades y errores de procesamiento.
- **Riesgos de Seguridad y Pérdida de Datos:** Los sistemas heredados pueden no cumplir con las normativas actuales de seguridad de datos, aumentando el riesgo de brechas de seguridad y pérdida de datos críticos.

Costes y Recursos Humanos

- **Altos Costes Operativos y de Mantenimiento:** La dependencia de sistemas heredados puede resultar en gastos operativos elevados, incluyendo costes de mantenimiento, actualizaciones y soporte técnico especializado.
- **Dependencia de Personal con Habilidades Específicas:** La operación y el mantenimiento de estos sistemas a menudo requieren personal con conocimientos técnicos especializados, lo que puede ser un reto en términos de capacitación y retención de empleados.

2.3.3. Modelos de intercambio de datos inconsistentes

La cooperación entre agencias de investigación criminal y control fronterizo a menudo se ve obstaculizada por modelos de intercambio de datos inconsistentes y descoordinados [25]. Este problema se presenta en varias facetas, impactando negativamente tanto en las operaciones cotidianas como en las situaciones de emergencia.

Diversidad en Modelos y Protocolos

- **Multiplicidad de Sistemas y Formatos:** Las agencias dependen de una variedad de sistemas para el manejo de datos, cada uno con su propio formato y estructura. Esto incluye desde bases de datos centralizadas hasta sistemas descentralizados y basados en la nube, lo que resulta en un mosaico complejo de formatos de datos y sistemas incompatibles.
- **Protocolos de Comunicación Fragmentados:** La existencia de múltiples protocolos de comunicación entre agencias y departamentos crea barreras significativas para un intercambio de datos fluido y sin fricciones,

especialmente en operaciones que involucran múltiples jurisdicciones o países.

Desafíos en la Integración y Sincronización

- **Falta de Sincronización de Datos:** La ausencia de un sistema unificado de intercambio de datos conduce a problemas de sincronización, donde la información no está actualizada o es inconsistente entre diferentes agencias.

- **Dificultades en la Agregación de Datos:** La recopilación y agregación de datos de múltiples fuentes se convierte en un proceso tedioso y propenso a errores debido a la falta de compatibilidad entre los sistemas.

Consecuencias en la Eficiencia y Seguridad Operativa

- **Retrasos en la Respuesta a Emergencias:** La ineficiencia en el intercambio de datos puede llevar a retrasos críticos en la respuesta a situaciones de emergencia, lo que afecta la eficacia de las operaciones conjuntas y la seguridad pública.

- **Vulnerabilidades de Seguridad:** Las diferencias en los protocolos de seguridad de datos y la transferencia entre sistemas incompatibles pueden exponer datos sensibles a riesgos de seguridad, incluyendo brechas y accesos no autorizados.

- **Duplicación de Esfuerzos:** La necesidad de adaptar o convertir datos entre diferentes sistemas conduce a una duplicación de esfuerzos y una asignación ineficiente de recursos humanos y tecnológicos.

Impacto en la Colaboración y Toma de Decisiones

- **Barreras en la Colaboración Transfronteriza:** La falta de modelos de intercambio de datos coherentes y estandarizados limita la capacidad de las agencias para colaborar eficazmente en operaciones transfronterizas.

- **Desafíos en la Toma de Decisiones Basada en Datos:** La inconsistencia en los datos compartidos y la falta de una visión integral y actualizada obstaculizan la toma de decisiones informada y basada en evidencia.

Estos desafíos subrayan la necesidad crítica de abordar las inconsistencias en los modelos de intercambio de datos para mejorar la colaboración, la eficiencia operativa y la seguridad en las operaciones de investigación criminal y control fronterizo.

2.3.4. Tecnología y recursos limitados

La efectividad de las agencias de investigación criminal y control fronterizo se ve comprometida frecuentemente por limitaciones en tecnología y recursos. Estos desafíos se manifiestan en diversos aspectos, limitando la capacidad operativa y la eficiencia en la respuesta a amenazas y delitos [26].

Limitaciones Tecnológicas

- **Infraestructura Tecnológica Obsoleta:** Muchas agencias operan con tecnologías anticuadas que no pueden integrarse eficientemente con sistemas modernos, lo que resulta en una disminución de la capacidad de respuesta y análisis.
- **Falta de Compatibilidad con Nuevas Tecnologías:** Las limitaciones en la infraestructura tecnológica existente a menudo impiden la adopción de nuevas tecnologías y herramientas avanzadas, lo que restringe la capacidad de las agencias para mejorar sus operaciones y adaptarse a nuevas amenazas y desafíos.

Restricciones de Recursos

- **Presupuestos Limitados:** Las agencias a menudo enfrentan restricciones presupuestarias, lo que limita su capacidad para actualizar tecnologías, capacitar personal y adquirir nuevos recursos.
- **Escasez de Personal Capacitado:** La falta de personal cualificado en áreas como análisis de datos, ciberseguridad y operaciones de inteligencia afecta la eficiencia y la efectividad de las operaciones.

Desafíos en Mantenimiento y Actualización

- **Costes Elevados de Mantenimiento:** El mantenimiento de sistemas antiguos o incompatibles a menudo requiere una inversión significativa, lo que puede desviar recursos de otras áreas críticas.
- **Dificultades en la Actualización de Sistemas:** La actualización de sistemas heredados para cumplir con los estándares modernos es una

tarea compleja y costosa, que puede verse obstaculizada por limitaciones presupuestarias y técnicas.

Impacto en la Capacidad Operativa

- **Respuesta Lenta a Amenazas Emergentes:** La incapacidad para implementar tecnologías avanzadas y adaptar rápidamente las estrategias operativas limita la capacidad de las agencias para responder a nuevas amenazas y desafíos de seguridad.
- **Dependencia de Procesos Manuales:** La falta de herramientas tecnológicas adecuadas a menudo lleva a una mayor dependencia de procesos manuales, lo que aumenta el riesgo de errores y reduce la eficiencia operativa.

Consecuencias a Largo Plazo

- **Desventaja Competitiva:** Las agencias con recursos limitados pueden encontrarse en desventaja competitiva frente a delincuentes y amenazas que utilizan tecnologías avanzadas y tácticas sofisticadas.
- **Desafíos en la Cooperación Interagencial:** La falta de recursos y tecnología adecuados también puede afectar la capacidad de las agencias para colaborar y compartir información de manera efectiva con otras organizaciones nacionales e internacionales.

En resumen, las limitaciones en tecnología y recursos presentan un obstáculo significativo para las agencias de investigación criminal y control fronterizo, afectando su capacidad para mantenerse al día con las demandas y desafíos operativos del entorno de seguridad actual.

2.4. Soluciones en la adquisición e intercambio de datos

2.4.1. Adaptadores para mejorar la interoperabilidad

Para enfrentar los desafíos de interoperabilidad entre las agencias de investigación criminal y control fronterizo, es crucial la implementación de adaptadores. Estos adaptadores sirven como puentes entre plataformas heterogéneas y sistemas dispares, facilitando un flujo de datos coherente y eficiente [27]. Una de las aplicaciones más críticas de estos adaptadores es en la integración de UxVs, que requieren compatibilidad con protocolos estándar como *JANUS*

[28], *Standardization Agreement* (STANAG) 4586 [29] y STANAG 4748 [30] para una operatividad óptima.

Funcionalidades de los Adaptadores

- **Conversión de Formatos de Datos:** Los adaptadores transforman datos de un formato a otro, permitiendo la integración de sistemas que utilizan diferentes estándares y estructuras de datos, incluyendo los provenientes de UxVs.

- **Normalización de Protocolos de Comunicación:** Estos sistemas armonizan los protocolos de comunicación, incluyendo protocolos especializados como *JANUS*, STANAG 4586 y STANAG 4748, para asegurar una transmisión de datos coherente entre diversas plataformas.

Beneficios de los Adaptadores

- **Mejora en la Colaboración Interagencial:** La compatibilidad entre sistemas, incluyendo la integración de UxVs, facilita una colaboración efectiva entre agencias, mejorando la capacidad de respuesta conjunta.

- **Reducción de Tiempos de Procesamiento:** La automatización en la conversión y normalización de datos acelera el procesamiento y análisis, aumentando la eficiencia operativa.

Implementación de Adaptadores

- **Diseño Personalizado:** Los adaptadores deben ser diseñados considerando las especificaciones únicas de cada sistema y vehículo, asegurando una integración efectiva con protocolos como *JANUS*, STANAG 4586 y STANAG 4748.

- **Actualizaciones y Mantenimiento:** Mantener actualizados los adaptadores es crucial para adaptarse a cambios en sistemas y estándares, incluyendo actualizaciones en protocolos de UxVs.

Desafíos en la Adopción de Adaptadores

- **Necesidad de Expertise Técnico:** La creación de adaptadores eficaces, especialmente para UxVs y protocolos especializados, requiere conocimientos técnicos avanzados.

- **Coordinación Interagencial:** Una implementación exitosa requiere una coordinación efectiva entre las agencias para asegurar que los adaptadores satisfagan las necesidades de todos los sistemas y plataformas involucrados.

Por lo tanto, la implementación de adaptadores, incluyendo aquellos para UxVs bajo protocolos como *JANUS*, STANAG 4586 y STANAG 4748, es esencial para mejorar la interoperabilidad y cooperación efectiva entre las agencias de investigación criminal y control fronterizo.

2.4.2. Modelos de Datos Estándar

El desarrollo y la adopción de modelos de datos estándar son cruciales para mejorar la interoperabilidad y la eficiencia en la cooperación interagencial, especialmente en el ámbito del control de fronteras y la investigación criminal [31]. Estos modelos estandarizados facilitan la organización, el procesamiento y el análisis uniforme de los datos, lo que es esencial para una colaboración efectiva entre diferentes organizaciones y plataformas.

Importancia de los Modelos de Datos Estándar

- **Uniformidad en el Almacenamiento de Datos:** Los modelos estándar proporcionan un marco común para almacenar datos de manera coherente, facilitando así su recuperación y análisis.

- **Eficacia en el Intercambio de Información:** Utilizar un formato común elimina la necesidad de conversiones complejas entre diferentes sistemas y agencias.

- **Calidad y Precisión de los Datos:** Estos modelos contribuyen a mantener la integridad y precisión de los datos, estableciendo estándares claros para su ingreso y mantenimiento.

Estándares Específicos en Modelos de Datos

- **EXDL (Extensible Data Language) [32]:** Un formato basado en *eXtensible Markup Language* (XML) diseñado para el intercambio eficiente de información entre diferentes entidades.

- **NIEM (National Information Exchange Model) [33]:** Un estándar que proporciona una metodología común para el intercambio de datos entre agencias, mejorando la interoperabilidad y la seguridad.

- **XML [34] y JSON [35]:** Lenguajes de marcado ampliamente utilizados para la estructuración de datos, facilitando su manipulación y transferencia entre diferentes sistemas.

Implementación y Desafíos

- **Desarrollo y Acuerdos:** La implementación de estos estándares requiere la colaboración y el consenso entre diversas agencias para desarrollar especificaciones aplicables en distintos contextos operativos.
- **Capacitación y Adopción:** Es fundamental capacitar al personal en el uso de estos modelos para asegurar su correcta aplicación y eficacia.
- **Integración y Actualización:** Estos modelos deben ser capaces de integrarse con los sistemas existentes, y ser actualizados continuamente para adaptarse a los avances tecnológicos y las necesidades cambiantes.

Superando la Resistencia al Cambio

- **Flexibilidad y Adaptabilidad:** Los modelos de datos deben ser lo suficientemente flexibles para satisfacer las necesidades específicas de cada agencia, manteniendo un estándar común.
- **Mantenimiento y Actualización Constantes:** Es crucial mantener los modelos de datos actualizados y relevantes frente a los cambios tecnológicos y las demandas operativas.

La adopción de modelos de datos estándar, incluyendo *Extensible data language* (EXDL), *National information exchange model* (NIEM), XML y *JavaScript Object Notation* (JSON), es esencial para una gestión eficiente de la información en el contexto de la cooperación interagencial, maximizando la eficacia en la lucha contra el crimen y en el control de fronteras.

2.4.3. Intercambio de Datos Optimizado

El intercambio de datos optimizado es esencial en el contexto de la cooperación entre agencias de control de fronteras e investigación criminal. La implementación de *Application programming interface* (API)s, API gateways, servicios web *Representation state transfer* (REST) [36] o *Simple object access protocol* (SOAP) [37], y middlewares especializados, se ha vuelto fundamental para facilitar un intercambio de datos eficaz y en tiempo real [38].

APIs y API Gateways: Puntos de Acceso Estandarizados

- **Interconexión Fluida entre Sistemas:** Las APIs proporcionan una interfaz estandarizada para permitir la interacción entre diferentes sistemas de software, facilitando el acceso, la gestión y la actualización de los datos de manera eficiente.
- **Control y Seguridad:** Los API gateways funcionan como intermediarios, ofreciendo un punto de control para el acceso a los datos. Implementan medidas de seguridad como la autenticación y la autorización, asegurando que solo los usuarios autorizados puedan acceder a la información relevante.
- **Facilitación de Integración:** La utilización de servicios web REST y SOAP proporciona un medio versátil para el intercambio de datos. Estos servicios permiten la comunicación entre distintas plataformas y lenguajes de programación, asegurando una interoperabilidad efectiva.

Middlewares para Comunicación en Tiempo Real

- **Mecanismos de Publicación-Suscripción:** Los middlewares especializados en la gestión de mensajes posibilitan la comunicación en tiempo real. Estos sistemas permiten a los usuarios suscribirse a temas específicos y recibir actualizaciones de datos de forma continua y automática.
- **Optimización de la Comunicación:** Estos sistemas mejoran la velocidad y eficiencia del intercambio de información, lo que resulta en una capacidad de respuesta más rápida y precisa ante situaciones críticas.
- **Adaptabilidad y Escalabilidad:** Los middlewares ofrecen una solución altamente adaptable y escalable, capaz de manejar diferentes volúmenes de datos y requisitos operativos. Esto es crucial para las agencias que enfrentan desafíos dinámicos y cambiantes en sus operaciones.
- **Consistencia de Datos:** Mediante la implementación de estos sistemas, se asegura la consistencia y actualización de los datos en tiempo real, lo cual es vital para mantener una información precisa y actualizada.

Desarrollos Avanzados en Intercambio de Datos

- **Uso de API Gateways Avanzados:** Los API gateways modernos no solo gestionan el tráfico y la seguridad, sino que también proporcionan capacidades analíticas, permitiendo monitorizar y optimizar el flujo de datos.

- **Servicios Web REST y SOAP:** La elección entre REST y SOAP puede depender de las necesidades específicas de la agencia. Mientras que REST es ideal para casos de uso con requerimientos de menor complejidad y mayor velocidad, SOAP es preferido para operaciones con necesidades de seguridad y transacciones más complejas.

Beneficios del Intercambio de Datos Optimizado

- **Mejora en la Toma de Decisiones:** Un flujo constante y actualizado de datos provee a las agencias la información necesaria para tomar decisiones informadas en tiempo real.
- **Reducción de Costes y Tiempos:** La eficiencia en el intercambio de datos reduce los tiempos de respuesta y minimiza los costes asociados con el manejo de información.
- **Facilitación de la Colaboración:** Un sistema de intercambio de datos bien estructurado y eficiente fomenta una cooperación más efectiva entre diferentes agencias y jurisdicciones, mejorando la capacidad general para enfrentar desafíos de seguridad.
- **Incremento de la Capacidad Analítica:** La estandarización y optimización del intercambio de datos permite el uso de herramientas analíticas más avanzadas, abriendo la puerta a análisis predictivos y profundos.

2.5. El Big Data, soluciones y mejoras en almacenamiento y procesado de datos

2.5.1. Silos de Datos y DataLakes: Aplicaciones Específicas y Soluciones Integradas

La utilización de Silos de Datos y DataLakes [39] constituye una solución integral a los retos del almacenamiento y procesamiento del Big Data en el ámbito de la seguridad y la inteligencia. Estas estructuras, con usos y capacidades distintas, se implementan para optimizar la gestión y análisis de datos masivos [40].

Silos de Datos: Especialización y Eficacia

- **Organización por Tipo y Origen:** Los Silos de Datos se organizan y optimizan para tipos específicos de datos, como registros de vigilancia,

inteligencia, o información geográfica, facilitando una gestión y acceso especializados.

- **Optimización de Rendimiento:** Cada silo se optimiza para operaciones particulares, adecuadas para almacenamiento a largo plazo o para consultas y análisis rápidos, según la naturaleza del dato.
- **Selección de Motores de Bases de Datos:** Se utilizan motores de bases de datos adecuados para cada tipo de datos. Por ejemplo, bases de datos orientadas a columnas para análisis de grandes volúmenes y bases de datos relacionales para transacciones y consultas complejas.

DataLakes: Flexibilidad y Centralización

- **Almacén Unificado:** A diferencia de los Silos de Datos, los DataLakes sirven como un repositorio centralizado para almacenar todo tipo de datos, tanto estructurados como no estructurados, permitiendo un análisis más integral y holístico.
- **Adaptabilidad:** Los DataLakes manejan diversos formatos de datos, haciéndolos ideales para almacenar desde texto hasta multimedia, adaptándose a las necesidades cambiantes de las agencias.
- **Escalabilidad:** Diseñados para ser escalables, se adaptan fácilmente a nuevos tipos de datos y tecnologías emergentes, facilitando la integración y el manejo de grandes volúmenes de información.

Ejemplos de Motores de Bases de Datos y Sistemas Integrados

- **Apache Hadoop y HDFS:** Hadoop, con su *Hadoop Distributed File System* (HDFS) [41], es un componente clave para el procesamiento eficiente de grandes conjuntos de datos en DataLakes, facilitando operaciones complejas de análisis a gran escala.
- **MinIO [42]:** Este sistema de almacenamiento de objetos de alto rendimiento es ideal para entornos de DataLakes, ofreciendo escalabilidad y compatibilidad con API de S3.
- **MongoDB [43] y Cassandra [44]:** Bases de datos *Not-Only SQL* (NoSQL) [45] que proporcionan flexibilidad y alto rendimiento para datos no estructurados o semiestructurados.
- **SQL Server [46] y Oracle [47]:** Estos sistemas de gestión de bases de datos son adecuados para datos altamente estructurados, ofreciendo seguridad y alta integridad en las operaciones de datos.

La implementación combinada de Silos de Datos y DataLakes, apoyada por una selección estratégica de motores de bases de datos y sistemas de almacenamiento, establece una infraestructura de datos robusta y adaptable. Esto facilita a las agencias de seguridad la gestión y consulta de datos de manera optimizada, mejorando significativamente el manejo y análisis de Big Data en un entorno de seguridad complejo.

2.5.2. Análisis en Tiempo Real de Grandes Volúmenes

El análisis en tiempo real de grandes volúmenes de datos representa una transformación fundamental en las operaciones de seguridad y vigilancia, permitiendo a las agencias responder rápidamente a situaciones complejas y dinámicas [48]. Esta capacidad es crucial para analizar y procesar de manera instantánea grandes cantidades de datos provenientes de diversas fuentes.

Procesamiento de Datos en Tiempo Real

- **Streaming de Datos:** La adopción de tecnologías de streaming de datos permite el procesamiento continuo y en tiempo real de flujos de información, como datos de sensores, comunicaciones en redes sociales, o transmisiones de CCTV.
- **Análisis Instantáneo:** Las herramientas de análisis procesan estos datos al instante, permitiendo la detección y el reconocimiento inmediato de patrones, anomalías y tendencias críticas.
- **Respuesta Automatizada:** La integración de sistemas de respuesta automatizada basados en el análisis de datos en tiempo real posibilita acciones rápidas, como el despliegue de alertas automáticas o la activación de medidas de seguridad.

Tecnologías y Herramientas Clave

- **Apache Kafka [49] y Apache Storm [50]:** Estas herramientas son esenciales para el manejo de grandes volúmenes de datos en tiempo real, ofreciendo alta disponibilidad y rendimiento.
- **Elasticsearch [51] y Kibana [52]:** Esta combinación permite el análisis y la visualización de datos en tiempo real, brindando una interfaz intuitiva para la exploración y comprensión de los datos.
- **RabbitMQ [53] y Mosquitto [54]:** Estos sistemas de mensajería y colas de mensajes facilitan la gestión eficiente del flujo de datos en tiempo real, apoyando la escalabilidad y fiabilidad en entornos distribuidos.

- **Plataformas de Inteligencia Artificial y Machine Learning:** La integración de estas tecnologías avanzadas posibilita el análisis predictivo y la identificación de patrones complejos en tiempo real.

Aplicaciones en Seguridad y Vigilancia

- **Monitorización de Fronteras y Espacios Públicos:** La capacidad de analizar datos en tiempo real es vital para la vigilancia efectiva, permitiendo la detección y respuesta inmediata a actividades sospechosas o inusuales.
- **Gestión de Emergencias y Respuesta a Crisis:** Esta tecnología facilita una gestión más eficaz de situaciones de emergencia, mejorando la coordinación y respuesta de los equipos de seguridad y emergencia.
- **Prevención de Delitos y Terrorismo:** El análisis en tiempo real ayuda en la detección proactiva y prevención de actividades delictivas y terroristas, fortaleciendo así la seguridad pública.

El análisis en tiempo real de grandes volúmenes de datos es un componente esencial para las operaciones modernas de seguridad y vigilancia, proporcionando a las agencias la capacidad de reaccionar rápidamente y tomar decisiones informadas en entornos complejos y cambiantes. La integración de estas tecnologías mejora significativamente la eficiencia operativa y la capacidad de respuesta ante amenazas y situaciones de riesgo.

2.5.3. Optimización en Gestión de Recursos

La gestión eficiente de recursos en el contexto de Big Data es un desafío crítico para las agencias de seguridad e inteligencia. La optimización no se limita solo al almacenamiento y procesamiento de datos, sino que también abarca la administración inteligente de energía, costes operativos y la maximización del rendimiento de los sistemas [55].

Eficiencia en el Uso de Recursos

- **Almacenamiento Distribuido:** Sistemas como HDFS y soluciones de almacenamiento de objetos como MinIO permiten una administración eficiente de datos en grandes volúmenes, distribuyendo la carga de almacenamiento a través de varios nodos y optimizando el espacio disponible.
- **Procesamiento Distribuido:** Apache Spark [56] y Hadoop MapReduce [57] facilitan el procesamiento de datos distribuido, donde la carga de

trabajo se reparte entre múltiples servidores. Esto no solo aumenta la eficiencia en el procesamiento, sino que también reduce significativamente los tiempos de respuesta.

Gestión de Costes Operativos

- **Escalabilidad Elástica:** Implementando soluciones en la nube, las agencias pueden ajustar los recursos de manera elástica, escalando hacia arriba o hacia abajo según las demandas operativas, lo que se traduce en un manejo más eficiente de los costes.
- **Automatización de Procesos:** La automatización de tareas rutinarias a través de herramientas de orquestación y scripts reduce la intervención manual y los errores humanos, lo que se traduce en una reducción de costes y un aumento de la eficiencia operativa.

Optimización del Consumo de Energía

- **Centros de Datos Eficientes:** La implementación de centros de datos con sistemas avanzados de refrigeración y gestión de energía reduce el consumo energético y los costes asociados.
- **Virtualización de Servidores:** La virtualización permite operar múltiples servidores virtuales en un solo hardware físico, disminuyendo el consumo de energía y optimizando el uso de recursos.

Maximización del Rendimiento

- **Balanceo de Carga:** Los balanceadores de carga garantizan que las solicitudes de datos se distribuyan equitativamente entre los servidores, evitando sobrecargas y asegurando un rendimiento óptimo.
- **Caché e Indexación Eficientes:** Implementar sistemas de caché y optimizar la indexación de bases de datos, mejora significativamente la velocidad de acceso a los datos y la eficiencia en las consultas.

Uso de Tecnologías Emergentes

- **Contenedores y Orquestación:** El uso de contenedores y herramientas de orquestación como Kubernetes [58] facilita la gestión de aplicaciones distribuidas, mejorando la agilidad y eficiencia en la implementación y operación de servicios.

- **Computación en la Nube Híbrida:** La adopción de la nube híbrida permite una combinación óptima de recursos en la nube y en las instalaciones, proporcionando flexibilidad y optimizando el uso de recursos locales y remotos.

La optimización en la gestión de recursos abarca una combinación de estrategias y tecnologías que maximizan la eficiencia, reducen costes y minimizan el consumo de energía, asegurando al mismo tiempo el máximo rendimiento en el procesamiento y análisis de Big Data. Estas estrategias son esenciales para que las agencias de seguridad manejen de manera efectiva los retos que presenta la gestión de grandes volúmenes de datos en la era moderna.

2.6. Soluciones para visualización e interacción con datos masivos

2.6.1. Herramientas de Visualización Orientadas a Dashboards

Las herramientas de visualización basadas en dashboards desempeñan un papel esencial en la gestión efectiva de datos masivos, especialmente en entornos de seguridad y vigilancia [59]. Herramientas como *Kibana* y *Grafana* [60], junto con *frameworks* de *JavaScript* [61] como *React* [62], *Angular* [63] y *Vue.js* [64], ofrecen soluciones robustas para crear dashboards interactivos y personalizables. Estas herramientas y tecnologías permiten a los usuarios no solo visualizar grandes volúmenes de datos de forma eficiente, sino también personalizar la experiencia de usuario según las necesidades específicas de cada caso de uso [65].

Plataformas Avanzadas de Dashboard

- **Kibana:** Integrada con *Elasticsearch*, *Kibana* es una herramienta de visualización poderosa, proporcionando una interfaz de usuario intuitiva para la exploración y visualización de datos en tiempo real. Su capacidad para manejar datos de series temporales la hace ideal para aplicaciones de seguridad y vigilancia.

- **Grafana:** Conocida por su flexibilidad y rica paleta de opciones de visualización, *Grafana* soporta una amplia gama de fuentes de datos y es altamente personalizable, lo que la hace adecuada para una variedad de contextos operativos.

- **Capacidades de Personalización:** Ambas plataformas ofrecen extensas opciones de personalización, desde la creación de dashboards específicos hasta la adaptación de visualizaciones para diferentes roles y escenarios operativos.

Frameworks de Desarrollo de Front-End

- **React, Angular y Vue.js:** Estos frameworks de JavaScript son fundamentales para el desarrollo de aplicaciones web modernas y responsive. Facilitan la creación de interfaces de usuario ricas y dinámicas, optimizadas para la interacción con dashboards complejos.

- **Desarrollo Multi-Plataforma:** La adaptabilidad de estos frameworks permite el desarrollo de aplicaciones que funcionan eficientemente en una variedad de dispositivos, desde computadoras de escritorio hasta dispositivos móviles, asegurando una experiencia de usuario coherente y accesible.

- **Customización y Adaptabilidad:** La arquitectura modular y la flexibilidad de estos frameworks permiten customizaciones rápidas y eficientes, adaptándose a las necesidades específicas de visualización y análisis de datos en entornos de seguridad.

Mejorando la Experiencia de Usuario y la Accesibilidad

- **Diseño Responsivo:** Estos frameworks facilitan el desarrollo de aplicaciones que se adaptan perfectamente a diferentes tamaños de pantalla, asegurando una experiencia de usuario fluida y accesible en todos los dispositivos.

- **Interactividad y Comprensión de Datos:** Las herramientas de visualización avanzadas combinadas con una interfaz de usuario bien diseñada mejoran significativamente la interacción del usuario con los datos, lo que resulta en una comprensión más profunda y una toma de decisiones más informada.

Visualizaciones Avanzadas y Análisis de Datos

- **Visualización de Datos Complejos:** La capacidad de estas herramientas para crear visualizaciones complejas, como mapas de calor, gráficos de línea y visualizaciones geoespaciales, es crucial para analizar tendencias y patrones en grandes conjuntos de datos.

- **Análisis en Tiempo Real:** La integración con sistemas de procesamiento de datos en tiempo real permite a los usuarios obtener insights operativos instantáneos, lo que es vital en situaciones de seguridad crítica.

La combinación de herramientas de visualización avanzadas y frameworks de desarrollo de front-end proporciona una solución integral para la interacción efectiva con datos masivos en el ámbito de la seguridad y vigilancia. Estas tecnologías no solo mejoran la experiencia del usuario, sino que también facilitan la adaptación y personalización de las visualizaciones de datos para satisfacer las demandas específicas de cada caso de uso.

2.6.2. Hardware Dedicado a xR

El avance en tecnologías de *Extended reality* (xR), que abarca *Virtual reality* (VR), *Mixed reality* (MR) y *Augmented Reality* (AR), ha abierto nuevas posibilidades para la visualización e interacción con datos masivos. Estas tecnologías son fundamentales en ámbitos como la seguridad, la vigilancia y la inteligencia, donde la capacidad de sumergirse en entornos virtuales o interactuar con elementos digitales superpuestos en el mundo real puede mejorar significativamente la eficiencia y la toma de decisiones [66].

Realidad Virtual (VR)

Los dispositivos de VR, como *Oculus Rift* [67] y *HTC Vive* [68], ofrecen entornos completamente inmersivos, ideales para la capacitación, la simulación de escenarios y el análisis detallado de datos en un entorno controlado. Estos dispositivos son esenciales para entrenamientos de seguridad, permitiendo a los usuarios experimentar situaciones de alto riesgo de manera segura.

Realidad Mixta (MR)

Los dispositivos de MR, como *Apple Vision Pro* [69], combinan elementos del mundo real con información y objetos digitales, permitiendo una interacción intuitiva con datos y entornos virtuales. Esta tecnología es especialmente valiosa en operaciones de campo, donde la información crucial puede superponerse en la vista en tiempo real de un agente.

Realidad Aumentada (AR)

La tecnología AR, representada por dispositivos como *Microsoft HoloLens* [70], ofrece una superposición de información digital sobre el entorno real, permitiendo a los usuarios acceder a datos relevantes en tiempo real. Estos dispo-

sitivos son cruciales en aplicaciones de vigilancia y reconocimiento, ofreciendo una capa adicional de información sin obstruir la percepción del entorno real.

Tabla de Especificaciones y Casos de Uso

Dispositivo	Tipo de xR	Especificaciones	Caso de Uso
Oculus Rift	VR	Pantalla OLED, Resolución 2160x1200	Entrenamiento, Simulación
HTC Vive	VR	Pantalla AMOLED, Resolución 2160x1200	Entrenamiento, Inmersión Total
Microsoft HoloLens	AR	Pantalla Holográfica, Resolución 2k	Interacción en Campo, Datos Superpuestos
Apple Vision Pro	MR	Tecnología MR, Integración con iOS	Vigilancia, Reconocimiento

Tabla 2.1: Comparación de Dispositivos xR

Cada uno de estos dispositivos ofrece una experiencia única y adecuada para diferentes aplicaciones dentro del ámbito de la seguridad y la inteligencia. Desde simulaciones inmersivas hasta visualizaciones superpuestas en tiempo real, el hardware xR juega un papel vital en la transformación de cómo interactuamos y comprendemos los datos en un mundo cada vez más digitalizado y conectado. Su implementación proporciona no solo mejoras en la eficiencia operativa y la toma de decisiones, sino también una capacidad mejorada para responder de manera efectiva en situaciones críticas y de alta presión [71].

2.6.3. Software y Aplicaciones Inmersivas, Mixtas y Aumentadas

Las tecnologías inmersivas, mixtas y aumentadas xR, abarcando VR, MR y AR, están revolucionando la forma en que interactuamos y visualizamos datos masivos. En el contexto de la seguridad y la inteligencia, estas tecnologías ofrecen soluciones avanzadas para simulación, entrenamiento, y análisis de datos. A continuación, se presentan algunos *frameworks* y herramientas de desarrollo que están a la vanguardia en el ámbito de xR.

Unity

Unity [72] se destaca por su flexibilidad y facilidad de uso en el desarrollo de aplicaciones VR y AR. Su interfaz intuitiva y el extenso conjunto de herramientas permiten a los desarrolladores crear experiencias inmersivas detalladas, que son cruciales en simulaciones de entrenamiento y reconstrucciones de escenarios en entornos de seguridad.

Unreal Engine

Unreal Engine [73] es ideal para proyectos que requieren gráficos de alta fidelidad. Su motor gráfico avanzado y el sistema de scripting Blueprint posibilitan la creación de entornos xR realistas, lo que es esencial para simulaciones detalladas y análisis visuales en el campo de la seguridad.

ARKit y ARCore

ARKit [74] y *ARCore* [75] están especializados en el desarrollo de AR para dispositivos iOS y Android. Estos frameworks ofrecen herramientas avanzadas para el seguimiento y la integración de objetos virtuales en el mundo real, facilitando aplicaciones como la visualización de datos en tiempo real y el mapeo de entornos para operaciones de campo.

Vuforia

Vuforia [76] es ampliamente reconocido por su capacidad para desarrollar experiencias AR robustas en diversas plataformas. Es especialmente útil para aplicaciones que requieren reconocimiento preciso de imágenes y objetos, lo que es vital en tareas como identificación de amenazas o análisis de escenarios en operaciones de seguridad.

Microsoft Mixed Reality Toolkit

Microsoft Mixed Reality Toolkit [77] es crucial para el desarrollo en dispositivos *Microsoft HoloLens* y plataformas MR. Facilita el desarrollo rápido de aplicaciones MR, con un enfoque en interacciones naturales y accesibles, proporcionando a los usuarios una manera más intuitiva de interactuar con datos y simulaciones complejas.

Además de estos *frameworks*, el desarrollo de aplicaciones xR en el contexto de la seguridad y la inteligencia se beneficia del uso de:

React, Angular, y Vue.js

Estos *frameworks JavaScript* modernos son esenciales para el desarrollo de interfaces de usuario web interactivas y multiplataforma. Permiten crear dashboards personalizados y aplicaciones que mejoran la experiencia del usuario, facilitando la visualización y manipulación de datos complejos.

Aplicación en el Contexto del Proyecto

En el proyecto, la integración de estas tecnologías xR abre nuevas dimensiones en el análisis de datos y la toma de decisiones. Por ejemplo:

- **Simulaciones de Entrenamiento con Unity y Unreal Engine:** Creación de entornos virtuales detallados para la formación de personal en escenarios de seguridad, mejorando la preparación y respuesta ante situaciones reales.
- **Aplicaciones AR para Reconocimiento en Campo:** Utilización de *ARKit, ARCore y Vuforia* para desarrollar aplicaciones que proporcionen a los agentes información crucial superpuesta en el entorno real, mejorando la eficiencia en operaciones de terreno.
- **Interfaz Intuitiva con Microsoft Mixed Reality Toolkit:** Desarrollo de aplicaciones MR para dispositivos como *HoloLens*, ofreciendo a los usuarios una interacción natural y avanzada con datos y simulaciones.

La implementación de software y aplicaciones xR en el proyecto representa un avance significativo en la manera en que las agencias de seguridad e inteligencia interactúan con datos y responden a situaciones críticas. Estas tecnologías no solo mejoran la eficiencia operativa y la toma de decisiones, sino que también abren nuevas posibilidades para la capacitación y el análisis avanzado de datos en un mundo cada vez más digitalizado y conectado.

Capítulo 3

Definición de la arquitectura

3.1. Introducción

Esta sección de la tesis doctoral aborda la arquitectura innovadora de dos proyectos distintivos en el ámbito de la tecnología de seguridad y análisis de datos: CAMELOT y PREVISION. Ambos proyectos representan avances significativos en sus respectivos campos, ofreciendo soluciones pioneras a los desafíos de seguridad contemporáneos y la gestión de datos complejos.

El proyecto CAMELOT se centra en el desarrollo de una plataforma distribuida para la interoperabilidad de sistemas autónomos y no tripulados. Esta plataforma está diseñada para integrar eficientemente activos operativos en dominios de aire, tierra y mar, superando las limitaciones de los sistemas no interoperables tradicionales. La arquitectura de CAMELOT incluye módulos clave como la *CAMELOT adaptor layer* (CAL), el *Automatic Asset Tasking and Control* (AATC), y la *Data management and analitycs* (DMA), los cuales trabajan en conjunto para mejorar la gestión y vigilancia fronteriza.

Por otro lado, el proyecto PREVISION adopta un enfoque de análisis de datos para apoyar a las LEAs en su lucha contra el terrorismo y el crimen organizado. PREVISION utiliza técnicas avanzadas de big data y análisis de inteligencia artificial para detectar patrones ocultos y predecir actividades criminales, mejorando la conciencia situacional de los tomadores de decisiones. La arquitectura de PREVISION es capaz de procesar datos heterogéneos de diversas fuentes, integrándolos en grafos de conocimiento dinámicos y autoaprendizaje.

La combinación de estos dos proyectos en esta tesis resalta la importancia de una arquitectura avanzada en la gestión de amenazas y seguridad. Cada uno, con su enfoque y metodología únicos, contribuye significativamente al avance de las tecnologías y métodos utilizados en seguridad y análisis de datos, demostrando la evolución y adaptabilidad necesarias en el mundo de la seguridad tecnológica.

3.2. Concepto general de la arquitectura

El desarrollo de arquitecturas de software ha experimentado una transformación significativa a lo largo de los años, marcada por una evolución desde estructuras monolíticas hacia enfoques más dinámicos y modulares.

De Monolitos a Módulos

En las primeras etapas, la programación monolítica dominaba el escenario del desarrollo de software. Las aplicaciones se construían como bloques únicos e indivisibles, lo que, aunque facilitaba el desarrollo inicial, pronto presentaba desafíos significativos en términos de escalabilidad y mantenimiento, tal y como se observa en la Figura 3.1.

Figura 3.1: Modelo de arquitectura monolítica

La introducción de la arquitectura modular, que descomponía las aplicaciones en módulos o componentes más pequeños, marcó un cambio fundamental. Esta aproximación mejoró la mantenibilidad y la flexibilidad del software, per-

mitiendo que diferentes módulos se desarrollaran y actualizaran de manera independiente.

Arquitectura Orientada a Servicios (SOA)

El siguiente gran avance fue la *Service-oriented architecture* (SOA). Se centró en descomponer las funciones de las aplicaciones en servicios individuales, reutilizables y acoplados de manera flexible [78]. Esta arquitectura promovió la eficiencia a través del reúso y la integración más sencilla de diversos componentes de software, a menudo distribuidos geográficamente.

Arquitectura Basada en Microservicios

La arquitectura de microservicios representa una evolución natural de SOA, llevando la modularidad y la flexibilidad a un nivel aún más avanzado. Las características principales de los microservicios es que son pequeñas unidades de software que funcionan de manera independiente, pero que pueden comunicarse entre sí a través de interfaces bien definidas, como APIs, para formar aplicaciones complejas [79]. Cada microservicio se centra en una función específica y opera en un entorno contenerizado, como Docker [80], que proporciona aislamiento y facilita la implementación en diversos entornos. Como se puede observar en la Figura 3.2.

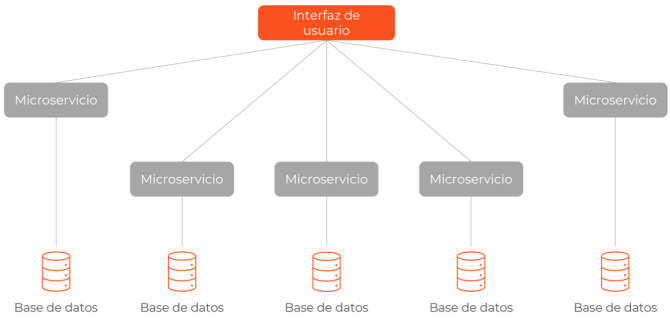

Figura 3.2: Modelo de arquitectura orientada a microservicios

Las características principales de una arquitectura orientada a microservicios son:

- **Adaptabilidad:** Los microservicios son extremadamente adaptativos, permitiendo el desarrollo, despliegue, actualización y escalado de manera

individual sin afectar al resto del ecosistema de la aplicación. Esto facilita la implementación de prácticas de *Continuous integration and continuous deployment* (CI/CD) [81], permitiendo una rápida adaptación a los cambios del mercado o las demandas de los clientes.

- **Interoperabilidad:** Utilizando APIs y protocolos estándar, como *Hypertext Transfer Protocol* (HTTP)/HTTPS y REST, los microservicios pueden comunicarse e intercambiar datos eficientemente, facilitando la creación de ecosistemas de software integrados.
- **Escalabilidad Flexible:** Si un microservicio alcanza su capacidad máxima, se pueden desplegar rápidamente nuevas instancias de ese servicio para aliviar la presión, permitiendo soportar tamaños de instancia más grandes y ofreciendo una arquitectura multitenant y sin estado.
- **Despliegue Continuo:** Con microservicios, se pueden tener ciclos de lanzamiento frecuentes y más rápidos, permitiendo actualizaciones varias veces al día en lugar de una vez a la semana.
- **Alta Mantenibilidad y Pruebas:** Facilita la experimentación con nuevas características y el rápido retroceso si algo no funciona, mejorando la actualización de código y acelerando el tiempo de comercialización de nuevas funcionalidades.
- **Despliegue Independiente:** Al ser unidades individuales, los microservicios permiten un despliegue rápido y fácil de características individuales.
- **Flexibilidad Tecnológica:** Permiten a los equipos la libertad de seleccionar las herramientas que deseen utilizar.
- **Alta Fiabilidad:** Posibilitan el despliegue de cambios en un servicio específico sin el riesgo de afectar toda la aplicación.
- **Equipos Más Satisfechos:** Los equipos que trabajan con microservicios tienden a estar más contentos debido a su mayor autonomía y capacidad de construir y desplegar por sí mismos sin largas esperas por aprobaciones.

Así pues, se puede determinar que la arquitectura de microservicios, con su énfasis en la modularidad, independencia y comunicación eficiente, proporciona una base sólida para el desarrollo ágil y adaptable de aplicaciones modernas. Su capacidad para integrarse en entornos tecnológicos complejos y en constante evolución los convierte en una elección preferida para empresas que buscan soluciones robustas y escalables.

Ante esta realidad, se ha optado por adoptar una arquitectura orientada a microservicios como solución propuesta, dada su capacidad para abordar y adaptarse eficientemente a estas características dinámicas. Esta arquitectura se destaca por su manejo eficaz de la ingesta de datos masiva de múltiples fuentes, empleando adaptadores de protocolo especializados que aseguran la coherencia y la integridad del modelo de datos genérico. Además, el uso de contenedores Docker en el desarrollo de microservicios proporciona una versatilidad sin precedentes en términos de despliegue, ya sea en entornos de nube o locales.

Beneficios Clave de la Arquitectura de Microservicios

La adopción de microservicios trae consigo una serie de beneficios fundamentales [82], que son esenciales para el éxito de proyectos que requieren alta adaptabilidad y escalabilidad. Entre estos, destacan:

1. **Flexibilidad Operativa:** Los microservicios ofrecen una gran flexibilidad en el manejo y procesamiento de datos, adaptándose fácilmente a los cambios y a la evolución de las necesidades del proyecto.

2. **Agilidad en el Desarrollo y Mantenimiento:** Esta arquitectura permite que los equipos de desarrollo trabajen de manera más ágil y eficiente. La independencia de cada microservicio facilita un ciclo de vida de desarrollo más rápido y un mantenimiento menos complejo.

3. **Robustez en la Integración de Sistemas:** Los microservicios están diseñados para integrarse sin problemas con una amplia gama de sistemas y tecnologías, lo que es vital para proyectos que involucran diversas fuentes de datos y sistemas externos.

4. **Optimización del Despliegue:** Gracias a la contenedorización con Docker, los microservicios se pueden desplegar de manera consistente y eficiente en una variedad de entornos, maximizando la disponibilidad y minimizando los tiempos de inactividad.

5. **Resiliencia y Escalabilidad:** La arquitectura de microservicios fortalece la resiliencia del sistema al permitir que los fallos en un servicio se manejen de manera aislada, evitando así afectaciones mayores. Además, ofrece una escalabilidad excepcional, ajustando los recursos de manera eficiente según la demanda.

La elección de una arquitectura basada en microservicios para proyectos colaborativos y evolutivos refleja un enfoque estratégico y visionario.

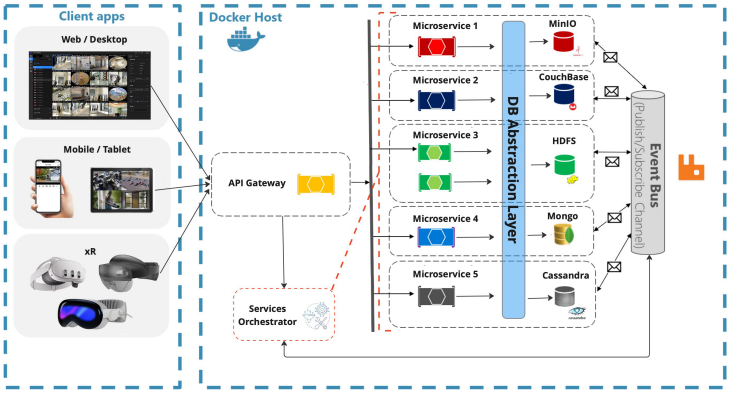

Figura 3.3: Modelo de arquitectura propuesta

La arquitectura de la Figura 3.3 no solo cumple con los requisitos de adaptabilidad y escalabilidad de los proyectos modernos, sino que también proporciona una base sólida para la gestión e ingestión eficiente de datos por medio del bus de eventos, la integración de sistemas y un despliegue flexible y robusto. La implementación de microservicios es, por lo tanto, una solución integral para enfrentar los desafíos y aprovechar las oportunidades en el dinámico panorama tecnológico actual.

3.3. Adquisición de datos

3.3.1. Adaptadores

En el contexto de una plataforma que maneja y procesa datos de múltiples fuentes, surge la necesidad crítica de implementar adaptadores. Estos adaptadores juegan un papel vital en la unificación de los datos en un modelo de datos coherente y estandarizado. Su propósito principal es facilitar la integración de dispositivos externos y activos heredados que no pueden interoperar directamente con la plataforma, asegurando así un flujo continuo y eficiente de información.

Propósito de los Adaptadores

La Figura 3.4 muestra el esquema propuesto para desarrollar adaptadores en cualquier plataforma. Estos adaptadores están diseñados para servir como puentes entre la plataforma y una variedad de dispositivos externos o sistemas heredados. La razón principal de esta implementación es permitir una

comunicación fluida y efectiva con activos que, de otra manera, no podrían intercambiar información de manera directa con la plataforma.

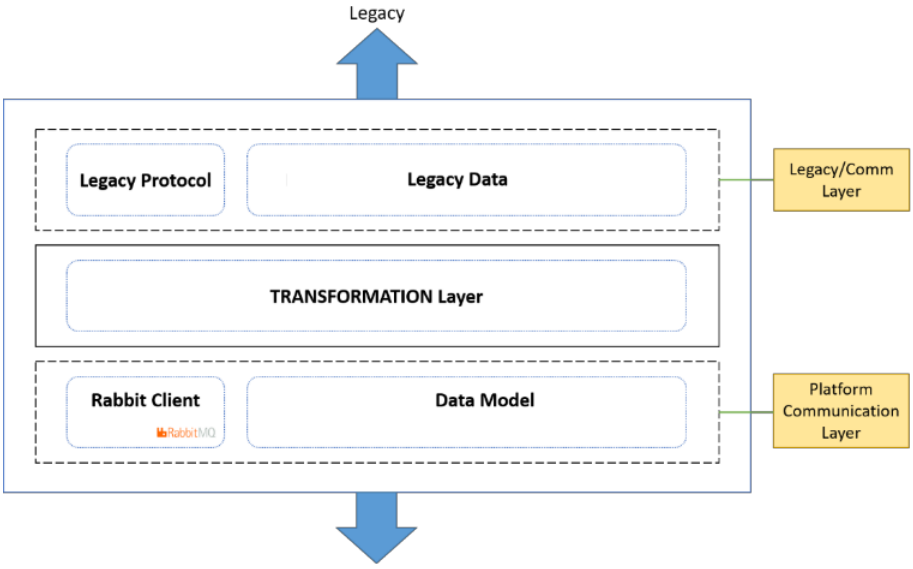

Figura 3.4: Esquema de un adaptador

Función de los Adaptadores

Los adaptadores se encargan de convertir, procesar y transmitir datos desde y hacia dispositivos externos. Al actuar como intermediarios, estos adaptadores toman los datos en su formato original y los transforman en un formato compatible con el modelo de datos de la plataforma. Esta conversión garantiza que la información de diversos orígenes se unifique bajo un esquema común, permitiendo un análisis y procesamiento coherentes.

Personalización según Activos Heredados

Dada la diversidad de dispositivos y sistemas heredados, cada adaptador puede requerir un diseño personalizado para satisfacer las especificaciones de comunicación y formato de datos de cada activo. Esto implica que para cada dispositivo externo o sistema heredado se debe desarrollar un adaptador específico que pueda interpretar y convertir adecuadamente sus datos al formato estandarizado de la plataforma.

Por lo tanto, la implementación de adaptadores es un componente esencial en la arquitectura de la plataforma, facilitando la integración de una amplia gama de dispositivos y sistemas heredados. Estos adaptadores no solo aseguran la interoperabilidad y la unificación de datos, sino que también amplían significativamente la capacidad de la plataforma para interactuar con un entorno tecnológico diverso, maximizando así su alcance y eficacia en la gestión de datos.

3.3.2. Modelo de datos

La plataforma se basará en un modelo de datos flexible y escalable, utilizando mensajes JSON para el intercambio de información entre los diferentes servicios a través del broker de mensajería. Esta subsección describe la estructura y el diseño de estos mensajes JSON.

Estructura de los Mensajes JSON

Los mensajes JSON creados para la plataforma se diseñan teniendo en cuenta las necesidades específicas de cada proyecto. La estructura de un mensaje típico incluye dos componentes principales: el tipo del mensaje y sus propiedades. El tipo del mensaje es un campo clave que identifica la naturaleza del mensaje y determina cómo debe ser procesado por el sistema. Este campo ayuda a clasificar los mensajes y dirigirlos a los servicios correspondientes. Las 'properties' del mensaje contienen los datos específicos del mensaje. Esta parte del mensaje alberga toda la información relevante que necesita ser transmitida, incluyendo campos específicos del proyecto.

Ejemplo de Mensaje JSON

A continuación se muestra un ejemplo simplificado de un mensaje JSON utilizado en la plataforma:

```
{
  "tipoMensaje": "TipoEjemplo",
  "properties": {
    "campo1": "valor1",
    "campo2": "valor2",
    "campo3": "valor3"
}
```

Listing 3.1: Ejemplo mensaje JSON

En este ejemplo, 'tipoMensaje' identifica la cola del mensaje y 'properties' contiene los campos específicos del mensaje. Cada campo dentro de 'properties' representa un dato diferente que necesita ser comunicado para el correcto desarrollo del proyecto y el flujo de datos.

La adopción de un modelo de datos basado en mensajes JSON proporciona una forma flexible y eficiente de intercambiar información entre los servicios en la plataforma. Este enfoque garantiza que la plataforma sea adaptable a diferentes necesidades de proyectos y facilita la integración y el procesamiento de datos a través del broker de mensajería.

3.3.3. Intercambio de datos

Un broker de mensajería es un intermediario software que se encarga de la transmisión de mensajes entre distintos sistemas, aplicaciones o servicios. Su propósito es gestionar, distribuir y almacenar mensajes, facilitando así la comunicación asincrónica. Los brokers de mensajería son esenciales en sistemas distribuidos donde los componentes necesitan intercambiar información de forma eficiente y confiable, sin estar directamente conectados entre sí [83]. Aquí es donde RabbitMQ, un avanzado sistema de colas de mensajes, juega un papel fundamental. Como un broker de mensajería eficiente, facilita el intercambio asincrónico de datos entre servicios desacoplados, contribuyendo significativamente a la escalabilidad, la resiliencia y la flexibilidad del sistema. Esta introducción explora cómo RabbitMQ se integra y beneficia a las arquitecturas de microservicios, proporcionando una base sólida para la comunicación eficiente y confiable entre servicios.

Características y Funcionamiento de RabbitMQ

RabbitMQ permite a las aplicaciones conectarse a colas de mensajes, definidas por un tema específico, para iniciar la comunicación. Estas colas almacenan los mensajes enviados por los productores hasta que una aplicación receptora se conecta y procesa el mensaje. Esta estructura de colas y temas permite la comunicación asincrónica entre aplicaciones, desacoplando la transmisión y recepción de datos y mejorando la modularidad del sistema.

Arquitectura de Colas de Mensajes

En la arquitectura básica de RabbitMQ, las aplicaciones productoras crean mensajes y los entregan al broker (la cola de mensajes), mientras que otras aplicaciones consumidoras se conectan a la cola y suscriben a los mensajes. Una aplicación puede actuar tanto como productor como consumidor, según

los requisitos de comunicación. Los mensajes se almacenan en la cola hasta que los consumidores los recuperan tal y como se observa en la Figura 3.5

Figura 3.5: Arquitectura de mensaje RabbitMQ

Enfoque en la Fiabilidad

RabbitMQ se centra en la fiabilidad más que en la velocidad. Las conexiones entre aplicaciones se realizan a través de *Transmission Control Protocol* (TCP) [84], donde el control de transporte es fundamental. Ofrece características para equilibrar el rendimiento con la fiabilidad, incluyendo la persistencia, confirmaciones de entrega, confirmaciones de publicación y alta disponibilidad. RabbitMQ es capaz de manejar la transmisión de miles de mensajes por segundo, lo que lo hace ideal para aplicaciones en tiempo real donde la pérdida de datos críticos no es una opción.

Escalabilidad y Alta Disponibilidad

El queuing de mensajes es clave para la escalabilidad de las aplicaciones. A medida que aumenta la carga de trabajo, se pueden añadir más trabajadores para procesar las colas más rápidamente. Además, las colas pueden ser espejadas en varios equipos de un clúster, garantizando la seguridad de los mensajes incluso en caso de fallo del hardware.

Ventajas de RabbitMQ en Microservicios

La integración de RabbitMQ en una arquitectura de microservicios aporta ventajas significativas [85]:

1. **Desacoplamiento y Flexibilidad:** RabbitMQ permite la comunicación entre servicios de manera flexible, promoviendo un diseño de sistema más modular y mantenible.

2. **Resiliencia y Fiabilidad:** Asegura la integridad de los datos y la continuidad del servicio, incluso en escenarios de fallos.

3. **Escalabilidad:** Facilita la gestión de cargas de trabajo crecientes y la expansión eficiente de la infraestructura.

4. **Soporte para Múltiples Protocolos:** RabbitMQ soporta varios protocolos de mensajería, incluyendo *Advanced Message Queuing Protocol* (AMQP) [86], *Simple text-oriented messaging protocol* (STOMP) [87], *Message Queuing Telemetry Transport* (MQTT) [88] y HTTP, ofreciendo versatilidad en la integración de sistemas.

5. **Extensibilidad:** La posibilidad de añadir plugins de terceros o desarrollar plugins personalizados permite una mayor adaptabilidad a necesidades específicas.

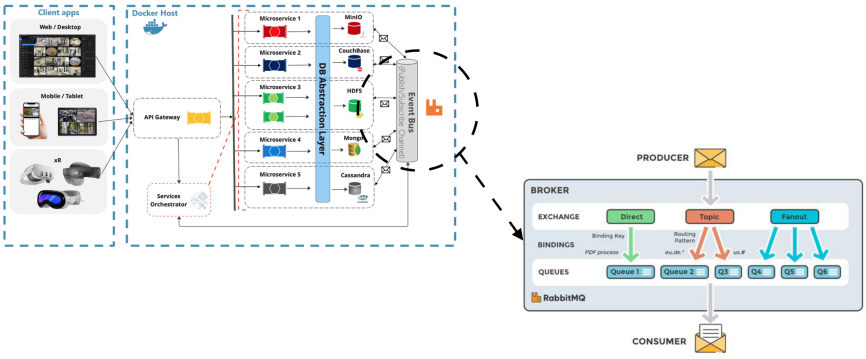

Figura 3.6: Esquema conceptual del middleware

Es por ello que RabbitMQ emerge como una herramienta poderosa y versátil y encaja a la perfección en la arquitectura orientada a microservicios propuesta véase la Figura 3.6, ofreciendo una solución robusta para el manejo de mensajes y la comunicación entre servicios. Su enfoque en la fiabilidad, la escalabilidad y la flexibilidad lo convierte en un componente esencial para sistemas modernos y dinámicos.

3.4. Almacenamiento de datos

3.4.1. Capa de abstracción de datos

La implementación de una capa de abstracción de base de datos es fundamental en la arquitectura de nuestra plataforma. Esta capa actúa como un mediador entre la aplicación y las bases de datos subyacentes, proporcionando

una interfaz genérica para interactuar con diferentes sistemas de almacenamiento de datos. Esta sección detalla la estructura y funcionalidad de la capa de abstracción de base de datos y cómo se adapta para conectar con diversas bases de datos según los requerimientos específicos de los proyectos [89].

Propósito de la Interfaz Genérica

La interfaz genérica es el núcleo de la capa de abstracción. Su objetivo es ofrecer un conjunto estandarizado de operaciones de base de datos, como consultas, inserciones, actualizaciones y eliminaciones, que pueden ser utilizadas independientemente del tipo de base de datos subyacente. Esta interfaz asegura que el resto de la aplicación pueda interactuar con la base de datos de una manera uniforme, sin necesidad de preocuparse por los detalles específicos de implementación de cada base de datos.

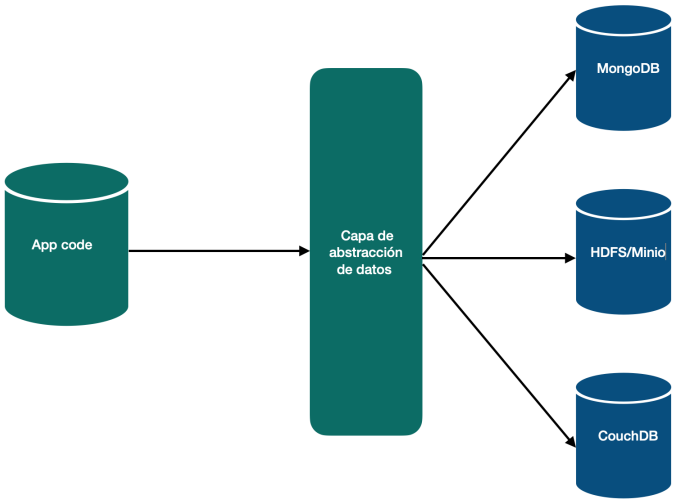

Figura 3.7: Concepto capa de abstracción de datos

La implementación de una interfaz genérica ofrece varias ventajas:

- **Desacoplamiento:** Separa la lógica de la aplicación de los detalles de implementación de la base de datos, permitiendo cambios en la base de datos sin afectar el resto de la aplicación.
- **Mantenibilidad:** Facilita el mantenimiento y la actualización del sistema, ya que los cambios solo necesitan realizarse en un solo lugar.

- **Flexibilidad:** Permite la fácil adición de nuevos tipos de bases de datos sin realizar grandes cambios en la aplicación.

Adaptación Según los Requerimientos del Proyecto

Reconociendo que diferentes proyectos pueden tener requisitos únicos para el almacenamiento de datos, la capa de abstracción está diseñada para ser altamente adaptable. Para cada proyecto, se pueden desarrollar y configurar conectores específicos que enlacen la interfaz genérica con el tipo particular de base de datos utilizado, ya sea SQL, NoSQL, o cualquier otro sistema de almacenamiento de datos.

Funcionalidad de los Conectores

Cada conector es responsable de traducir las operaciones definidas por la interfaz genérica a las llamadas específicas de la base de datos a la que está conectado. Esto incluye la conversión de consultas genéricas a consultas específicas del lenguaje de la base de datos y el manejo de las respuestas de la base de datos para que se ajusten al formato esperado por la aplicación.

En definitiva, la capa de abstracción de base de datos es un componente crucial en la arquitectura de nuestra plataforma, proporcionando la flexibilidad y escalabilidad necesarias para adaptarse a una variedad de requerimientos de proyectos y tipos de bases de datos. Esta capa garantiza que la plataforma pueda evolucionar y expandirse sin estar limitada por restricciones específicas de almacenamiento de datos.

3.4.2. Motores de almacenamiento

Las bases de datos son fundamentales en el almacenamiento y gestión de datos en cualquier plataforma digital. En nuestra plataforma global, la integración de diversos motores de base de datos es clave para ofrecer flexibilidad, escalabilidad y rendimiento óptimo. Esta sección explora cómo varios motores de base de datos se conectan a la plataforma global y su relevancia en distintos contextos de proyectos.

La plataforma global está diseñada para ser compatible con una variedad de motores de base de datos, cada uno ofreciendo características únicas y ventajas específicas para diferentes necesidades de proyectos. A continuación, se detallan algunos de los motores de base de datos más relevantes y cómo se integran en la plataforma:

Base de Datos	Tipo de Datos Almacenados
MongoDB	Datos no estructurados, Documentos
CouchDB	Datos no estructurados, Documentos
Minio	Objetos grandes (imágenes, videos, backups)
Cassandra	Datos distribuidos en múltiples servidores
HDFS	Grandes conjuntos de datos distribuidos

Tabla 3.1: Resumen de Bases de Datos y sus Tipos de Datos Específicos

Conexión con la Plataforma

Cada uno de estos motores de base de datos se conecta a la plataforma global a través de la capa de abstracción de base de datos, utilizando conectores específicos que traducen las operaciones de la plataforma en llamadas compatibles con cada tipo de base de datos. Esta integración permite que la plataforma aproveche las fortalezas de cada motor de base de datos, adaptándose a los requisitos específicos y la naturaleza de cada proyecto.

Por lo que la inclusión de diversos motores de base de datos refuerza la capacidad de la plataforma global para manejar una amplia gama de necesidades de datos. Desde el almacenamiento de documentos hasta el manejo de grandes volúmenes de datos distribuidos, la plataforma se beneficia de la flexibilidad y especialización que cada uno de estos motores ofrece, asegurando así un rendimiento óptimo y una adaptabilidad sin precedentes a los requisitos de los proyectos.

3.4.3. Fusión de datos

Tras establecer el marco de trabajo en la recolección e indexación de datos de diferentes fuentes, el siguiente paso clave en nuestra plataforma es la integración de estos datos heterogéneos. Esta fase crucial convierte los datos crudos y fragmentados en un conjunto estructurado y coherente, aplicando metodologías avanzadas de fusión de datos.

Técnicas de Fusión y Homogeneización de Datos

La fusión de datos implica la aplicación de algoritmos especializados que combinan y sintetizan datos de diferentes formatos y fuentes. Este proceso es esencial para transformar información desorganizada en datos lógicamente estructurados y uniformes. Una vez que los datos han sido refinados y fusionados, se almacenan en una ontología diseñada específicamente para cada proyecto.

Esto asegura una gestión eficaz y un acceso simplificado a la información, alineándola con las necesidades y especificaciones de cada proyecto.

Implementación de un Modelo de Representación Común

Con los datos ya procesados, es imprescindible implementar un *Conceptual Reference Model* (CRM) para estructurar la información de forma cohesiva. Las ontologías, que definen un conjunto de conceptos y relaciones en un dominio específico, son fundamentales en este contexto. Proporcionan un marco formal para organizar la información de manera significativa y semánticamente rica. La integración coherente de información de diversas fuentes y formatos es posible gracias a la aplicación de ontologías adecuadas [90]. Estas definen un marco de referencia estandarizado que promueve la interoperabilidad y el intercambio de datos eficiente.

La *Knowledge base* (KB) es un repositorio central que almacena conocimiento del dominio, incluyendo hechos, relaciones, reglas e inferencias. Se enriquece constantemente con información estructurada, facilitando análisis y generando nuevo conocimiento. La KB se actualiza continuamente con nueva información, reflejando una visión completa y actualizada del dominio. La KB no solo se nutre de datos actualizados, sino que también evoluciona con el tiempo, incorporando nuevos conocimientos y mejorando la toma de decisiones. El uso de técnicas de procesamiento de lenguaje natural, aprendizaje automático y minería de datos en la KB permite realizar análisis avanzados, descubriendo patrones y extrayendo conocimientos valiosos para informar decisiones y recomendaciones [91].

La integración y estructuración de datos en nuestra plataforma implica un proceso dinámico de fusión, almacenamiento y análisis de datos. A través de ontologías personalizadas y una base de conocimiento en constante evolución, aseguramos una gestión eficiente de los datos y una comprensión profunda del dominio investigado.

3.5. Procesado de datos

3.5.1. Encapsulación de servicios

En la planificación de nuestra arquitectura basada en microservicios, hemos elegido la encapsulación de servicios como nuestra estrategia principal. En esta sección, detallaremos cómo se implementa esta técnica de encapsulación y las razones por las que se considera el enfoque más adecuado para el desarrollo de módulos en nuestros proyectos.

Implementación de la Encapsulación mediante Contenedores Docker

La encapsulación de servicios en nuestra arquitectura se lleva a cabo a través del uso de contenedores Docker. Docker proporciona un entorno ligero, eficiente y estándar para que cada servicio se ejecute de manera aislada, asegurando la coherencia en múltiples entornos de desarrollo, pruebas y producción.

El empleo de contenedores Docker para la encapsulación de servicios ofrece múltiples ventajas:

- **Aislamiento de Servicios:** Cada microservicio se ejecuta en su propio contenedor, lo que garantiza que los procesos, la memoria y el espacio de almacenamiento estén aislados de otros servicios. Esto mejora la seguridad y reduce las posibles interferencias entre servicios.
- **Consistencia entre Entornos:** Docker asegura que los microservicios funcionen de manera idéntica en diferentes entornos, ya que cada contenedor contiene todas las dependencias del servicio.
- **Escalabilidad y Manejo de Recursos:** La arquitectura basada en contenedores facilita la escalabilidad, permitiendo que los servicios se escalen hacia arriba o hacia abajo rápidamente según la demanda. Además, la gestión eficiente de recursos reduce los costos operativos.
- **Despliegue y Actualizaciones Rápidas:** Los contenedores Docker permiten despliegues y actualizaciones rápidas y consistentes, lo que es crucial para la entrega continua y la rápida iteración de productos.
- **Simplicidad y Rapidez en el Desarrollo:** Docker simplifica el proceso de desarrollo y configuración, permitiendo a los desarrolladores centrarse en la lógica del servicio sin preocuparse por el entorno de ejecución.

La adopción de contenedores Docker para la encapsulación de servicios en una arquitectura orientada a microservicios ofrece un enfoque robusto y eficiente para el desarrollo y la gestión de servicios [92]. Esta metodología no solo mejora la seguridad y la coherencia entre entornos, sino que también facilita la escalabilidad, la gestión de recursos y la agilidad en el desarrollo, lo que resulta en una mayor eficiencia operativa y una mejor calidad de producto.

3.5.2. Orquestador de eventos

Dentro de nuestra arquitectura basada en microservicios, que utiliza Docker para la encapsulación de servicios, la orquestación de eventos juega un papel crucial en el control y la gestión eficiente de recursos. Esta sección aborda cómo la orquestación de eventos contribuye a optimizar el rendimiento y la utilización de recursos en la plataforma.

Control Dinámico y Gestión Eficiente de Recursos

La orquestación de eventos permite un control dinámico sobre los contenedores Docker, habilitando la activación y desactivación de servicios según las demandas de la plataforma. Esta flexibilidad es esencial para minimizar el uso de recursos, ajustándose a las necesidades operativas en tiempo real. Mediante la orquestación, los contenedores que no son necesarios pueden ser apagados o puestos en un estado latente, reduciendo así significativamente el consumo de recursos como *Central processing unit* (CPU) y memoria. Esta gestión inteligente de los contenedores asegura que solo se utilicen los recursos necesarios, evitando el desperdicio y optimizando el rendimiento general de la plataforma.

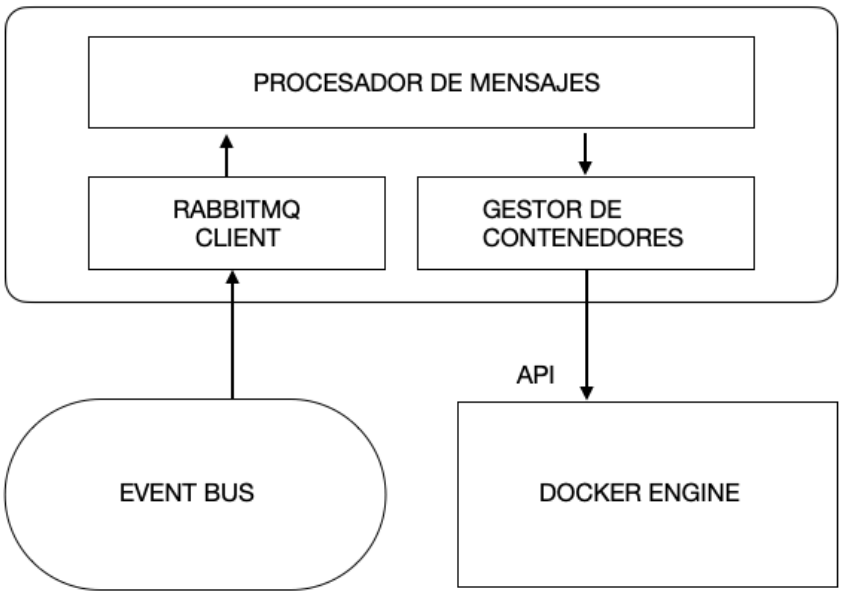

Figura 3.8: Esquema del gestor de eventos

Mejora del Rendimiento de la Plataforma

La capacidad de encender y apagar los contenedores según la demanda permite a la plataforma adaptarse a diferentes cargas de trabajo sin comprometer el rendimiento. Esta escalabilidad dinámica es crucial para mantener una al-

ta disponibilidad y eficiencia operativa, especialmente en escenarios de carga variable.

Puntos Clave de la Solución de Orquestación

- **Adaptabilidad:** La orquestación de eventos facilita la adaptación rápida a los cambios en las necesidades de la plataforma, mejorando la respuesta ante diferentes escenarios operativos.
- **Eficiencia en Costes:** Reduciendo el consumo innecesario de recursos, la orquestación de eventos contribuye a una mayor eficiencia en costos, lo que es beneficioso desde una perspectiva económica y operativa.
- **Mantenimiento y Actualizaciones Simplificados:** La gestión centralizada de contenedores permite un mantenimiento y actualizaciones más sencillos y menos propensos a errores, mejorando la fiabilidad del sistema.

La orquestación de eventos en una arquitectura de microservicios encapsulada con Docker es un enfoque estratégico que mejora significativamente la gestión de recursos y el rendimiento de la plataforma. Al proporcionar un control dinámico y adaptable sobre los contenedores, se asegura un funcionamiento eficiente, económico y confiable de la infraestructura de servicios.

3.6. Representación de datos

Esta sección se sumerge en el mundo de la representación de datos, un paso crucial que sigue a la intensiva fase de procesamiento de datos detallada previamente. Aquí, el énfasis se coloca en cómo los conjuntos de datos extensos y analíticamente procesados se transforman en visualizaciones comprensibles y operativas. Este proceso es de suma importancia, ya que sirve de puente entre el análisis detallado de los datos y su aplicación práctica, especialmente en escenarios críticos como la prevención de riesgos, la investigación profunda y la gestión eficiente de situaciones de emergencia.

La visualización de datos es un componente esencial que sigue al análisis de datos. Mientras que el análisis se concentra en identificar tendencias, anomalías y correlaciones, la visualización se encarga de transformar estos descubrimientos en representaciones gráficas claras y entendibles. Esta transición es vital para que los operarios y los responsables de toma de decisiones accedan a información relevante de manera intuitiva, apoyando sus acciones con datos contextualizados y profundamente analizados.

Aplicaciones Prácticas de la Visualización de Datos

En el ámbito de la prevención y la supervisión de misiones, las visualizaciones intuitivas y detalladas son herramientas clave para la interpretación de tendencias emergentes y patrones en los datos. Esto es esencial para anticipar posibles escenarios de riesgo y para formular respuestas basadas en información sólida [93]. Las herramientas de visualización desempeñan un papel crucial en simplificar la complejidad de grandes volúmenes de datos, convirtiéndolos en información manejable y significativa.

En contextos de respuesta rápida, la claridad y la capacidad de presentar la información de forma directa y rápida son críticas. Las visualizaciones deben ser diseñadas para resaltar la información más relevante, permitiendo a los operarios actuar con precisión y rapidez bajo presión.

En nuestra arquitectura, se han desarrollado *Human Machine Interface* (HMI)s especializados que utilizan diversas técnicas de visualización, adaptadas a la naturaleza de los datos. Se exploran pruebas de concepto innovadoras que incorporan tecnologías de realidad virtual o realidad aumentada, expandiendo el alcance de las herramientas de visualización disponibles.

Como se detalla en los capítulos 4 y 5, las metodologías de visualización se adaptan específicamente al contexto de uso. Para investigaciones y prevención, donde las tareas pueden ser más estáticas, entornos de escritorio pueden ser suficientes. En cambio, para respuestas inmediatas, se prioriza la movilidad, integrando dispositivos como tablets para uso en terreno, complementando los sistemas de control centralizados.

Este apartado evidencia cómo la representación visual de datos es fundamental en la transición del análisis a la aplicación práctica. Al enfocarse en la claridad, la contextualización y la accesibilidad, la visualización de datos se convierte en una herramienta indispensable en la gestión y toma de decisiones basada en datos.

3.6.1. Dashboard

Para facilitar el acceso a estas visualizaciones, se ha creado un dashboard web unificado, como se muestra en la Figura 3.9. Este entorno centralizado permite a los usuarios ejecutar análisis y visualizar resultados de manera consolidada, fortaleciendo la conciencia situacional y apoyando la toma de decisiones informadas.

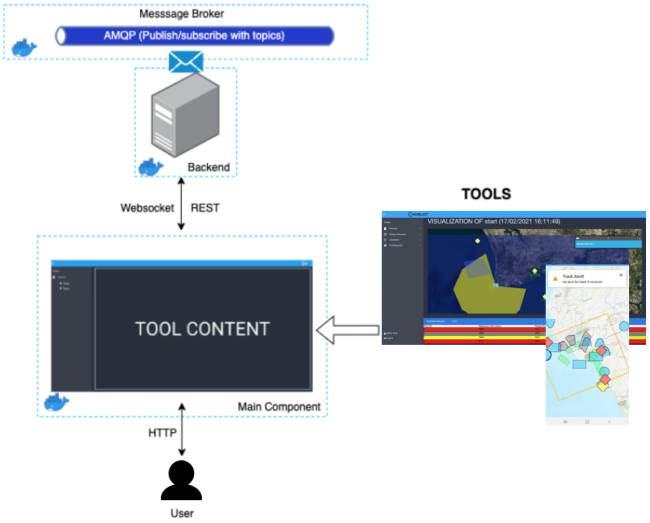

Figura 3.9: Arquitectura HMI

La interacción entre las distintas HMIs y los datos almacenados se estructura a través de una capa intermedia, el *Backend*, que coordina el flujo de información. Para análisis en tiempo real, el *Backend* se sincroniza con actualizaciones activas, mientras que para recuperaciones de datos más convencionales, realiza consultas directas a la base de datos. La comunicación entre el *Frontend* y el *Backend* se adapta según las necesidades operativas, utilizando *websockets* para actualizaciones en tiempo real y una API REST para intercambios de datos estructurados.

3.6.2. Visualización xR

En esta sección, se explora la implementación de tecnologías de xR, incluyendo VR y AR, en la visualización de datos para proyectos. Estas tecnologías avanzadas, como las gafas de realidad virtual y aumentada, ofrecen modos innovadores y efectivos de interactuar con los datos, proporcionando experiencias inmersivas y enriquecidas. En los capítulos 4 y 5, se examinan en detalle estas modalidades de visualización y su aplicación en distintos contextos de proyecto.

A continuación, se presenta la Tabla 3.2 que genera la comparativa sobre las ventajas clave de la VR y la AR:

Característica	Realidad Aumentada (AR)	Realidad Virtual (VR)
Interacción con el entorno	Interactúa con el mundo real	Entorno completamente virtual
Aplicación en proyectos	Enriquecimiento de entornos reales	Simulaciones y entornos controlados
Inmersión	Parcial, mantiene la percepción del entorno real	Total, aislamiento del entorno real
Movilidad	Generalmente alta, portátil	Limitada por el espacio físico
Casos de uso	Mantenimiento, formación, diseño	Entrenamiento, educación, entretenimiento

Tabla 3.2: Comparativa de las Ventajas de Realidad Aumentada y Realidad Virtual

Integración de xR en los Proyectos

La visualización xR se integra en los proyectos para mejorar la comprensión y la interacción con los datos. En el ámbito de la AR, se explora cómo la superposición de información digital en el entorno físico puede asistir en tareas como mantenimiento y diseño.

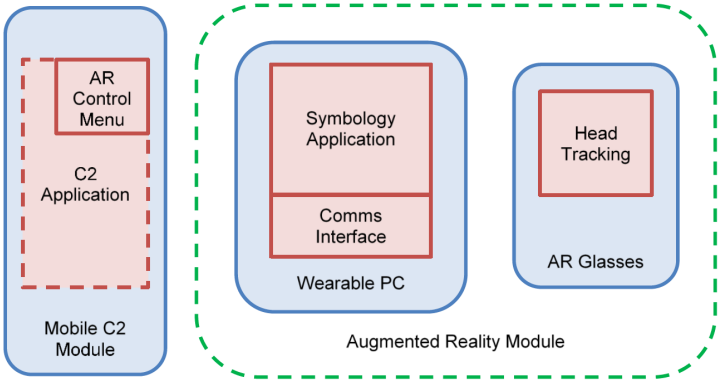

Figura 3.10: Esquema general AR

Por otro lado, la VR se utiliza para crear simulaciones detalladas, permitiendo a los usuarios interactuar con entornos virtuales para formación o análisis detallado de datos. Esto hará que se tenga conocimiento más extenso sobre la conciencia situacional.

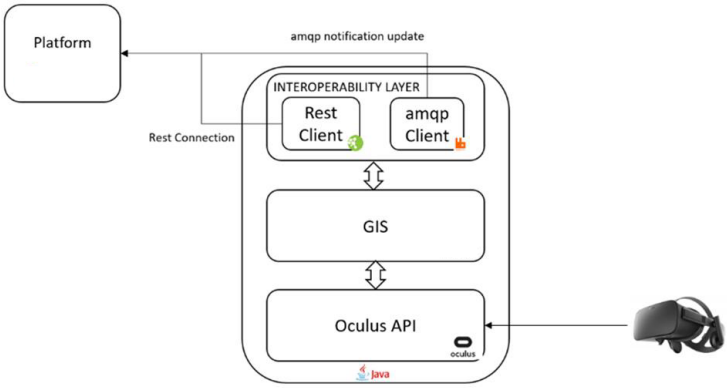

Figura 3.11: Esquema general VR

La visualización xR, abarcando tanto la realidad aumentada como la virtual, ofrece oportunidades sin precedentes para la visualización y el análisis de datos en proyectos. Estas tecnologías no solo mejoran la experiencia del usuario, sino que también abren nuevas vías para la interacción intuitiva y profunda con los datos, respaldando la toma de decisiones informadas y la comprensión detallada de entornos complejos.

Capítulo 4

Validación de la arquitectura: Caso 1 - CAMELOT

4.1. Introducción

La historia de los *Unmanned Aerial System* (UAS) [94] ha estado marcada por un enfoque centrado en el vehículo. El *Original equipment manufacturer* (OEM) se ha concentrado en el diseño de aeronaves, relegando las *Ground Control Station* (GCS) a un papel secundario, principalmente como herramientas para probar los dispositivos. Esta tendencia ha dado su resultado en una falta de estandarización entre diferentes sistemas, así como en la prevalencia de flujos de datos telemétricos y de sensores propietarios [95]. Esta situación ha creado una barrera tecnológica significativa, impidiendo la interoperabilidad entre los UAS existentes, un aspecto crítico para su integración efectiva en las operaciones de los profesionales en el campo.

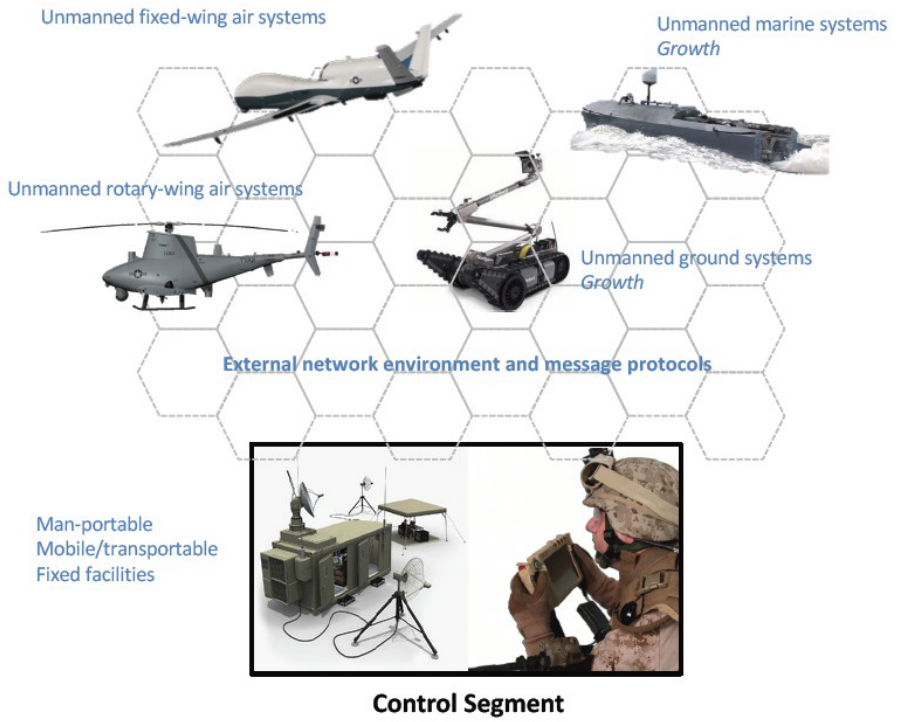

Figura 4.1: Visión del segmento de control de vehículos no tripulados (UxV)

Sin embargo, los profesionales no solo adquieren vehículos aéreos no tripulados, sino que también adquieren sistemas no tripulados capaces de operar en todos los dominios: aire, tierra y mar. En este contexto, la interoperabilidad entre estos sistemas se considera un elemento crucial para la próxima generación de sistemas no tripulados. Esto potenciaría significativamente la eficiencia y capacidad operativa, a través del intercambio de recursos y la utilización de información común generada por dichos sistemas [96].

Actualmente, para los sistemas no tripulados multidominio, no existe una arquitectura de C2 ampliamente adoptada. Por tanto, este capítulo se enfoca en presentar un análisis de la arquitectura propuesta para CAMELOT, describiendo la solución seleccionada, así como los servicios desarrollados.

Se realizará un análisis basado en los criterios definidos y validados. Estos criterios incluyen:

- **Aceptabilidad por los usuarios y la industria**: Probabilidad de que los usuarios y la industria de sistemas no tripulados adopten la arqui-

tectura analizada para comunicar comandos de misión y/o controles de plataforma desde la estación de control al vehículo no tripulado.

- **Facilidad de uso**: Conocimiento avanzado de CAMELOT sobre la arquitectura analizada y su implementación.
- **Diseño para interoperabilidad**: Capacidad de diferentes aplicaciones para interactuar dinámicamente, facilitando la interfaz fluida de múltiples fuentes de información.
- **Diseño para reutilización**: Grado de aceptabilidad de la arquitectura analizada para incluir componentes previamente diseñados.
- **Diseño para interoperabilidad**: Grado en que la arquitectura analizada puede emplear diversas combinaciones de módulos y/o funcionalidades del sistema.
- **Diseño para mantenibilidad**: Grado en que un producto permite el reemplazo seguro, rápido y fácil de sus componentes/partes.
- **Diseño para extensibilidad**: Capacidad de la arquitectura analizada para agregar o modificar el comportamiento de las funcionalidades del sistema. Así como la inclusión de nuevos servicios.
- **Modularidad**: Estructura de la arquitectura analizada en términos de organización de servicios.
- **Uso de estándares abiertos**: Uso de estándares previamente desarrollados y actualmente en uso.

En este entorno de rápida evolución tecnológica, el proyecto CAMELOT se propone liderar el camino hacia una nueva era de sistemas no tripulados, destacando la importancia de una arquitectura robusta, interoperable y adaptable. Este capítulo sienta las bases para comprender los desafíos y las soluciones propuestas en el desarrollo de dicha arquitectura.

4.2. Objetivos técnicos

Los objetivos técnicos del proyecto CAMELOT se centran en desarrollar una solución integral de comunicaciones y gestión de datos para operaciones en áreas remotas y críticas. Los objetivos incluyen:

1. **Integración Multi-dominio:** Desarrollar una plataforma que integre capacidades operativas en diferentes dominios (tierra, mar, aire, ciberespacio y espacio), asegurando una coordinación efectiva y eficiente entre ellos.

2. **Optimización de la Toma de Decisiones:** Implementar algoritmos avanzados de aprendizaje automático y análisis de datos para optimizar la toma de decisiones en entornos operativos complejos y dinámicos.

3. **Visualización y Conciencia Situacional:** Crear interfaces de usuario avanzadas para proporcionar visualización en tiempo real y conciencia situacional mejorada, incluyendo realidad aumentada y aplicaciones móviles.

4. **Comunicaciones Seguras y Resilientes:** Establecer un sistema de comunicaciones seguro y resistente que asegure la transmisión de datos confiable en diferentes escenarios operativos.

5. **Interoperabilidad y Estándares:** Garantizar la interoperabilidad entre diferentes sistemas y plataformas, siguiendo estándares internacionales y adaptándose a diferentes necesidades operativas.

6. **Formación y Simulación:** Desarrollar herramientas de formación y simulación para capacitar al personal en el uso de las tecnologías CAMELOT, mejorando así su eficacia operativa.

7. **Establecer una Red de Comunicación Híbrida Segura:** Desarrollar una red híbrida segura para garantizar conectividad de alta disponibilidad en áreas remotas fuera de la cobertura de redes de comunicación tradicionales.

8. **Sistema de Alerta Temprana y Gestión de Datos:** Desarrollar el *Early Warning Engine* (EWE) para procesar datos entrantes y generar alertas relevantes, apoyándose en un eficiente sistema de gestión de datos.

9. **Servicios de Monitorización y Configuración Centralizados:** Establecer servicios de monitorización y configuración para facilitar la gestión eficiente de todos los componentes del proyecto.

El proyecto CAMELOT busca liderar el desarrollo de tecnologías avanzadas para operaciones multi-dominio, estableciendo nuevos estándares en eficiencia operativa, seguridad y capacidad de respuesta. Los objetivos técnicos aquí presentados son esenciales para el éxito del proyecto y la consecución de sus metas a largo plazo.

4.3. Arquitectura de CAMELOT

La plataforma CAMELOT se fundamenta en una arquitectura distribuida, la cual ha sido meticulosamente diseñada para cumplir con los requisitos esenciales de diseño: escalabilidad, disponibilidad y seguridad [97]. Esta estructura no solo responde eficientemente a las necesidades actuales, sino que también posee la flexibilidad necesaria para adaptarse y evolucionar según las demandas futuras y los cambios en los requerimientos de los usuarios.

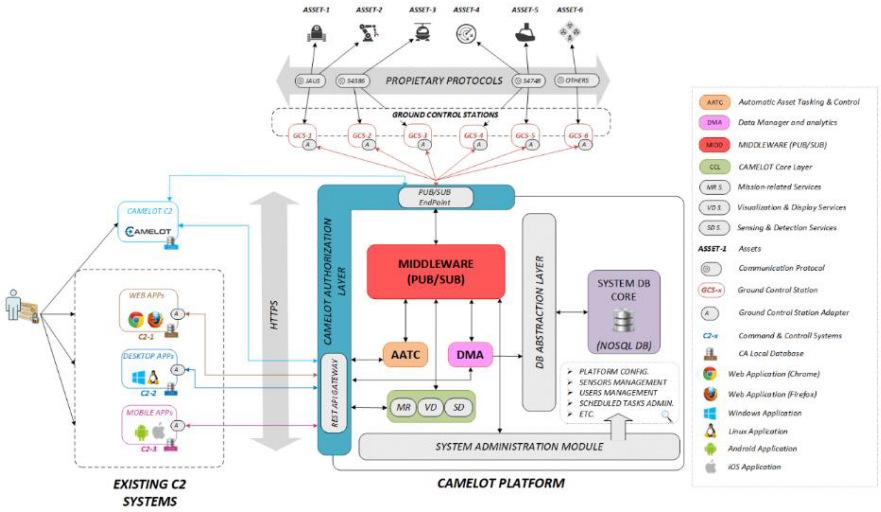

Figura 4.2: Concepto CAMELOT

El núcleo de la plataforma se estructura en cuatro módulos principales, desarrollados a lo largo del proyecto:

1. **CAL:** Es un módulo clave que se encarga de adaptar los distintos modelos de datos e información procedentes de los activos conectados, alineándolos con el modelo de datos CAMELOT. Su función es esencial para garantizar una integración coherente de los datos dentro de la plataforma.

2. **AATC:** Proporciona métodos diversos para el control efectivo de los activos que se encuentran conectados a la plataforma. Este módulo es vital para la gestión y operativa eficiente de los recursos disponibles.

3. **DMA:** Aporta a la plataforma un conjunto de funciones avanzadas para el análisis y la gestión de datos, permitiendo realizar operaciones de información de alto nivel.

4. **Middleware:** Facilita la interacción y el intercambio de información entre los distintos submódulos y servicios implementados en la plataforma CAMELOT. Este componente, basado en el paradigma de Publicar-Suscribir, permite desacoplar todas las interacciones, proporcionando servicios e información conforme al modelo de datos de CAMELOT. Para el middleware de la arquitectura se ha seleccionado RabbitMQ, utilizando JSON como formato para el intercambio de mensajes.

5. **Capa Central CAMELOT:** Engloba todas las funcionalidades internas requeridas por la plataforma para desempeñar las capacidades principales de CAMELOT. Este módulo abarca servicios relacionados con la misión, servicios de visualización, y servicios de detección y sensorización.

Además, la plataforma ofrece diversos servicios de interoperabilidad accesibles a través de una API REST, lo que permite a los sistemas C2 legados interactuar con la plataforma, obtener y alimentar información o consumir los servicios proporcionados.

La arquitectura de CAMELOT descrita anteriormente se ha desarrollado dentro del contexto de un "Marco de Mando y Control", que incluye también el desarrollo de los adaptadores necesarios para la infraestructura C2 existente, así como la integración del resto de activos en CAMELOT (principalmente las GCS de los diferentes UxVs).

4.3.1. Servicios relacionados con misiones

En el innovador entorno del sistema CAMELOT, el módulo de preparación de misiones desempeña un papel crucial como coordinador entre los demás módulos del sistema. Esta funcionalidad principal se encarga de asegurar una gestión eficiente y coherente de las diversas operaciones, actuando como un eje central en la comunicación y coordinación de las tareas.

A pesar de la interdependencia operativa de los módulos dentro del sistema CAMELOT, es importante destacar que ciertos módulos, específicamente el de optimización de misiones, replanificación de misiones y gestión de la energía de los UxV, operan de manera independiente y no interactúan directamente entre sí. Esta característica de diseño refleja una estrategia deliberada para maximizar la eficiencia y efectividad de cada módulo, permitiendo una especialización y un enfoque más concentrado en sus respectivas funciones.

El modelo de datos utilizado para la comunicación entre el módulo de preparación de misiones y los otros módulos, es un aspecto fundamental en la arquitectura del sistema CAMELOT. Este modelo garantiza que la información se transmita de manera eficiente, precisa y coherente, facilitando así una preparación de misiones más efectiva y una ejecución exitosa de las operaciones.

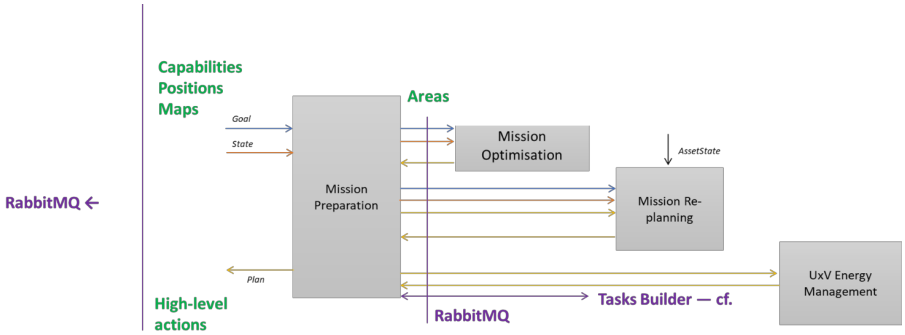

Figura 4.3: Flujo del módulo de misiones

Para poder establecer una comunicación entre módulos se han generado una serie de mensajes, que se pueden observar en las Tablas 4.1-4.2 :

Nombre del Mensaje	Descripción Corta
AssetStateRequest	Mensaje para solicitar el estado del asset
AssetStateResponse	Mensaje enviado desde AvailableResourceMapper tras recibir un mensaje AssetStateRequest
AssetLinkedInfoRequest	Mensaje para solicitar el AssetLinkedInfo
AssetLinkedInfoResponse	Mensaje enviado desde AvailableResourceMapper tras recibir un mensaje AssetLinkedInfoRequest
VehicleRequest	Mensaje utilizado por la Interfaz de Usuario para recopilar la lista de vehículos en el área de la misión
VehicleResponse	Respuesta del mensaje que lista los vehículos dentro del área de la misión
PrepareMissionRequest	Mensaje enviado por la interfaz de usuario que contiene el contexto completo de la misión
MissionPreparationRequest	Mensaje enviado para calcular la lista de acciones a realizar en la misión por los UxVs
Plan	Lista de acciones para cada UxV

Tabla 4.1: Descripción de Mensajes - Parte 1

Nombre del Mensaje	Descripción Corta
OptimizeMissionEnergyRequest	Mensaje para solicitar una optimización en el consumo de energía. Este mensaje contiene la lista de acciones para cada UxV.
MissionEnergyPack	Mensaje que contiene la nueva lista de acciones para cada UxV después de la optimización.
DetailedPlanRequest	Este mensaje contiene el contexto de la misión y la lista de alto nivel de acciones.
DetailedPlan	Lista de planes detallados para cada UxV (que contiene trayectoria y configuración del sensor) para ejecutar la misión
MissionVehicle	Mensaje enviado a cada GCS conteniendo el plan detallado para su propio UxV. GCS es responsable de enviar el plan al UxV.
Mission	Este mensaje contiene toda la misión (contexto, UxV, plan detallado, configuración del sensor).

Tabla 4.2: Descripción de Mensajes - Parte 2

Optimización de la misión

Los sistemas *Command, control, communications, computers, intelligence* (C4I) se ven fundamentalmente afectados por la toma de decisiones. Debido al amplio alcance de estos sistemas y a la enorme cantidad de datos, es necesario automatizar algunas partes de este proceso. Un ejemplo de un problema donde los sistemas C4I son de interés es la gestión de múltiples vehículos que deben colaborar para llevar a cabo una misión. Hoy en día, los vehículos están cada vez más automatizados y equipados con consolas C2, que permiten explorar los sistemas con un nivel de abstracción más alto. En los sistemas industriales, la parte de soporte de decisiones de un sistema de vehículo C2 de última generación se entrega con piloto automático, sensor, actuador y modelos de misión, así como un sistema experto. Uno de los primeros problemas encontrados en los sistemas C2 es el gran número de variables involucradas en las decisiones [98]. Aunque existe literatura sobre cómo optimizar estos problemas [99], los inconvenientes de la toma de decisiones no siempre pueden modelarse de manera efectiva y a menudo nos encontramos con problemas de rendimiento o flexibilidad para optimizar las acciones de los agentes considerados. La implementación

de C4I para múltiples vehículos en el marco del proyecto CAMELOT tiene como objetivo extender el uso de *Autonomous Underwater Vehicle* (AUV)/*Remote Operated Vehicle* (ROV) para facilitar la creación, planificación y ejecución de operaciones de vigilancia fronteriza. De hecho, la mayoría de las operaciones de vigilancia son llevadas a cabo por las guardias nacionales, con medios humanos, sensores, etc. Al ser su número limitado de activos, la dependencia de su trabajo constituye un riesgo en términos de eficiencia. El uso prolongado de vehículos no tripulados o pilotados a distancia podría resolver este problema, pero dado que generalmente están adaptados a una tarea específica y son difíciles de usar, su despliegue es complejo [100].

Es por ello que se plantea un módulo de planificación de misiones, que será el encargado de implementar modelos y algoritmos para encontrar la mejor secuencia de tareas para realizar una misión específica. Dado un estado inicial del sistema, un objetivo deseado (parcial o completo) y un conjunto de posibles acciones y su duración, el módulo de planificación calculará y devolverá una secuencia de acciones que conducen a un estado compatible con el objetivo, teniendo en cuenta que existe una concurrencia requerida entre acciones.

Planificador de Misiones

El planificador de misiones es un algoritmo ad-hoc que resuelve el siguiente problema:

$$\text{minimizar } J = \sum_{j=1}^{NM} c_j x_j$$

sujeto a las siguientes restricciones:

$$\sum_{j=1}^{NM} V_{ij} x_j = 1$$

y:

$$\sum_{j=1} x_j = 1$$

Donde los *petals* del vehículo p están numerados N_p a $N_{p+1} - 1$, con $N_1 = 1$ y $N_{Nv+1} = NM + 1$, y los índices tienen los rangos $i \in \{1, \ldots, Nw\}, j \in \{1, \ldots, NM\}, p \in \{1, \ldots, Nv\}$. c_j es un vector de costes (tiempos de misión) para cada *petal*, x_j es una variable de decisión binaria igual a uno si el *petal* j es seleccionado, y 0 en caso contrario. La primera restricción garantiza que la tarea i se realice exactamente una vez. La segunda restricción impide que se asigne más de un *petal* a cada vehículo. Este planificador de misiones se basa en la formulación del problema propuesto por *John Bellingham, Michael*

Tillerson, Arthur Richards y Jonathan P. How, del *Massachusetts Institute of Technology* (MIT). Estos autores demuestran que el problema de la asignación óptima de M tareas entre V vehículos puede formularse como un problema de *Mind Mapping Knowledgebase Prototyping* (MMKP).

El planificador de misiones realiza los siguientes pasos:

1. Construir la lista de todos los *petals* posibles. Un *petal* es un subconjunto de L índices en el intervalo $\{1, \ldots, Nw\}$.

2. Evaluar el coste de cada *petal* para cada drone. Esta evaluación se basa en trayectorias proporcionadas por una capa de transporte. Esta evaluación se realiza para todos los $L!$ órdenes posibles de los índices del *petal* evaluado (esta evaluación puede realizarse utilizando algún enfoque heurístico). Se devuelve el coste del mejor orden. El mejor orden de ejecución de un *petal* puede depender del drone considerado (debido, por ejemplo, a diferentes puntos de partida o radios de giro).

3. Seleccionar Nv *petals* (uno por drone) de tal manera que la unión de estos satisfaga las dos restricciones explicadas anteriormente: cada tarea se realiza exactamente una vez.

Ilustramos estos conceptos a continuación con $Nw = 4$ y $Nv = 2$ (4 tareas a ser asignadas entre 2 drones). Para cada dron, los 15 *petals* a evaluar son los siguientes:

- 4 *petals* de longitud 1:
  - $p = 0 \rightarrow \{0\}$,
  - $p = 1 \rightarrow \{1\}$,
  - $p = 2 \rightarrow \{2\}$,
  - $p = 3 \rightarrow \{3\}$
- 6 *petals* de longitud 2:
  - $p = 4 \rightarrow \{0, 1\}$,
  - $p = 5 \rightarrow \{0, 2\}$,
  - $p = 6 \rightarrow \{0, 3\}$,
  - $p = 7 \rightarrow \{1, 2\}$,
  - $p = 8 \rightarrow \{1, 3\}$,
  - $p = 9 \rightarrow \{2, 3\}$
- 4 *petals* de longitud 3:

- $p = 10 \rightarrow \{0, 1, 2\}$,
- $p = 11 \rightarrow \{0, 1, 3\}$,
- $p = 12 \rightarrow \{0, 2, 3\}$,
- $p = 13 \rightarrow \{1, 2, 3\}$

- 1 *petal* de longitud 4:
  - $p = 14 \rightarrow \{0, 1, 2, 3\}$

La evaluación de cada *petal* (desde $p = 0$ hasta 15) se realiza para cada dron. En el caso más general, el coste de un *petal* p difiere de un drone a otro, ya que no se supone que los drones tengan las mismas posiciones iniciales, radio de giro, velocidad, etc.

En el siguiente ejemplo (con 2 drones y 3 tareas), se puede ver que el dron 1 y el dron 2 no realizarán el *petal* {1, 2, 3} en el mismo orden, debido a su diferente estado inicial. Más concretamente, para cada dron, se tendrán que probar múltiples hipótesis de ordenación. Si la combinatoria es débil, se pueden evaluar todas las permutaciones. Si la combinatoria es alta (si la longitud de los pétalos excede típicamente 9), este paso de ordenación se puede realizar utilizando una heurística, como 2-opt. Por ejemplo, para un *petal* de longitud 3, hay 3! = 6 órdenes posibles. Para el *petal* de longitud 4, hay 4! órdenes posibles a evaluar. Dada una hipótesis de orden a evaluar, se utilizará la capa de transporte para determinar la trayectoria correspondiente para el drone considerado. En el siguiente ejemplo, la capa de transporte es trivial, ya que los drones vuelan en línea recta. En el caso más general, la capa de transporte tiene en cuenta la velocidad, el radio de giro del dron, etc., y se ocupa de áreas prohibidas que deben evitarse. Dichas áreas prohibidas podrían, en el caso más general, diferir de un drone a otro debido a su diferente altitud, por ejemplo.

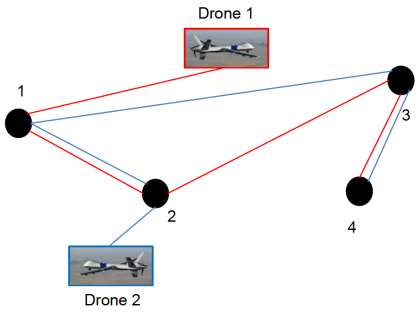

Figura 4.4: Ejemplo de ejecución de pétalo por el dron 1 y dron 2.

En la Figura 4.4, el drone 1 ejecuta el *petal* {1, 2, 3, 4} en el orden [1, 2, 3, 4], mientras que el dron 2 lo ejecuta en el orden [2, 1, 3, 4]. Finalmente, una vez que los 15 pétalos han sido evaluados para cada uno de los 3 drones, se debe seleccionar un *petal* por dron (primera restricción), de tal manera que la unión de los 3 *petals* sea [1, 2, 3, 4, 5], lo que significa que cada tarea se realiza exactamente una vez (segunda restricción). Un ejemplo de asociación correcta de dichos *petals* se ilustra a continuación en la Figura 4.5. Al dron 1 se le asigna el *petal* {1, 3} y al drone 2 el *petal* {2, 4}

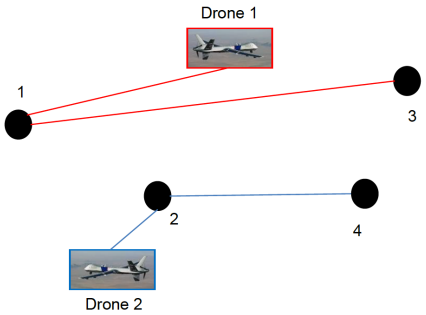

Figura 4.5: Asociación de *petals* para los drones 1 y 2.

La Figura 4.6 muestra el resultado de la asignación con 11 tareas y 4 drones.

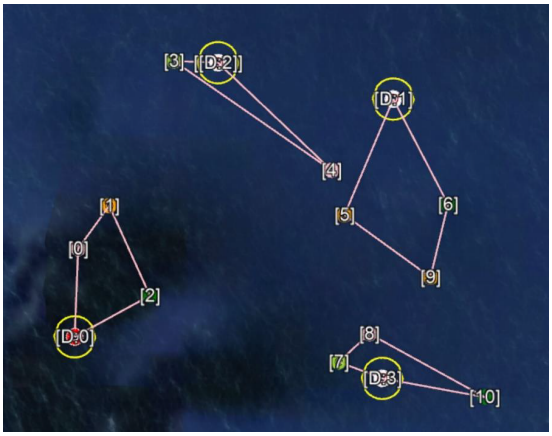

Figura 4.6: Resultado de la asignación de tareas a 4 drones.

Enfoque del Concepto de Tarea en CAMELOT

En el presente caso, una tarea es la cobertura de una zona de interés. Desde el punto de vista del movimiento, esto significa que el dron seguirá una trayectoria cubriendo esta zona (llamamos recorrido a tal trayectoria). Generalmente, hay muchas formas de cubrir la misma zona, por lo que hay muchos recorridos posibles para cualquier zona de interés. El dron al que se le asigna una tarea tendrá que elegir un recorrido r entre R.

El planificador de recorridos es responsable de la definición de un conjunto de trayectorias candidatas utilizadas para cubrir una zona de interés. Se llama recorrido a cualquier trayectoria. Se puede observar el concepto de recorrido en la Figura 4.7 con un sensor de huella h:

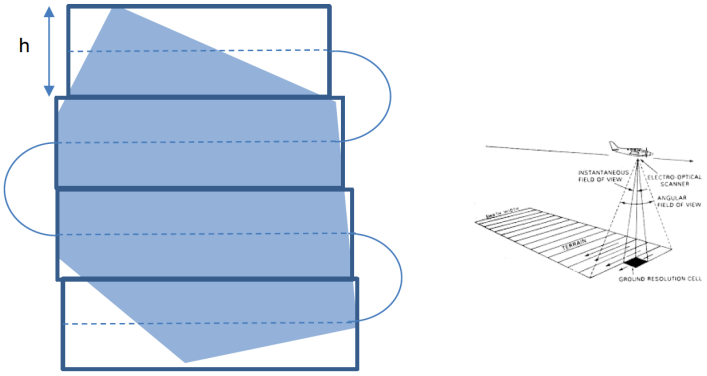

Figura 4.7: Ejemplo de un recorrido cubriendo una zona de interés, dado un campo de visión del captor h.

La Figura 4.7 es un ejemplo de recorrido que cubre una zona de interés (polígono en azul), dado un campo de visión proyectado en el suelo h. Una zona de interés dada puede ser cubierta por múltiples recorridos, es decir, trayectorias que cumplen con la misión (proporcionando imágenes de la resolución especificada). Desde el punto de vista de la misión, cualquiera de ellas es aceptable.

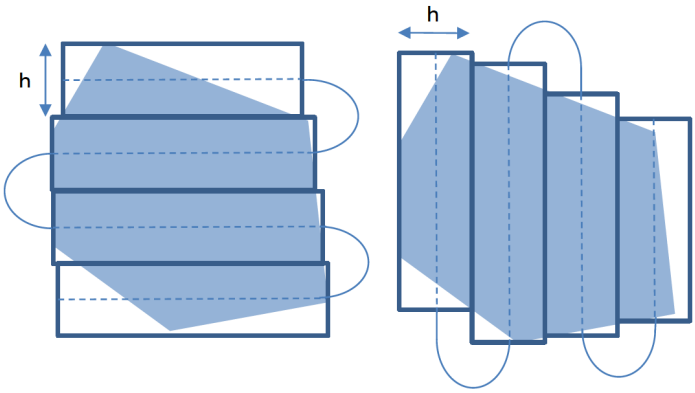

Figura 4.8: Ejemplo de recorridos candidatos para una zona de interés dada. Se podrían imaginar otras estrategias de cobertura de zona.

Como se puede ver, los recorridos pueden tener diferentes longitudes. Un candidato de longitud $L1$ podría ser elegido sobre un recorrido de longitud $L2 < L1$ si el coste global (ir a la zona, cubrir la zona y regresar) es mejor. La capa de transporte tendrá que elegir el mejor recorrido, en función del contexto (de qué punto de referencia viene el dron y a qué punto de referencia tendrá que unirse después de que termine la cobertura del área).

Arquitectura del Planificador de Misiones

El planificador de misiones tiene la siguiente arquitectura:

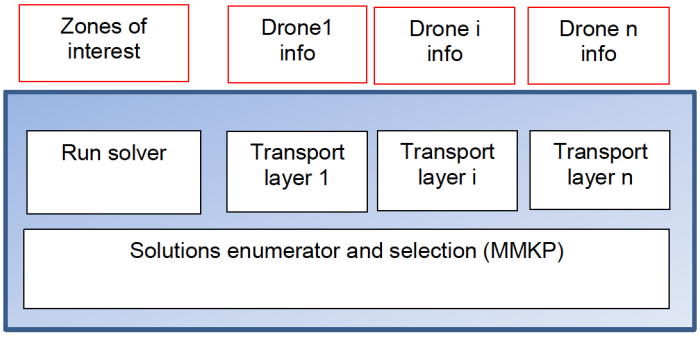

Figura 4.9: Arquitectura del planificador de misiones.

La Figura 4.10 muestra el plan resultante calculado y devuelto, utilizando el conjunto de datos en la *Graphical User Interface* (GUI). En este ejemplo, podemos ver 3 vehículos que realizarán algunas misiones de reconocimiento en las áreas a cubrir, tránsito entre zonas y finalmente regresando a su posición inicial.

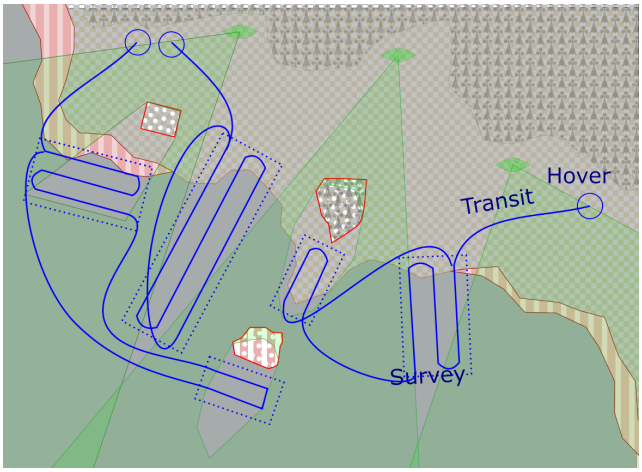

Figura 4.10: GUI utilizada para verificar el cálculo de un plan en diversas situaciones.

Esta GUI ha sido ampliamente utilizada para verificar el cálculo de un plan en muchas situaciones. Además, es muy conveniente para mostrar y analizar resultados que un archivo de texto puro.

Preparación de la misión

El objetivo principal es organizar el cálculo de la preparación de la misión siguiendo diferentes pasos que permitirán enviar un plan detallado a cada UxV a través del GCS. Este apartado permite al usuario definir el contexto de la misión definiendo:

- Amenazas (fuente, objetivos, velocidad, rumbo)
- Diferentes tipos de áreas (ciegas, imposibles, prohibidas)
- Brechas (área donde el UxV tiene que realizar un reconocimiento)

Esta implementación se basa en llamadas asíncronas que permiten que esta tarea procese varias misiones al mismo tiempo (escalabilidad). Uno de los principales objetivos es la capacidad de construir una misión con muchos UxV.

Detrás del proceso del flujo de trabajo entre todas las tareas, se implementa una interfaz de usuario para definir el contexto de la misión.

A continuación se mostrará el proceso cómo el usuario puede definir las amenazas para la misión. Dentro del cual será posible definir:

- Cuadrados rojos que representan el origen de la amenaza (uno o muchos para cada amenaza)
- Triángulos rojos que representan el objetivo de la amenaza (destino final) (uno o muchos para cada amenaza)
- Velocidad que define la velocidad de la amenaza (metros/segundo)
- Rumbo que define la dirección de la amenaza (grados)

El color de las amenazas puede ser modificado por el usuario.

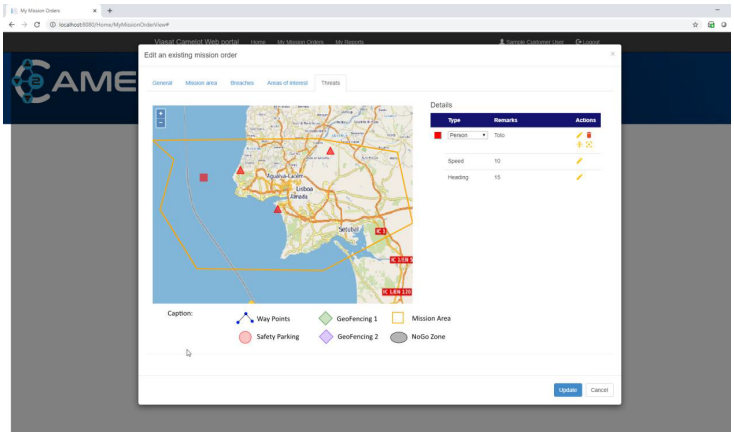

Figura 4.11: Interfaz de usuario para definir amenazas.

Esta interfaz de usuario describe cómo definir las diferentes áreas de la misión. Cada polígono define un área, los usuarios clasifican estas áreas seleccionando un valor en el selector (Prohibido, Ciego, Imposible).

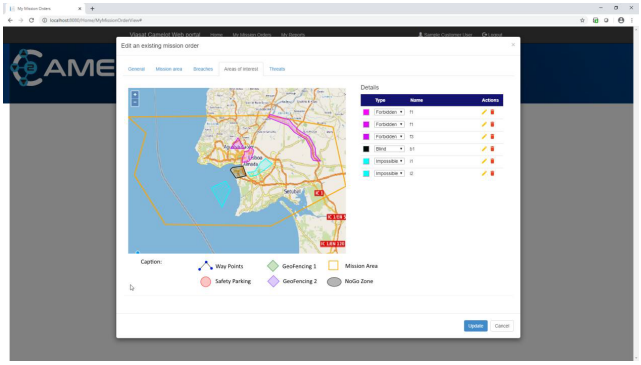

Figura 4.12: Interfaz de usuario para definir áreas de la misión.

De este modo, los usuarios podrán dibujar polígonos que representan las diferentes áreas a inspeccionar, básicamente serán las brechas de actuación. Los usuarios pueden definir tantas zonas como deseen. En esta etapa, cada área no está asignada a un UxV. Cada área tiene su propia observación, que ayudará a los usuarios a reconocer e identificar cada una de ellas. De hecho, para ayudar a los usuarios a definir estas áreas, esta interfaz también puede mostrar *SystemTracks*. Y finalmente, la pestaña área de misión será la encargada de resumir toda la información en una pantalla. La información previa definida por el usuario se muestra en esta caja de diálogo. En esta interfaz, los usuarios pueden crear/actualizar toda el área de la misión y permite al servicio descubrir activos que pueden estar involucrados. En la Figura 4.13, los activos (UxV y sensor heredado) se muestran con varios iconos.

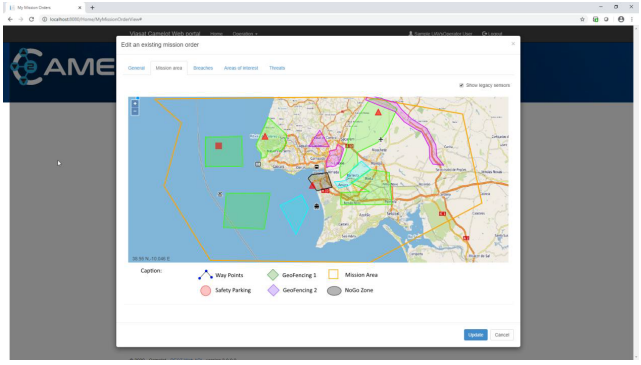

Figura 4.13: Interfaz de usuario para la creación/actualización del área de la misión.

La Figura 4.14 muestra el cálculo de la lista de acciones (alto nivel) después del cálculo del plan de optimización. En la Figura 4.14, el usuario puede ver la lista de UxV involucrados en esta misión (después del cálculo). Esta es la información más relevante que proviene de este módulo.

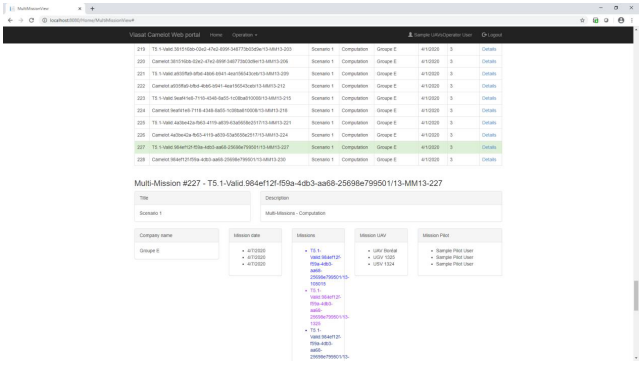

Figura 4.14: Visualización de UxV involucrados y sus trayectorias.

La lista de acciones está representada por una trayectoria:

- La acción de tránsito es básicamente una línea recta.
- La acción de reconocimiento es básicamente la lista de puntos del polígono.
- La acción de espera es solo un punto en la ubicación anterior (por eso a veces parece que se salta un número).

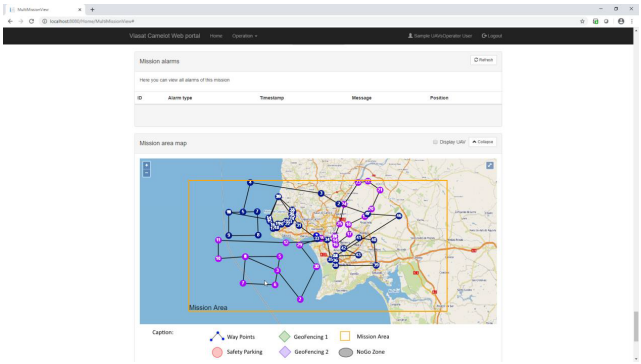

Figura 4.15: Representación de las acciones como trayectorias.

Después de la preparación de la misión, se procederá a su envío a los módulos de:

- Control Remoto de Sensores. Este módulo permite al usuario seguir un objetivo. Utiliza cámaras para seguir un objetivo.
- Replanificación de la misión. Esto calcula la deriva del estado y realiza una replanificación si es necesario.

También será el encargado de enviar el mensaje *MissionVehicle* a cada GCS, para darle las instrucciones pertinentes de la misión. A continuación se detallará como la GCS permite al piloto remoto controlar la cámara alojada en el Vehículo Terrestre. La GCS también nos permite validar todo el proceso de preparación de la misión como un proceso de principio a fin.

La Figura 4.16 muestra el mensaje *MissionVehicle* recibido por GCS, en el cual, el piloto puede ver la trayectoria detallada (con todos los puntos de referencia).

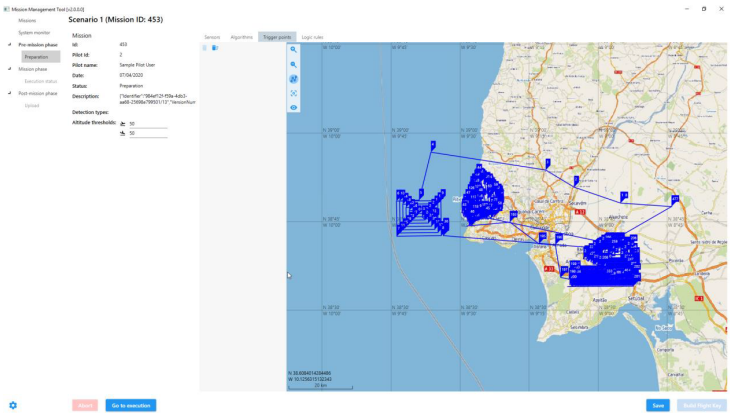

Figura 4.16: MissionVehicle recibido por la Estación de Control Terrestre.

Replanteamiento de la misión

El objetivo principal es detectar una desviación entre los vehículos disponibles y la misión actual. Un desvío puede ser detectado por la indisponibilidad de un sensor o una posición incorrecta del vehículo. Una vez detectado el desvío, este módulo proporciona información a otros servicios para poder corregirlo. Para poder detectar las desviaciones se realizarán consultas sobre el estado del vehículo que vendrán implícitas dentro del mensaje *AssetState*, el cual servirá de referencia para estimar el posible desvío.

Una vez que se recibe una misión válida, se inicializa el módulo. Para verificar si una misión es válida, hay dos vías:

- Validar que no se conoce ninguna misión
- La versión de la misión recibida es superior a la misión conocida

En ese momento, la misión se guarda y se procede a verificar la posición inicial de cada vehículo. Cada segundo se consulta los *AssetStates*, que nos informarán del estado del dron. Luego, un algoritmo llamado *computeStateDrift* verificará si hay un desvío.

Para entender mejor cómo funciona el mensaje *computeStateDrift*:

Se realiza una prueba sobre la disponibilidad de cada vehículo necesario para la misión. Posteriormente, se verifica el estado de disponibilidad de cada *AssetState* correspondiente. Si un vehículo está disponible, se verifican específicamente los sensores, en caso de ser necesarios para la misión actual. Si la posición y cada sensor de un vehículo están operativos, se realiza una verificación sobre su posición. Se crea un área de misión para cada vehículo a partir de la información incluida en el objeto de la misión. Combinando la información contenida en el objeto de la misión con las posiciones iniciales de cada vehículo, se crean áreas punto por punto. Si un vehículo está fuera de su área de misión, se detecta automáticamente un desvío.

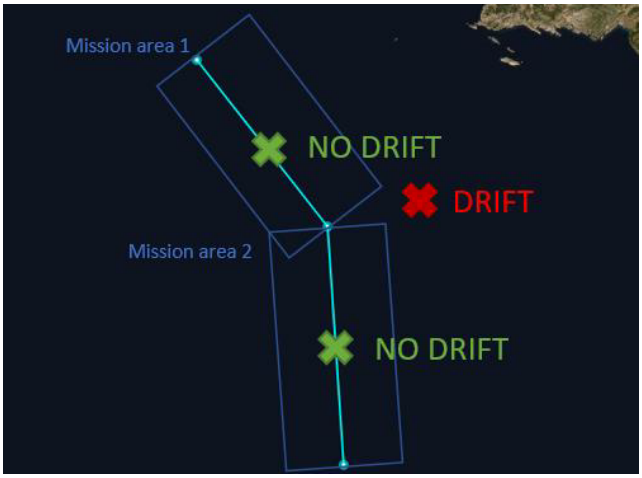

Figura 4.17: Detección de desvío y áreas de misión de los vehículos.

Durante estos pasos de cálculo, se guardan varios elementos:

- La lista de *Identificator* (ID) de vehículos no disponibles
- La lista de sensores no disponibles por ID de vehículo
- La lista de acciones a reprogramar con sus eventuales dependencias de sensores

4.3.2. Servicios de asignación y control automático de activos (AATC)

Asignador de disponibilidad de recursos

Dentro del sistema, CAMELOT tiene un rol vital en construir, actualizar y compartir información acerca de todos los activos disponibles. Esta función es crucial para mantener una base de datos actualizada que se centra únicamente en las características de los activos.

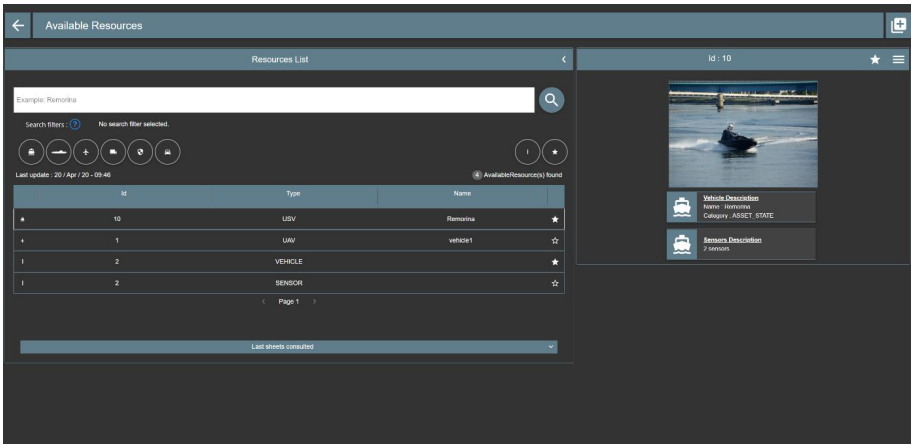

Figura 4.18: Módulo de recursos disponibles

Actualizaciones Dinámicas:

La base de datos se actualiza dinámicamente para reflejar cualquier nueva incorporación, como un nuevo sensor mencionado en un mensaje *AssetState*, garantizando así que la información de los activos esté siempre al día.

Tareas y control de UxV

Esta sección se divide en dos modos distintos de operativa: uno para la estimación rápida de costes dentro de un bucle de optimización y otro para el cálculo de trayectorias más detallado dentro de un bucle de refinamiento.

Modo 1: Estimación Rápida de Costes. El Modo 1 funciona como un módulo de servicio para calcular los costes asociados a acciones específicas. Este servicio, utilizado durante la etapa de preparación de la misión, está diseñado para asignar tareas a cualquier tipo de UxV. Los insumos incluyen ubicación inicial, ubicación final, plan, contexto y mensajes meteorológicos. El resultado es un plan con los costes asociados. Este módulo, parte integral de un bucle de optimización, se caracteriza por su rapidez y enfoque general.

Figura 4.19: Esquema de Entradas/Salidas en Modo 1

Modo 2: Cálculo Detallado de Trayectorias. Por otro lado, el Modo 2 se utiliza para obtener la trayectoria después de asignar una tarea al UxV en una misión de alto nivel. Además de los insumos del Modo 1, este modo incluye un par adicional de entrada/salida (mensajes de configuración de sensores y solicitud de configuración de sensores) para seleccionar el mejor sensor para una acción en el plan. Este módulo se activa una vez finalizada la optimización de la misión y se centra en la precisión, aunque puede ser más lento en términos de tiempo de procesamiento.

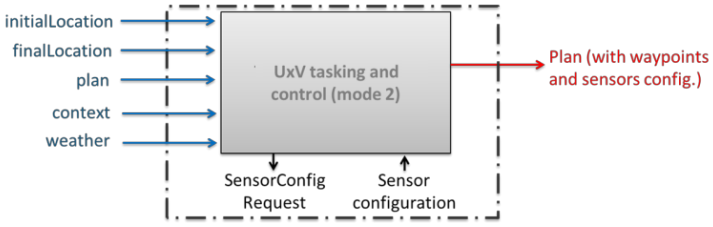

Figura 4.20: Esquema de Entradas/Salidas en Modo 2

Detalles de la Implementación

La implementación incluye cuatro componentes principales y alguno auxiliar:

- Interfaces con el protocolo CAMELOT.
- Manejo del formato de mensajes CAMELOT.
- Algoritmo de escaneo.
- Algoritmo de seguimiento de objetivos.
- Modos de demostración y pruebas.

Algoritmo de Planificación de Trayectorias

El algoritmo básico para el escaneo busca un equilibrio entre una cobertura óptima y una robustez suficiente. Los resultados demuestran que este equilibrio se logra con una división adecuada del área a cubrir, seguido de un algoritmo de escaneo ad-hoc.

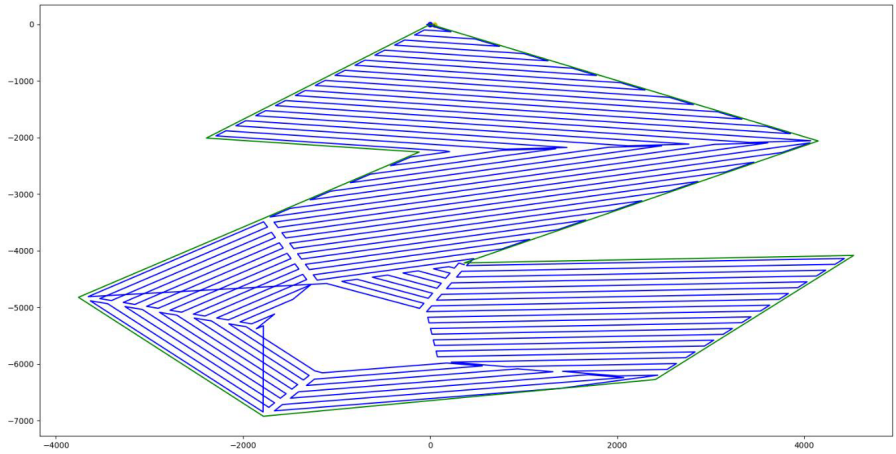

Figura 4.21: Implementación del Algoritmo de Escaneo

Algoritmo de Asignación de Objetivos

Este algoritmo se basa en la reducción de costes seguida de una ley de orientación para estimar con precisión el momento de intercepción. La adecuación

con las capacidades propias del UxV es crucial, ya que tanto las capacidades de la carga útil como las del vehículo influyen significativamente en la trayectoria final.

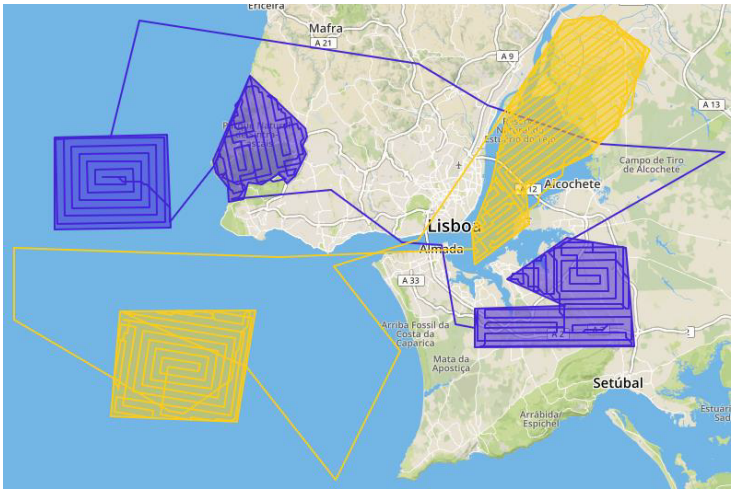

Figura 4.22: Ejemplo del resultado del algoritmo de asignación

Gestión automática de sensores

Este módulo tiene como objetivo encontrar el mejor sensor para una acción planificada. El módulo calcula la elección del mejor sensor, pero el control de un sensor real se realiza por la GCS correspondiente. Los insumos de este servicio son los mensajes *SensorConfigRequest*, información meteorológica y datos relacionados con los activos y sensores (mensajes *AssetState* y *AssetLinkedInfo*). La salida es el mensaje *SensorConfiguration*.

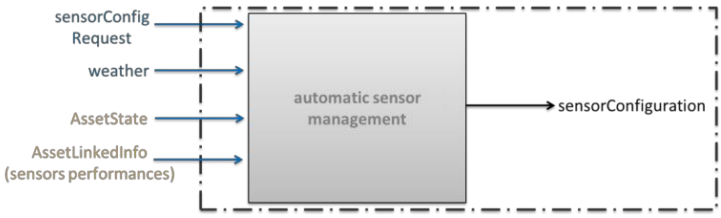

Figura 4.23: Entradas/Salidas del Módulo de Selección de Sensores

Detalles de la Implementación

Para responder lo más rápido posible, este módulo mantiene una lista actualizada de activos disponibles y sus sensores integrados. Esto se realiza enviando periódicamente un mensaje *AssetStateRequest* y analizando la respuesta (mensaje *AssetStateResponse*), que contiene:

- La lista de todos los activos disponibles.
- Para cada activo, la lista de sensores integrados con información adicional:
  - El tipo de sensor (radar, cámara, etc.).
  - El estado del sensor (disponible/no disponible, activo/inactivo, etc.).

Para cada sensor, el módulo mantiene información sobre su rendimiento, enviando periódicamente un mensaje *AssetLinkedInfoRequest* para cada sensor y extrayendo la información del rendimiento de la respuesta.

Cuando se recibe un mensaje *SensorConfigRequest*, se realizan las siguientes verificaciones:

- El activo está presente en la lista interna de activos disponibles.
- El activo tiene sensores integrados.
- Al menos un sensor está disponible.
- La información de rendimiento del sensor está presente.

Si estas verificaciones fallan, el módulo envía un mensaje *SensorConfiguration* con un estado de fallo y la razón del mismo.

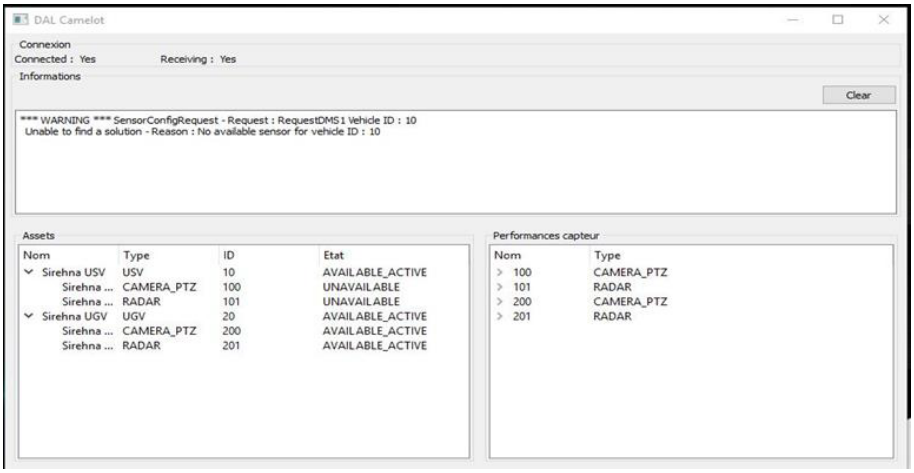

Figura 4.24: Ejemplo de Respuesta Negativa

Si las verificaciones son exitosas, el módulo elige el mejor sensor para cumplir con la misión.

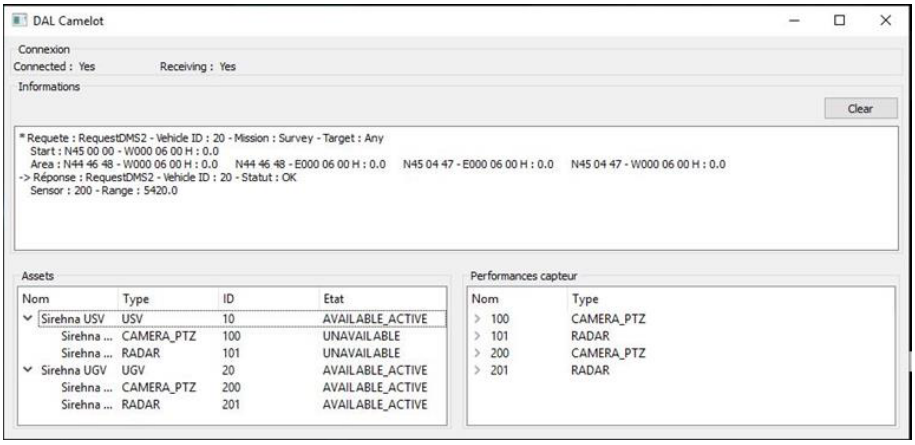

Figura 4.25: Ejemplo de Respuesta Positiva

Es importante destacar que, por el momento, la información meteorológica no se utiliza. Esto es una provisión en caso de cámaras ópticas integradas, ya que las condiciones meteorológicas (lluvia, niebla...) pueden influir en el rendimiento

de ese tipo de sensor. Suponemos que las condiciones meteorológicas son lo suficientemente buenas y no degradan el rendimiento de la cámara.

Tareas y control de sensores

Este módulo es un servicio utilizado para establecer el control remoto de sensores durante la ejecución de la misión. Este control de sensores puede realizarse según el plan establecido o de manera asincrónica por un operador. A continuación, se muestra en la Figura 4.26 las entradas y salidas de este servicio.

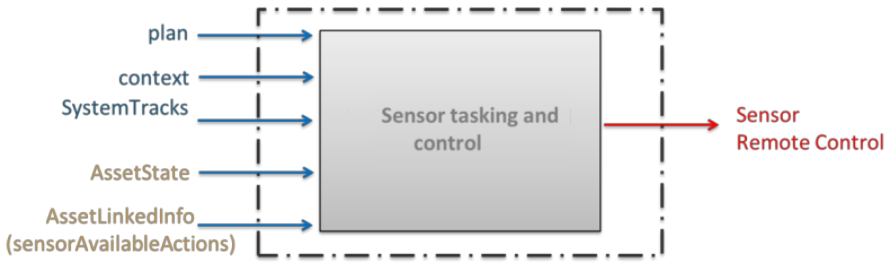

Figura 4.26: Entradas y Salidas del Control Remoto de Sensores

Como se puede observar, las entradas al servicio son los mensajes *plan*, *context*, *SystemTrack*, *SystemTrackDrop* e información relacionada con los activos y sensores (mensajes *AssetState* y *AssetLinkedInfo*). La salida es un mensaje *SensorRemoteControl* enviado a la GCS para que ejecute las acciones correspondientes.

Detalles de la Implementación

Este módulo se desarrolla y diseña para estar siempre disponible en el sistema desde la preparación de la misión hasta su ejecución. Cada cálculo automático de comandos remotos de sensores se realiza como un hilo separado en este servicio.

Como se describe en la arquitectura general, este servicio se lleva a cabo en el módulo AATC. Para complementar el servicio se desarrollan nuevas funcionalidades en su estación terrestre para poder recibir comandos remotos procedentes del C2, aunque, en cualquier caso, el piloto es responsable de acceder a su propio UxV.

La Figura 4.27 muestra la recepción de un mensaje *SensorRemoteControl* en la estación terrestre, donde el piloto remoto tiene tres opciones:

- Rechazar: el piloto remoto rechaza el comando, y este se elimina de la lista.
- Aceptar: el piloto remoto acepta el comando y debe ejecutarlo con las capacidades propias de la GCS.
- Ejecutar: el comando es conocido por la GCS y se ejecutará automáticamente.

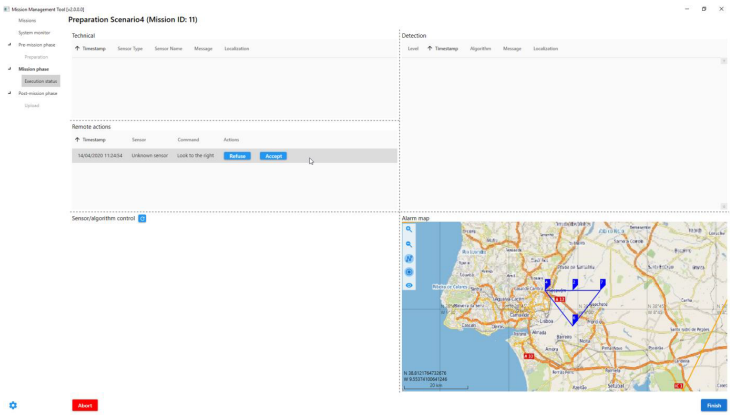

Figura 4.27: Recepción de Comandos SensorRemoteControl

Funcionalidad de Designación de Objetivos

Esta funcionalidad recibe una solicitud para seguir un objetivo. Un objetivo en CAMELOT se define básicamente como un mensaje *SystemTrack* (que contiene una ubicación). Al recibir una solicitud *TargetDesignationRequest*, el módulo calcula los valores de paneo, inclinación y distancia desde el sensor hasta el objetivo y envía el primer comando *SensorRemoteControl* a la GCS para mirar hacia el objetivo.

Para calcular los nuevos valores de *SensorRemoteControl*:

- Se suscribe al *SystemTrack* designado.
- Solicita *AssetState* para conocer la nueva ubicación del UxV involucrado.

Cuando se conocen nuevos datos, el módulo calcula y envía un nuevo *SensorRemoteControl* a la GCS asociada.

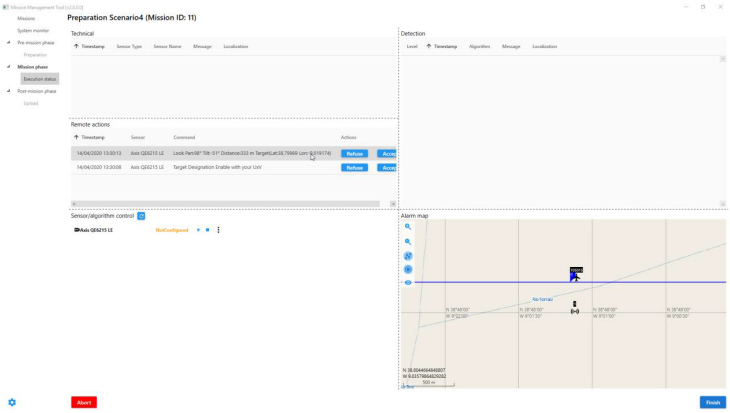

Figura 4.28: Recepción de Mensajes SensorRemoteControl para Designación de Objetivos

El seguimiento de un objetivo continúa hasta que se recibe un *SystemTrackDrop* o una *TargetDesignationRequest* (deshabilitada). El módulo detiene su proceso interno de cálculo y cancela su suscripción a la información de *SystemTrack* y *AssetState*.

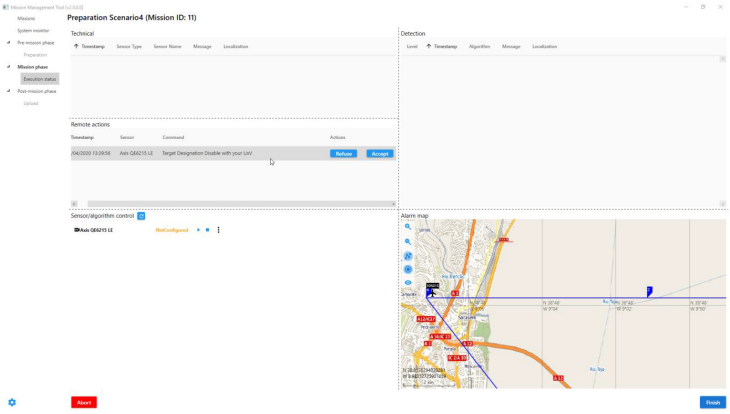

Figura 4.29: Información al Piloto Remoto sobre la Finalización de la Misión

Multitarea de plataformas

Este módulo es un servicio utilizado para calcular un nuevo plan cuando se detecta una desviación durante la ejecución de la misión. A continuación, se muestra un esquema de las entradas y salidas de este servicio.

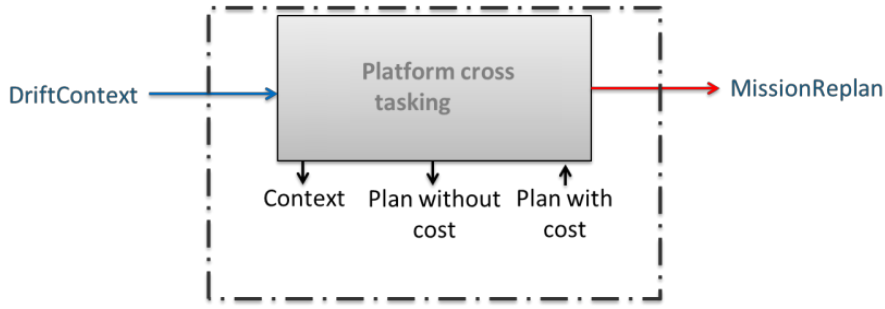

Figura 4.30: Entradas y Salidas de la Replanificación de Misiones

Como ya existe una misión inicial, este servicio calcula o repara esta misión existente. Las entradas de este módulo son los mensajes *mision*, *AssetState* y alguna información sobre el fallo de la misión, todo empaquetado en un objeto llamado *DriftContext*. La salida es un mensaje *MissionReplan*. Durante el proceso de optimización, esta tarea necesita obtener costes asociados a acciones, por lo que hay una entrada/salida adicional (Plan, Contexto).

Detalles de la Implementación

El servicio tiene como objetivo reprogramar una misión con vehículos disponibles, para ello se informará a través del canal de *Remote Procedure Call* (RPC) RabbitMQ para comunicar servicios estrechamente vinculados. La función que inicia el cálculo del mensaje *MissionReplan* es *driftDetected*. El cual contiene varios atributos de especial interés:

- La misión actual.
- La última lista de *AssetState*.
- La lista de vehículos que no están disponibles.
- La lista de sensores no disponibles por vehículos.
- La lista de acciones a reprogramar asociadas con sus restricciones específicas, como un requisito de sensor.

Para la implementación, se envía el mensaje *context* para iniciar el canal de comunicación. Se realiza un cálculo para determinar qué vehículos son compatibles con cada uno de los lugares específicos que necesitan ser reprogramados a través de la función *getCompatibleAssetStatesBySensorId*. Cada vehículo se instancia como un *CamelotVehicule* y cada tarea como una *TacheImpl*.

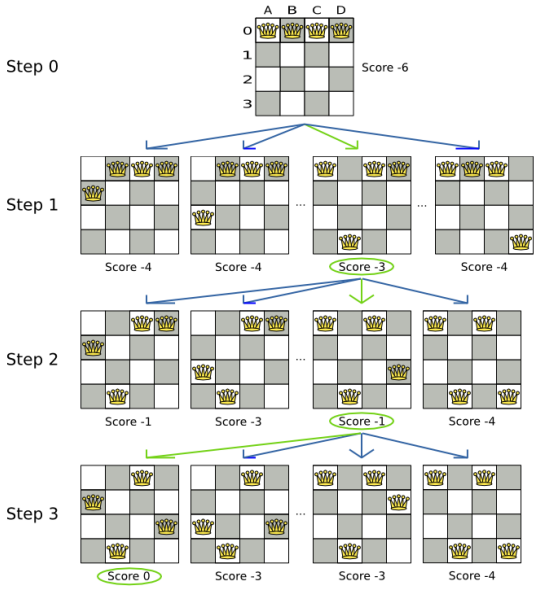

Figura 4.31: Aplicación de Búsqueda Local para la Replanificación

El algoritmo utilizado para construir un nuevo plan se basa en un *Team orientation problem* (TOP).

El *Orientation problem* (OP) es una combinación de selección de nodos y determinación del camino más corto entre los nodos seleccionados. El objetivo es maximizar el puntaje total recolectado de los nodos visitados. Por lo tanto, el OP se puede ver como una combinación entre dos problemas combinatorios clásicos, el problema de la mochila y el problema del viajante.

El modelo TOP y el algoritmo de optimización de búsqueda local anterior permiten construir un nuevo plan óptimo basado en el anterior. Este algoritmo consultará para aprender sobre los costos de cada tarea para cada vehículo y determinará una reprogramación de alto nivel. Se llama a un método para recuperar el resultado del algoritmo y construir el mensaje MissionReplan. Las acciones se establecen directamente y el número de versión de la misión se incrementa.

Finalmente, el resultado se envía por un evento responsable de probar la integridad del mensaje y luego enviarlo.

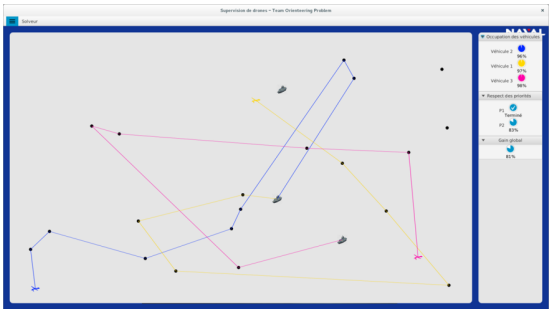

Figura 4.32: Resultado de la Replanificación de la Misión

4.3.3. Servicios relacionados con sensores

El objetivo principal es identificar y aplicar métodos innovadores para proporcionar ayuda automatizada a los operadores de vigilancia fronteriza. Esto se logra mejorando el procesamiento y análisis de datos provenientes de múltiples sensores, así como la detección de comportamientos sospechosos en múltiples objetivos. La consecución de este objetivo se realiza a través del desarrollo de los siguientes módulos:

- **Correlación AIS/Radar/Vídeo:** Este módulo se enfoca en la integración y análisis combinado de datos provenientes de *Automatic Identification System* (AIS) [101], radares y cámaras de vídeo para una vigilancia más efectiva y precisa.
- **Correlación de Sensores CBRN:** Desarrollo de un sistema de correlación para sensores de *Chemical, Biological, Radiological And Nuclear risks* (CBRN), mejorando la capacidad de detección y respuesta ante amenazas de esta naturaleza.
- **UUV acústica LBS:** Implementación de un sistema de *Sound based in Location* (LBS) para *Unmanned Underwater Vehicles* (UUV) [102], mejorando la capacidad de rastreo y análisis en entornos subacuáticos.
- **Detección Automática de Objetivos en Vídeo de Movimiento Completo:** Desarrollo de un módulo para la identificación automática y en tiempo real de objetivos en vídeos de movimiento completo, aumentando la eficiencia en la vigilancia y seguimiento de actividades sospechosas.

- **Identificación Automática (Clasificación) en Información de Vídeo:** Este módulo se dedica a la clasificación y reconocimiento automático de objetos o personas en la información de vídeo, lo cual es esencial para la identificación rápida de posibles amenazas o situaciones irregulares.
- **Detección de Comportamientos Sospechosos:** Focalizado en el análisis avanzado de patrones de comportamiento para identificar actividades potencialmente sospechosas o irregulares, crucial para la prevención y respuesta rápida ante incidentes de seguridad.

Cada uno de estos módulos representa un paso adelante en la tecnología de vigilancia fronteriza, ofreciendo a los operadores herramientas más eficaces y sofisticadas para mantener la seguridad y responder de manera efectiva ante cualquier amenaza o irregularidad detectada.

Correlación de video/radar/AIS

El servicio presentado en esta sección tiene como objetivo crear una imagen situacional detallada y precisa mediante la fusión de datos de múltiples sensores. La Figura 4.33 incluye seguimientos de sistema de alto nivel que representan posiciones, direcciones, velocidades de objetos, entre otros.

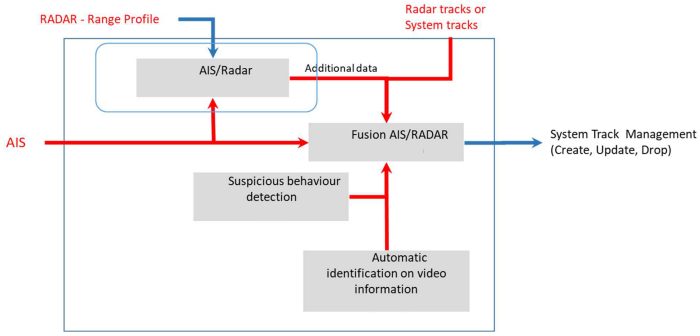

Figura 4.33: Parte Detallada de la Arquitectura Funcional Global

Proceso de Fusión de Datos

La fusión de datos se realiza utilizando información de sensores heterogéneos, como radar, AIS y vídeo, provenientes de diferentes plataformas. Estos datos se combinan para construir una representación única de la situación.

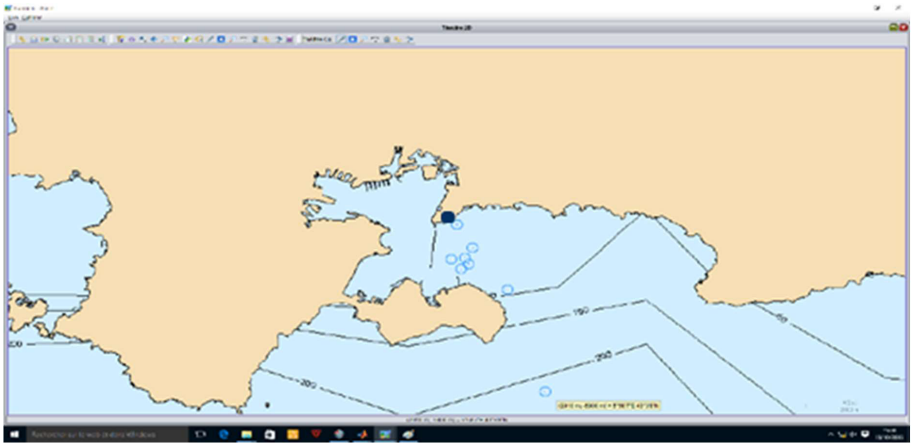

Figura 4.34: Ejemplo de Imagen Situacional Cerca de Toulon, Francia

Método de Medición Automatizada y Correlación con AIS

Se implementa un método para medir la longitud de un barco a partir de la señal de perfil de alcance del radar. Esta medida se compara con la información transmitida por el AIS para verificar la coherencia de los datos.

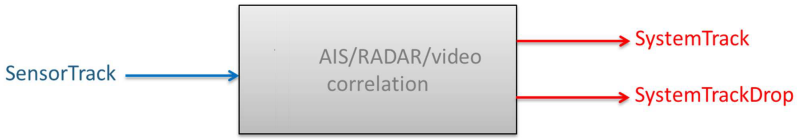

Figura 4.35: Entradas y Salidas del Proceso de Fusión de Datos

Arquitecturas y Algoritmos de Fusión

Se utiliza una arquitectura orientada a la fusión de seguimientos. Los seguimientos de sensores locales se correlacionan y fusionan para producir seguimientos de sistema finales.

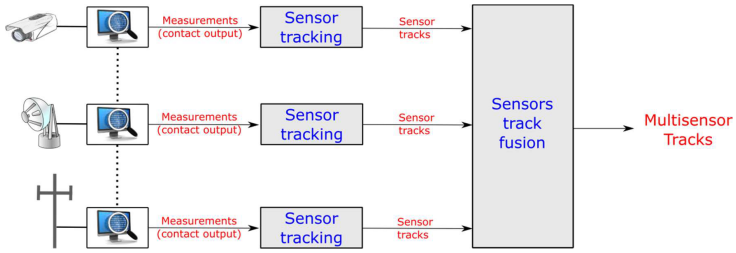

Figura 4.36: Arquitectura del Servicio de Fusión de Datos

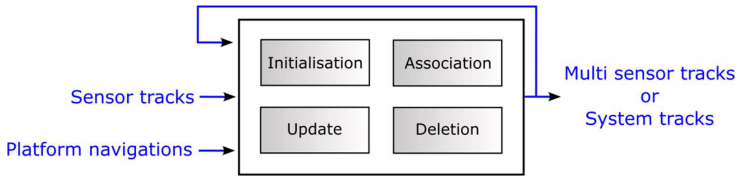

Figura 4.37: Módulos Principales del Servicio de Fusión

Correlación Radar AIS y Generación de Alertas

La correlación del perfil de alcance del radar con AIS es un componente esencial del servicio, ya que permite comparar las longitudes medidas por radar con las reportadas por el AIS y se generan alertas en caso de discrepancias significativas.

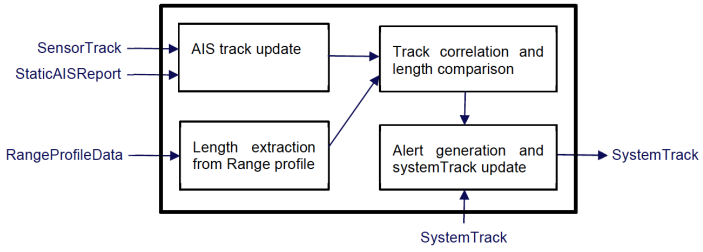

Figura 4.38: Correlación del Perfil de Alcance del Radar con AIS

Por su lado, el módulo de extracción de longitud juega un papel fundamental en la determinación de la longitud de los barcos a partir de perfiles de alcance radar. Esta técnica mide la potencia reflejada de los puntos más destacados del

objetivo, que varía según el ángulo de incidencia del radar y las condiciones del mar.

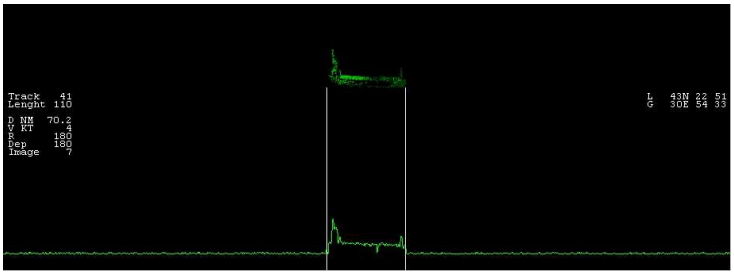

Figura 4.39: Simulación del Perfil de Alcance de un Barco y Generación de Alertas

Este servicio representa un avance significativo en la capacidad de fusionar y analizar datos de múltiples sensores, mejorando la vigilancia y el monitoreo en entornos complejos y dinámicos. La integración efectiva de estas tecnologías avanzadas mejora la conciencia situacional y facilita la toma de decisiones rápida y precisa.

La comparación de la longitud del barco obtenida del radar con la información proporcionada por el AIS es esencial para identificar discrepancias. Si los datos no coinciden, se genera una alerta. Este proceso de verificación es vital para asegurar la precisión de la información y para detectar posibles irregularidades o amenazas.

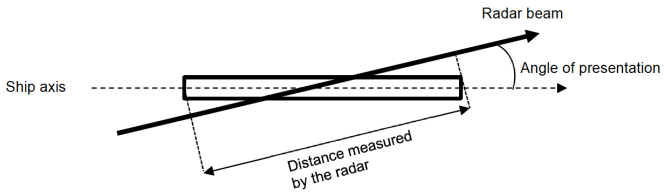

Figura 4.40: Proceso de Correlación y Verificación de Datos entre Radar y AIS

La fusión de datos de sensores y la detección de comportamientos en el sistema CAMELOT representan una innovación significativa en la vigilancia fronteriza. Estas técnicas no solo aumentan la precisión en la identificación y

seguimiento de objetivos, sino que también mejoran la capacidad de respuesta ante situaciones anómalas o sospechosas.

Correlación del sensor CBRN

El objetivo es desarrollar un componente dedicado a la fusión de datos para su uso en escenarios CBRN dentro del sistema CAMELOT. Este proceso implica la recopilación y procesamiento de datos de posicionamiento y lecturas de sensores para su uso posterior en el sistema.

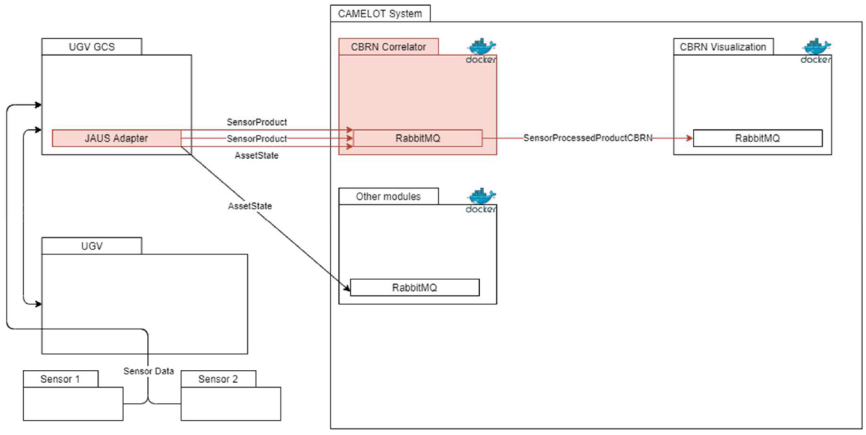

Figura 4.41: Fusión de Datos en Escenarios CBRN

Modelo de Datos y Correlación de Sensores CBRN

En el módulo de correlación de sensores CBRN, las entidades de datos relevantes del middleware de CAMELOT son:

- *AssetState* (consumir)
- *SensorProduct* (consumir)
- *SensorProcessedProductCBRN* (producir)

El adaptador *JAUS*, otra parte crucial, será el encargado de interactuar con las siguientes entidades de datos del middleware de CAMELOT:

- *AssetState* (producir)

- *AssetLinkedInfo*: Vehículo (producir)
- *AssetLinkedInfo*: Sensor (producir)
- *SensorProduct* (producir)
- *MissionVehicle* (consumir)
- *SensorRemoteControl* (consumir)

Desarrollo de Módulos de Software

Los módulos de software desarrollados son:

- Módulo de correlación de sensores CBRN
- Adaptador *JAUS*

El adaptador *JAUS* forma parte de la capa de adaptación de CAMELOT y su función principal es traducir los mensajes relevantes de *JAUS* a mensajes del middleware de CAMELOT y viceversa. Proporciona una capa de abstracción entre el modelo de CAMELOT y el modelo de vehículo de *JAUS*. Este adaptador funcionará en la GCS del *Unmanned ground vehicle* (UGV). Dado que en el entorno del sistema CAMELOT, el UGV es el único proveedor de lecturas de sensores CBRN, el adaptador *JAUS* se convierte en el único productor de datos de entrada para el módulo de correlación de sensores CBRN.

El módulo de correlación de sensores CBRN, por su parte, forma parte del sistema CAMELOT como una imagen Docker que se ejecuta en el servidor. Su funcionalidad principal es procesar datos en bruto para análisis posteriores o la creación de visualizaciones.

Procesamiento de Datos y Visualización

El procesamiento de datos en el módulo de correlación de sensores CBRN generalmente implica tomar cada tipo de dato medible y extraer el valor real, calculando el error de medición relativo. Esto incluye considerar la frecuencia con la que se necesitan los datos procesados y la frecuencia con la que el módulo recibe lecturas de sensores.

Este módulo no es responsable del procesamiento de mensajes sobre la configuración, calibración y mantenimiento de parámetros operativos para los sensores CBRN o plataformas conectadas. Sin embargo, juega un papel importante en el funcionamiento del sistema CAMELOT, ya que los datos procesados por este módulo son consumidos por el módulo de visualización, que crea capas con

datos CBRN para su visualización en interfaces orientadas al usuario, como VR o HMI.

En definitiva, el desarrollo de componentes para la fusión de datos en escenarios CBRN en CAMELOT representa un avance significativo en la capacidad de gestionar y analizar datos en situaciones de alta complejidad y riesgo. Este enfoque integrado no solo mejora la capacidad de respuesta ante incidentes CBRN, sino que también facilita la toma de decisiones informadas y la visualización efectiva de datos críticos.

UUV acústica LBS

En el contexto de los sistemas de C2 multidominio, el ámbito submarino presenta desafíos únicos, particularmente en términos de comunicaciones. La limitación principal reside en el ancho de banda comunicativo actual, que resulta insuficiente para soportar la carga de un modelo de datos avanzado y el correspondiente exceso de datos que esto implica [103]. Esta situación conlleva la necesidad de soluciones innovadoras, como la utilización de activos de superficie, que actúan como puertas de enlace entre la comunicación acústica submarina y la comunicación de *Radiofrequency* (RF) aérea.

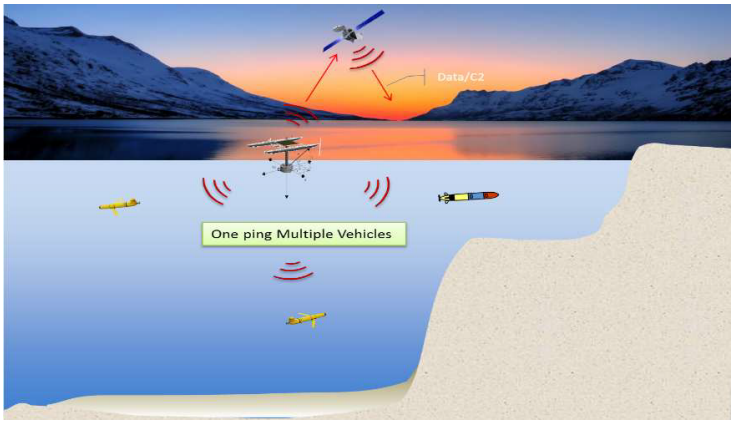

Figura 4.42: Comunicación y localización acústica submarina

En el ámbito de la localización submarina, se utiliza predominantemente la tecnología acústica. Existe una variedad de sistemas y productos de localización acústica en el mercado actual, algunos de los cuales combinan las capacidades de comunicación con las de localización. Estos sistemas suelen depender de un nodo interrogador que se comunica con cada participante de manera secuencial,

lo que puede generar ineficiencias, especialmente en escenarios con múltiples participantes. Alternativamente, se emplean múltiples balizas, aunque esto introduce complejidades adicionales en términos de logística y precisión de despliegue.

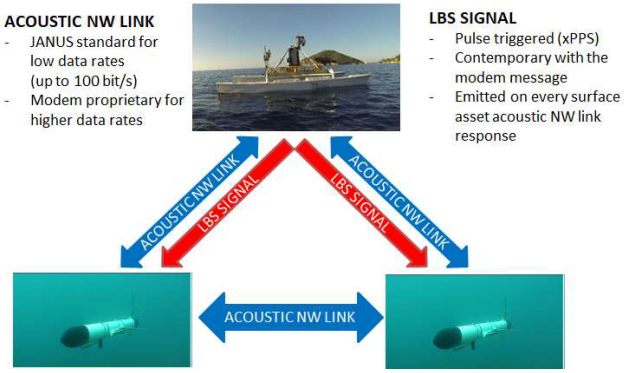

Figura 4.43: Sistema de localización con múltiples vehículos submarinos

Modelo de Datos y Plataforma Móvil de Superficie

El enfoque innovador de integrar la plataforma móvil de superficie que alberga el transpondedor LBS en el sistema C2 CAMELOT, con un adaptador para la interfaz *JAUS*, es un avance significativo. Esta integración proporciona una solución eficiente para la localización de activos submarinos, superando las limitaciones de ancho de banda y ofreciendo un método de comunicación más robusto y adaptable.

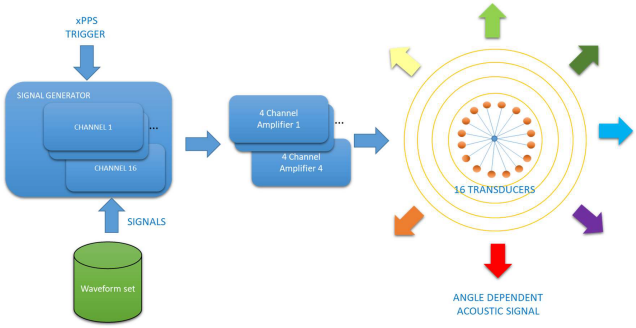

Figura 4.44: Integración del transpondedor LBS en la plataforma móvil de superficie

La creciente utilización de AUV en aplicaciones comerciales, militares y científicas subraya la necesidad de sistemas de navegación y posicionamiento submarinos precisos y fiables. A pesar de la diversidad de tecnologías aplicables, la localización acústica sigue siendo un enfoque central y robusto para la navegación submarina, ofreciendo una combinación única de precisión y confiabilidad en entornos desafiantes.

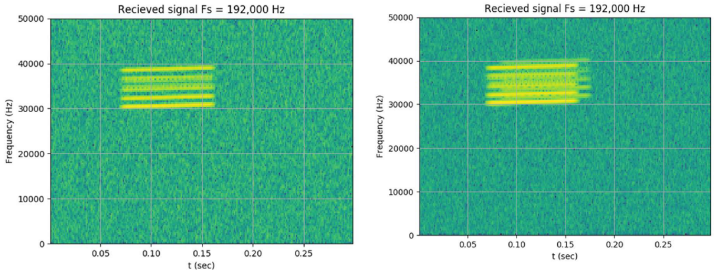

Figura 4.45: Herramientas acústicas para navegación submarina

El sistema de localización LBS representa un avance significativo en la localización submarina. Proporciona capacidades de localización a un conjunto ilimitado de vehículos submarinos mediante la emisión de un único pulso de localización que es recibido por todos los sistemas no tripulados submarinos en el rango operativo. Este enfoque innovador permite superar los desafíos logísticos y de precisión asociados con los sistemas de localización acústica tradicionales, abriendo nuevas posibilidades para operaciones submarinas complejas y en gran escala.

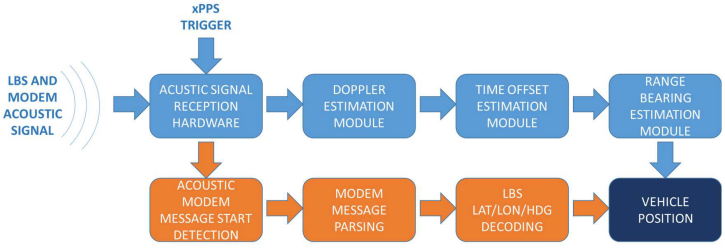

Figura 4.46: Sistema CAMELOT LBS

Detección automática de objetivos en vídeo a cámara completa

El flujo óptico es la capacidad de determinar el vector de movimiento de un píxel entre dos imágenes de la misma escena, es decir, dos fotogramas consecutivos en un flujo de video. Se utiliza ampliamente en el campo del vídeo para rastrear objetos, determinar la matriz de transición entre las dos imágenes, segmentar regiones o determinar la profundidad en la visión estéreo. Los algoritmos para resolver el flujo óptico son variados y siguen siendo un área activa de investigación [104]. Conociendo el desplazamiento de los píxeles, es interesante tener marcadores en las imágenes. Con estos, es posible realizar un análisis para determinar el movimiento de los objetos en relación con otros.

Este módulo conduce a la implementación de un algoritmo basado en varios enfoques para realizar la detección y el seguimiento de objetivos en movimiento en grabaciones de video o directamente desde una tasa de flujo en tiempo real. El objetivo es detectar objetivos con un tamaño de 5x5 píxeles manteniendo las restricciones de tiempo real. El formato de video puede ser un video normalizado (JP2000, H264, *Moving Picture Experts Group* (MPEG4), etc.) o un formato formalizado por la *Organización del Tratado del Atlántico Norte* (OTAN) [105] como el STANAG 4609 [106] dedicado al video en movimiento.

4.3.4. Modelo de Datos

. La siguiente Figura 4.47 describe las entradas y salidas producidas por el servicio:

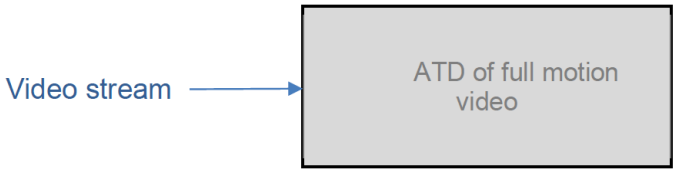

Figura 4.47: Entradas y Salidas del Proceso de Detección

Como se describió anteriormente, el formato de video es un formato normalizado o formalizado por la OTAN. Este servicio no produce ningún mensaje de salida. Los objetivos detectados se muestran en una HMI como una superposición de las imágenes de video.

Etapas en la Detección de Objetivos Móviles

La Figura 4.48 detalla las diferentes etapas involucradas en la detección de objetos en movimiento en un flujo de video:

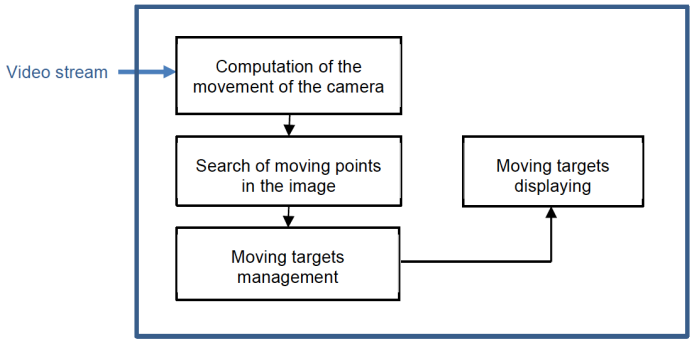

Figura 4.48: Etapas de Detección de Objetivos Móviles

El objetivo principal es extraer activos en movimiento de un flujo de video. Esto se hace buscando píxeles que se mueven de un fotograma de video al siguiente. Sin embargo, este movimiento resulta tanto del movimiento del propio objetivo como del movimiento de la cámara.

Identificación automática (clasificación) a partir de información de vídeo

Este módulo tiene dos objetivos principales:

1. Detectar automáticamente la presencia de objetivos en el mar en un flujo de video, sabiendo que el entorno operativo es cambiante y el propio ambiente es móvil (olas y espuma).

2. Determinar automáticamente el tipo de objetivos detectados a partir de una base de datos de imágenes. El contexto del estudio es la vigilancia marítima, por lo que los posibles objetivos deben ser del siguiente tipo: fragata, portaaviones, buque de carga, etc.

La automatización de la detección y la identificación de objetivos conduce a una reducción del trabajo del operador.

Modelo de Datos

La Figura 4.49 describe las entradas y salidas para dicho servicio:

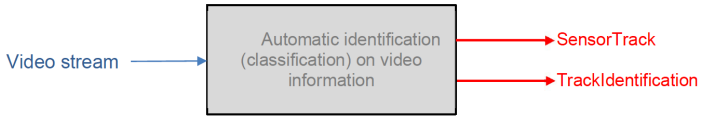

Figura 4.49: Entradas y Salidas del Proceso de Detección e Identificación

El formato del flujo de video debe ser un formato formalizado por la OTAN, como el STANAG 4609. De hecho, el algoritmo utilizado necesita información adicional disponible en ese tipo de formato de video.

Etapas en la Detección e Identificación de Objetivos

. La Figura 4.50 detalla las diferentes etapas involucradas en la detección e identificación de objetivos:

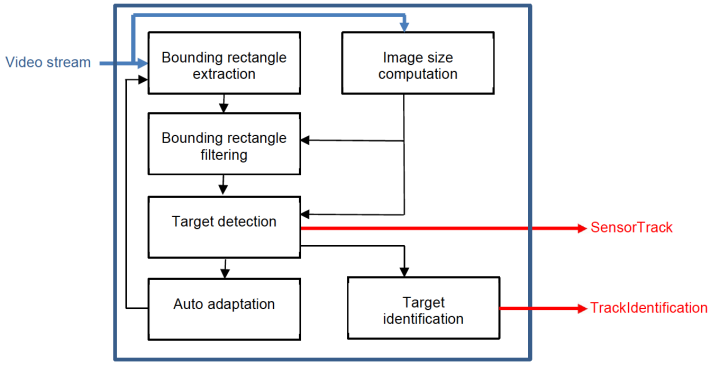

Figura 4.50: Etapas de Detección e Identificación de Objetivos

Para detectar un objetivo en el flujo de video, el servicio extrae los rectángulos que delimitan los objetos que aparecen en la imagen. Desafortunadamente, dependiendo del contexto (olas, reflejo del sol...), algunos rectángulos extraídos podrían generar falsas alarmas. Para evitar esto, se aplica un filtro para suprimir esos rectángulos no deseados en la imagen actual. Luego se aplica un

segundo filtro en imágenes sucesivas, que elimina los rectángulos transitorios que no habrían sido suprimidos por el primer filtro.

Detección de comportamientos sospechosos

El objetivo de este módulo es correlacionar las trayectorias proporcionadas a través del sistema CAMELOT con información contextual, con el fin de comprender las intenciones de un objetivo y generar alertas apropiadas. Teóricamente, la información se puede dividir en tres tipos:

- Controlada/medida: información basada en mediciones de sensores, como rastreos de radar o información extraída de vídeo.
- Declarativa: información obtenida directa o indirectamente de informes generados por los objetos presentes en la situación, típicamente rastreos AIS.
- Curada: información agregada en bases de datos confiables con cierta verificación humana, como bases de datos de registro de barcos.

Para caracterizar estos comportamientos, el sistema se basa en un conjunto de reglas y métricas que caracterizan la adecuación entre la información procesada y los patrones que definen los comportamientos sospechosos.

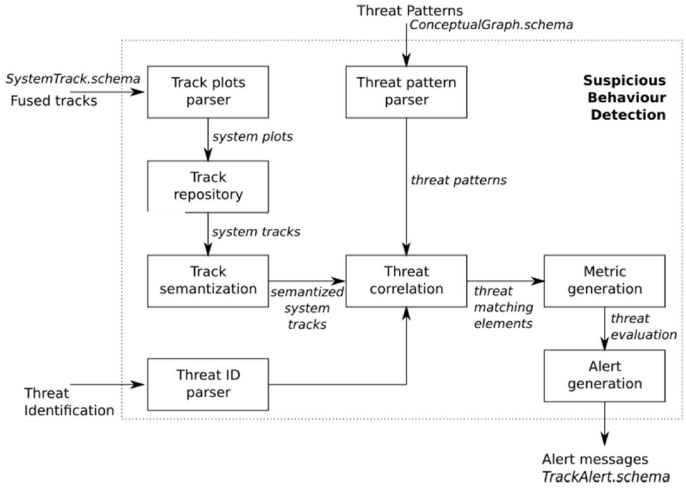

Figura 4.51: Procesamiento de Información y Generación de Alertas

Software y Submódulos

El software de este servicio consta de varios submódulos que realizan tareas de preprocesamiento, análisis algorítmico central y generación de alertas. Está integrado en el sistema y no está diseñado para la interacción del usuario.

El repositorio de trayectorias es un componente necesario para la detección de comportamientos anómalos, ya que otros servicios procesan la fusión de trayectorias de manera dinámica, mientras que este módulo necesita recordar el estado del conjunto completo de tramas para comprender la trayectoria completa de los objetos en movimiento. Este repositorio es principalmente una agregación de la información presente en los mensajes de *SystemTrack*, con simples controles de integridad.

La semantización de trayectorias se llama cada vez que se requiere un análisis de una trayectoria dada para la detección de comportamientos. Está diseñado como un servicio de semantización interno, transformando un vector de longitud/latitud anotado en una representación conceptual/relacional de la trayectoria.

Figura 4.52: Semantización y Análisis de Trayectorias

Los patrones de amenazas utilizados por este servicio se comunican directamente desde el módulo de fusión. Consisten en una descripción de los patrones típicos que un objetivo sospechoso seguiría si su intención es alcanzar un objetivo de manera rápida pero indetectable.

Finalmente, a partir de estas métricas, se crean (o descartan) alertas, y se transmiten al sistema CAMELOT con indicadores de alto nivel, como un nivel de confianza, un tiempo estimado de finalización y elementos geográficos a destacar.

Figura 4.53: Generación de Alertas en el Sistema CAMELOT

4.3.5. Servicios de visualización

En este apartado de la tesis, nos enfocamos en el desarrollo de módulos innovadores para la visualización y exhibición en diversas plataformas y formatos. Nuestro objetivo es explorar y mejorar las capacidades tecnológicas en cuatro áreas clave:

- Proyección de Sensores en *3 dimensiones* (3D): Investigamos métodos avanzados para la proyección de datos sensoriales en entornos tridimensionales, buscando mejorar la interpretación y la interacción con la información espacial.
- Modelado y Visualización en Tiempo Real 3D: Desarrollamos soluciones para la creación y visualización en tiempo real de modelos 3D, permitiendo una inmersión y comprensión más profunda de los entornos virtuales.
- Visualización en Realidad Aumentada y Dispositivos de Visualización Montados en la Cabeza: Nos centramos en la integración de tecnologías AR y *Helmet-mounted display* (HMD) para crear experiencias inmersivas que superponen información digital en el mundo real.
- Aplicaciones de Módulos para Smartphones y Tabletas: Extendemos la funcionalidad de estos dispositivos móviles para soportar aplicaciones avanzadas de visualización, aprovechando su ubicuidad y capacidad de procesamiento.

La integración de estas tecnologías promete revolucionar la forma en que interactuamos y percibimos la información digital, abriendo nuevos caminos en campos como la educación, la medicina y el diseño industrial.

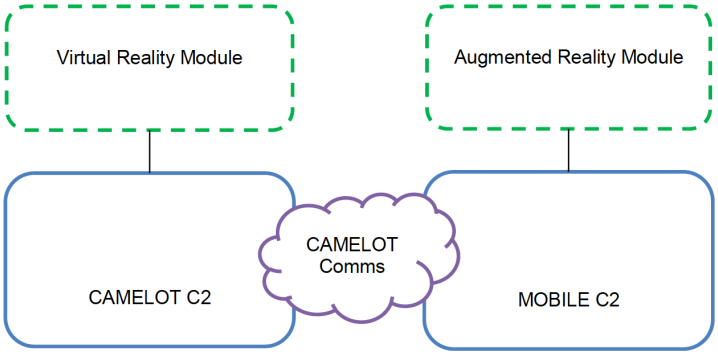

Figura 4.54: Representación gráfica de las tecnologías avanzadas de visualización y exhibición.

Proyección de sensores 3D

El objetivo de este módulo es realizar la proyección de un flujo de video en un *Geographic Information System* (GIS) 3D. Los datos de video están normalizados con el STANAG. Proporcionará el módulo de servicio para la extracción de metadatos de datos estandarizados para habilitar la proyección y visualización en un GIS 3D.

Este módulo proporciona los siguientes servicios:

- Extracción de metadatos del flujo de video.
- Proyección y visualización del video en GIS 3D.

Los metadatos utilizados para georreferenciar un video se insertan periódicamente entre los fotogramas del video. Estos metadatos siguen el formato de *Conjunto de datos locales* (LDS) del enlace de datos del UAS. Este formato es un Conjunto de Metadatos Locales de *Value-Length-Key* (KLV) diseñado para la transmisión a través de un enlace de comunicación inalámbrico, y es un estándar del *Motion imagery standards board* (MISB) [107].

Figura 4.55: Captura de pantalla del video y metadatos asociados.

Proyección de Video en GIS 3D

Cuando se extraen o calculan las ubicaciones de las cuatro esquinas del video, el fotograma actual se proyecta en el GIS 3D. Esta es una operación gráfica habitual: se crea un cuadrilátero y se localiza con las esquinas del video; luego se texturiza con la imagen del video. El motor gráfico se encarga de superponer esa imagen en la visualización de la situación táctica.

Figura 4.56: Proyección de video en GIS 3D.

Modelado y visualización 3D en tiempo real

El principal resultado es un módulo de software que permite la localización y seguimiento en 3D de todos los sistemas no tripulados desplegados en un escenario específico, ofreciendo una visualización en tiempo real de todos los

activos registrados y alertas, clasificándolos por tipo. Esta herramienta permite a los usuarios operativos analizar el entorno de un vistazo y adquirir una conciencia situacional completa con una carga mental reducida.

Funcionalidades del Módulo

La aplicación permite filtrar los activos disponibles en un área de interés específica y mostrar la información de los metadatos de los sensores montados en las plataformas no tripuladas. El módulo C2 desarrollado se ha orientado a resolver el problema de visualizar la situación operativa en un entorno lo más realista posible mediante una HMI de múltiples capas que incluye modelos 3D y funcionalidades tácticas como áreas de interés, alertas o simbología. Se ha adoptado la simbología de la *Publicación Procedural Aliada* (APP-6A) [108] de la OTAN como la más adecuada para reconocer y distinguir las diferentes alertas/activos.

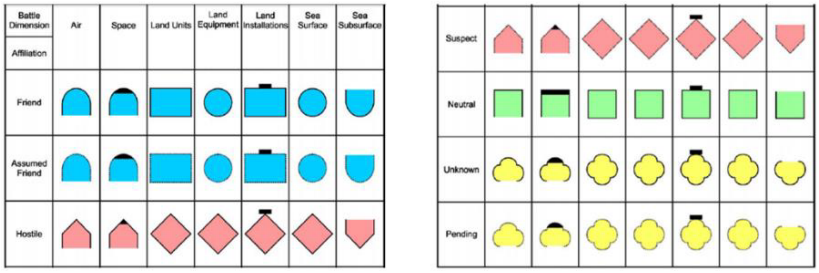

Figura 4.57: Visualización del Módulo de Software con Simbología OTAN.

Arquitectura y Prototipo de Visualización

Se ha definido el esquema de arquitectura de una aplicación que permite recoger de la base de datos todos los elementos almacenados (como activos o alertas) y mostrarlos en una pantalla para su visualización. Tras un análisis exhaustivo de lo disponible actualmente en el mercado y los requisitos funcionales del proyecto CAMELOT, se decidió desarrollar un prototipo de visualización inmersiva utilizando las gafas de VR Oculus Rift. El objetivo es generar conjuntos de datos reales anonimizados de información relevante para analizar/estudiar las herramientas del proyecto de una manera más precisa.

Figura 4.58: Prototipo de Visualización Inmersiva con Oculus Rift.

La arquitectura desarrollada incluye los siguientes componentes principales:

- Una conexión de cliente de Transferencia de Estado Representacional para realizar solicitudes a la plataforma CAMELOT.
- Un cliente del AMQP para suscribirse a posibles actualizaciones.
- Un sistema C2 basado en un GIS de *LUCIAD* [109].
- Interacción con la API de Oculus.
- Plataforma CAMELOT para interactuar con los servicios disponibles.

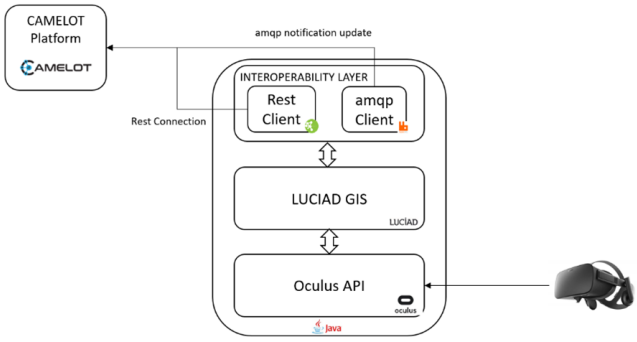

Figura 4.59: Componentes de la Arquitectura para Visualización VR.

Flujo de Trabajo Seguido para el Desarrollo

El flujo de trabajo seguido para el desarrollo es el siguiente:

1. Inserción de conjuntos de datos e información en la base de datos con la siguiente estructura:


```
{
  "timestamp": 1559925935,
  "alert_type": "track_aiming_towards_objective",
  "system_track_id": 25,
  "confidence_level": 0.91,
  "estimated_delay": 185,
  "point_of_interest": [
    {
      "geodeticLongitude": 45.02,
      "geodeticLatitude": 44.99
    }
  ]
}
```


Figura 4.60: Estructura de la Base de Datos.

2. Análisis de datos que podrían ser interesantes según las necesidades del prototipo. Es importante destacar que el prototipo no pretende interactuar con los datos, por lo que no requiere metadatos.

3. Encuesta de mercado de herramientas GIS existentes. Se decidió utilizar *LUCIAD* por las siguientes razones:

   a) Es un GIS especializado en la visualización y análisis de eventos en tiempo real.

   b) Interoperabilidad con VR más potente y preciso que otros GIS en el mercado.

   c) API potente con un número infinito de métodos.

   d) Gran comunidad de usuarios activos.

4. Selección del modo de representación de la información en el mapa, eligiendo rangos de formas y colores para la distinción de incidentes.

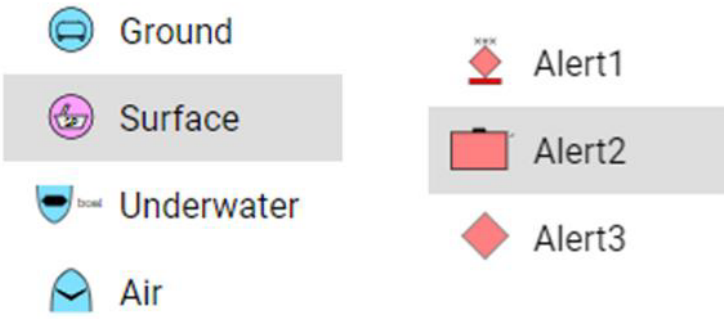

Figura 4.61: Modo de Representación de Información en el Mapa.

Una vez completados todos los pasos anteriores, se desarrolló una aplicación para visualizar los datos utilizando VR (en el caso del prototipo con Oculus Rift). Finalmente, se ha desarrollado un prototipo de laboratorio para pruebas funcionales como se muestra en la Figura 4.62. La pantalla muestra lo que el usuario vería a través de las gafas una vez que los datos se recolectan y muestran.

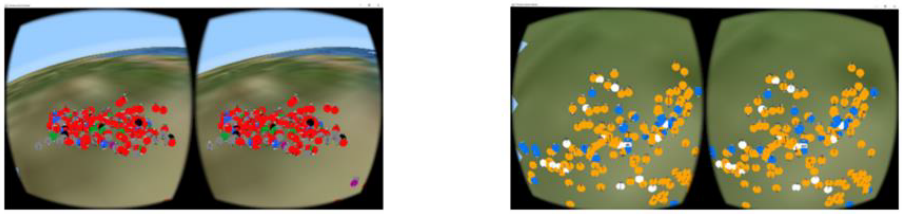

Figura 4.62: Prototipo de Laboratorio de Pruebas Funcionales.

Visualización datos CBRN

El módulo de Visualización CBRN es un componente basado en Docker que se almacena en el servidor CAMELOT junto con otros archivos Docker. Este módulo recibe mensajes de RabbitMQ del módulo de correlación CBRN. La comunicación se puede describir como interna, ya que la correlación CBRN es el único publicador y la Visualización es el único suscriptor de los datos.

El visualizador convierte los mensajes recibidos en archivos de *Keyhole Markup Language* (KML) [110] que se transfieren a la base de datos donde se almacenan y desde donde pueden transmitirse a componentes de visualización, como el prototipo de VR desarrollado o el HMI. El módulo de visualización CBRN

no proporciona información constantemente, sino que funciona como un servicio y necesita solicitudes para proporcionar los datos. Las solicitudes de datos pueden ser realizadas por componentes de visualización o por un script que solicita los datos automáticamente, por ejemplo, cada 30 segundos. El papel del módulo de visualización CBRN en el flujo de datos CBRN se presenta en la Figura 4.63:

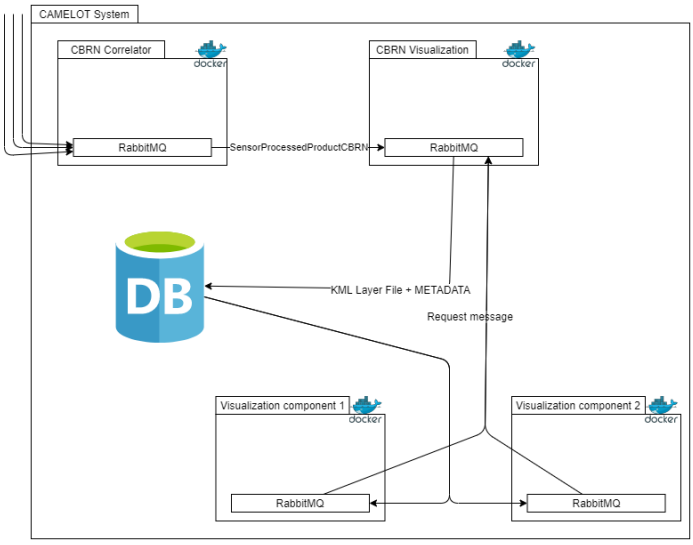

Figura 4.63: Flujo de Datos y Rol del Módulo de Visualización CBRN.

Realidad aumentada y visualización HMD

Este módulo implica el desarrollo de hardware y módulos de visualización de software en AR para mejorar la conciencia situacional de los operativos en campo. La información mostrada se recibe del sistema C2 CAMELOT a través del uso del marco de comunicaciones desarrollado.

La simbología mostrada incluye la ubicación en tiempo casi real de otros operativos y activos de la misión; las últimas ubicaciones conocidas/detectadas de sospechosos o alertas; órdenes de tareas asignadas, como puntos de paso y ubicaciones de búsqueda; y alertas emergentes y mensajes de misión. Toda la simbología puede ser despejada por dominio, afiliación o alcance, en tiempo real utilizando la aplicación móvil.

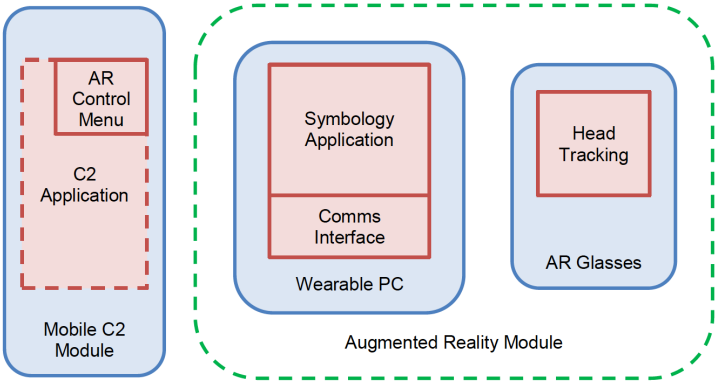

Figura 4.64: Interfaz de Usuario de la Aplicación AR para Conciencia Situacional.

Gafas AR y Sensores Inerciales

Las gafas AR incorporan sensores inerciales junto con algoritmos de seguimiento sofisticados para proporcionar orientación de la cabeza en el espacio libre. Los datos están disponibles a alta frecuencia para ofrecer movimiento suave y con latencia minimizada en tres ejes - cabeceo, balanceo y guiñada - leídos mediante una biblioteca de interfaz de *Bus serie universal* (USB).

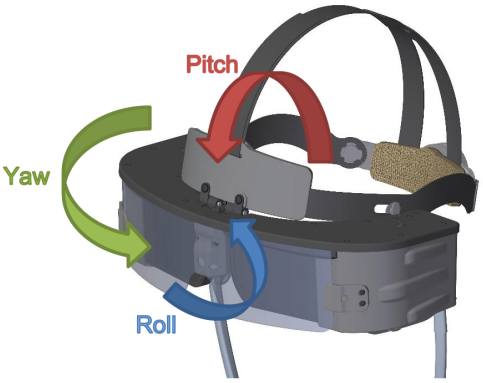

Figura 4.65: Gafas AR y Sensores Inerciales.

Componentes del Módulo AR

Los componentes principales del módulo AR son: el generador principal de símbolos AR y el controlador de visualización, el fireware de seguimiento de las gafas AR y un menú de software para controlar las gafas y la simbología mostrada. Los servicios se distribuyen en tres elementos de hardware, con la aplicación principal en un pequeño *Personal computer* (PC) usable. Las gafas actúan principalmente como un dispositivo de visualización, pero también incluyen la solución de seguimiento de cabeza en espacio libre, y el menú de control es una pantalla Android que forma parte de la aplicación móvil C2 principal.

La Figura 4.66 muestra el software de visualización AR funcionando en un PC de escritorio.

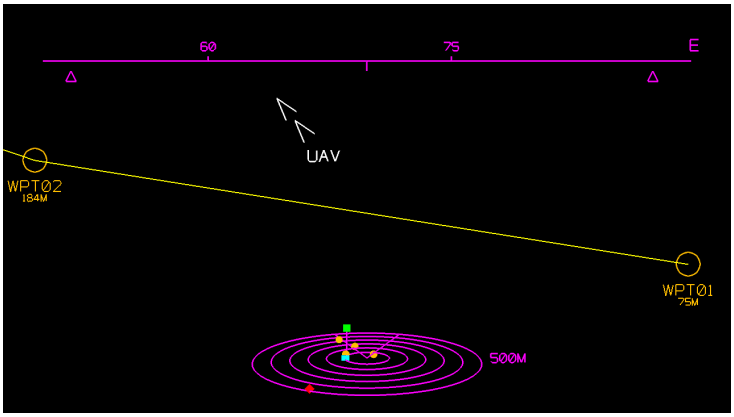

Figura 4.66: Captura de Pantalla del Software de Visualización AR.

De arriba abajo, la Figura 4.66 muestra:

- Una cinta de rumbo coloreada de magenta mostrando la orientación actual del cabeceo. Esto muestra 40 grados de una brújula con lecturas de 15 grados. Los dos triángulos son marcadores que representan la dirección de los dos puntos de ruta en el campo de visión.

- Un círculo de señalización de color blanco mostrando la dirección que el usuario debe girar su cabeza para poder ver el objeto destacado (en este caso, un *Unmanned Aerial Vehicles* (UAV)). El número de galones (<) es relativo a la diferencia en la dirección entre la línea de visión del usuario y el objeto destacado.

- Una ruta de color naranja, con dos puntos de ruta en el campo de visión. Los símbolos de los puntos de ruta (círculos naranjas) superponen posiciones en el mundo real y están unidos con la línea de ruta. Los puntos de ruta están anotados con su nombre y una lectura de distancia desde el usuario, en metros.

- Un radar 3D de color magenta, mostrando el rango relativo y la elevación de objetos circundantes. Las barras de elevación por encima del plano del radar indican que el objeto tiene una altitud mayor que el usuario, y viceversa para las barras por debajo del plano del radar.

Se eligió el magenta como el color principal para la visualización, ya que es el más visible en contraste con los colores normalmente vistos en la naturaleza.

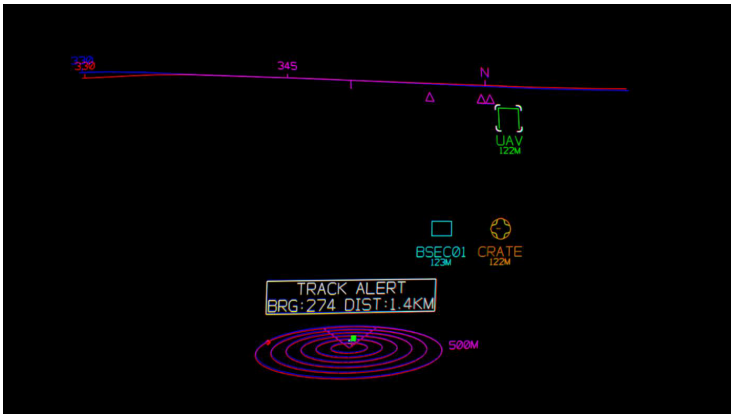

Figura 4.67: Vista a Través de las Gafas AR en un Escenario de Seguridad Fronteriza.

Gafas AR para Conciencia Situacional

Las gafas AR han sido diseñadas para mejorar la conciencia situacional del equipo de seguridad fronteriza, proporcionando al usuario ubicaciones actualizadas de aliados, activos de la misión y la posición detectada/última conocida de sospechosos. La simbología se muestra en las lentes transparentes de tal manera que se superpone al objeto en el mundo real.

Figura 4.68: Prototipo AR.

Aplicaciones móviles para tablet y/o smartphone

La aplicación móvil de CAMELOT tiene como objetivo mejorar la conciencia situacional de los usuarios finales, especialmente cuando no es factible acceder a una estación de trabajo o cuando se encuentran en el campo. Su propósito es facilitar la comunicación entre los dispositivos móviles y la plataforma C2 CAMELOT, constituyendo un subconjunto del conjunto de funcionalidades de la plataforma principal. El tipo de teléfono inteligente que alojará la aplicación es el Ulefone Armor 6s (Ulefone Armor 6s). A través de la aplicación, los usuarios podrán:

1. Monitorizar el estado y la ubicación exacta de los activos.
2. Acceder al mapeador de disponibilidad de recursos.
3. Recibir notificaciones y alertas sobre amenazas y situaciones urgentes o no planificadas.

Conexión con la Plataforma CAMELOT y Servicios Periféricos

La aplicación móvil se conecta al middleware de CAMELOT para recibir información que será utilizada para crear una imagen operacional. Además, tres servicios periféricos de la aplicación móvil respaldan su funcionalidad:

- Servicio de Autenticación
- Servicio de Configuración
- Registro de Servicios

En la siguiente Figura 4.69 se muestran las interfaces entre la aplicación móvil y otros servicios.

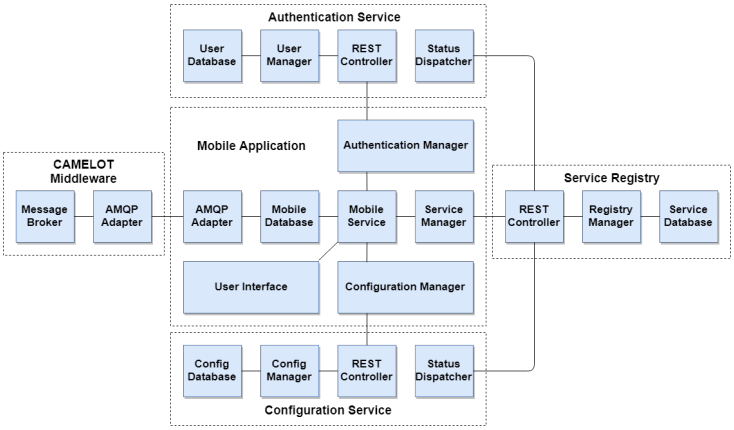

Figura 4.69: Interfaces entre la Aplicación Móvil y Otros Servicios.

Registro de Servicios

El registro de servicios es una aplicación que contiene información sobre los servicios periféricos de la aplicación móvil y se puede acceder a través de una interfaz REST. Esto ayuda a la aplicación móvil a descubrir los servicios de configuración y autenticación. Además, el registro de servicios monitorea el estado de los servicios periféricos, informando a la aplicación móvil sobre su disponibilidad. En resumen, el registro de servicios ofrece capacidades de descubrimiento de servicios y monitoreo de estado de los mismos. Consiste en los siguientes módulos:

- Base de datos de servicios
- Gestor de registros
- Controlador REST

La base de datos de servicios es una base de datos en memoria que contiene información sobre los servicios periféricos de la aplicación móvil. El gestor

de registros es responsable de mantener el registro actualizado y recupera la información necesaria cuando se solicita. El controlador REST maneja las solicitudes de la aplicación móvil y de otros servicios periféricos. El protocolo de comunicación se basa en una interfaz REST.

Servicio de Autenticación

El servicio de autenticación es una aplicación que gestiona los usuarios de la aplicación móvil. Expone una interfaz REST para ser consultada por la aplicación móvil cuando se necesita autenticar a un usuario. El servicio de autenticación consta de los siguientes módulos:

- Base de datos de usuarios
- Gestor de usuarios
- Controlador REST
- Despachador de estado

Los módulos del servicio de autenticación son similares a los del registro de servicios. Sin embargo, existen algunas diferencias en cuanto a las funciones que realizan. La base de datos de usuarios es una base de datos en memoria que contiene la siguiente información sobre los usuarios de la aplicación móvil:

- Identificador de usuario
- Nombre de usuario
- Contraseña
- Parámetros de autenticación opcionales

A diferencia de la base de datos del registro de servicios, la base de datos de usuarios del servicio de autenticación contiene información que necesita ser mantenida después de que se cierra la aplicación móvil. Por ejemplo, la información sobre los servicios en ejecución se reconstruye cuando los servicios se inician. Sin embargo, las credenciales de usuario deben recuperarse del almacenamiento, ya que no es práctico reconstruir manualmente la base de datos de usuarios desde cero cada vez que se inicia el servicio. Por esta razón, el gestor de usuarios mantiene la base de datos en memoria, pero también mantiene una base de datos relacional externa para lograr la persistencia de los datos.

En general, el gestor de usuarios es responsable de mantener actualizadas las bases de datos de usuarios y recupera la información necesaria cuando se solicita.

El controlador REST maneja una única solicitud que corresponde a la autenticación de un usuario. Además, se implementa un módulo adicional para el servicio de autenticación, el despachador de estado. Este módulo es responsable de:

- Registrar el servicio de autenticación en el registro de servicios cuando el servicio se inicia.
- Informar el estado del servicio de autenticación al registro de servicios.
- Dar de baja el servicio de autenticación del registro de servicios antes de que el servicio termine.

Servicio de Configuración

El servicio de configuración almacena las preferencias de cada usuario de la aplicación móvil para poder restaurarlas desde cualquier otro dispositivo que el mismo usuario pueda usar la aplicación móvil. El servicio de configuración consta de los siguientes módulos:

- Base de datos de configuración
- Gestor de configuración
- Controlador REST
- Disparador de estado

Estos módulos funcionan de manera similar a los módulos de los servicios de autenticación con las siguientes diferencias:

- La base de datos de configuración contiene las preferencias de los usuarios.
- El controlador REST maneja solicitudes sobre la recuperación de las preferencias de un usuario.

La UI está diseñada para proporcionar al usuario final un subconjunto de las capacidades que puede ofrecer una plataforma C2. Esto incluye lo siguiente:

- Proporcionar una imagen operacional que incluye activos y objetos detectados.
- Notificar al usuario sobre alertas generadas.
- Mostrar una lista de activos.
- Mostrar una lista de los objetos detectados.

- Proporcionar ayuda sobre la aplicación móvil.
- Almacenar las preferencias del usuario.

Las vistas funcionales de la aplicación y su jerarquía se muestran en la siguiente Figura 4.70:

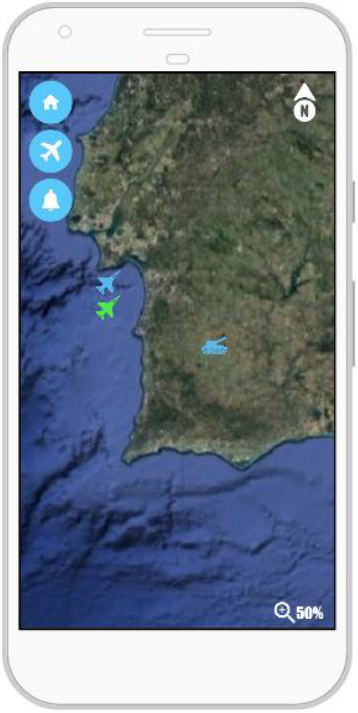

Figura 4.70: Dashboard aplicación móvil

La interfaz permitirá a los agentes mostrar y rastrear su ubicación, buscar activos o ubicaciones específicas en el mapa, obtener rutas y direcciones, tiempo estimado para que los activos alcancen su destino, así como rutas al destino más cercano.

4.3.6. Servicios de eficiencia energética

El objetivo principal de este servicio es mejorar la autonomía de la batería de cualquier sistema no tripulado (terrestre, superficial o aéreo). El aspecto más

importante al desarrollar una plataforma no tripulada es analizar los factores que más afectan el consumo total de energía. Por ello, el estudio se centró en el intercambio de información entre la GCS y la plataforma no tripulada, ya que es un proceso que se repite continuamente y consume mucha energía.

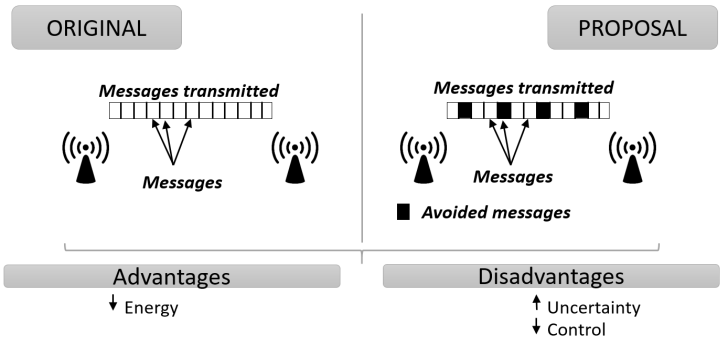

Figura 4.71: Proceso de Intercambio de Información y Consumo de Energía

Modelo Propuesto

Para minimizar este problema, se propone reducir la frecuencia del proceso de intercambio de comunicaciones entre la GCS y el sistema no tripulado. No es necesario comunicarse constantemente, pero se debe encontrar un equilibrio entre la incertidumbre aumentada sobre la posición del activo no tripulado y la vida útil de su batería.

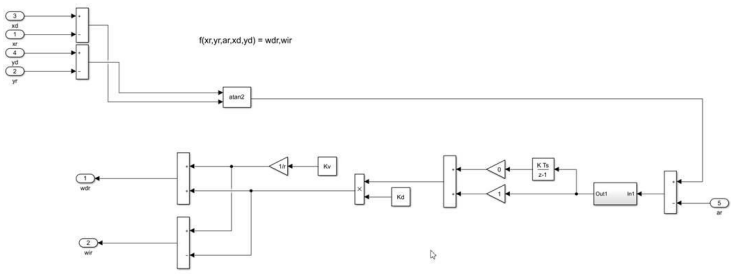

Figura 4.72: Modelo Propuesto para Estimación de Trayectoria

Algoritmos de Estimación

El modelo propuesto para estimar la trayectoria del sistema no tripulado en ausencia de comunicación con su GCS se basa en varios algoritmos que estimarán su posición:

- Algoritmo de estimación de posición
- Algoritmo de control de trayectoria
- Algoritmo de estimación de orientación

Algoritmo de Estimación de Posición

Para estimar la posición de un sistema no tripulado en ausencia de datos reales, se ha creado un algoritmo para el desarrollo de un prototipo de laboratorio. La función de entrada es $f(xr, yr, ar, xd, yd)$ que obtiene como resultado wdr, wir, donde:

- xr: Medición real de x
- yr: Medición real de y
- ar: Medición real de orientación
- xd: Medición calculada de x
- yd: Medición calculada de y
- wdr: Potencia de la rueda derecha
- wir: Potencia de la rueda izquierda

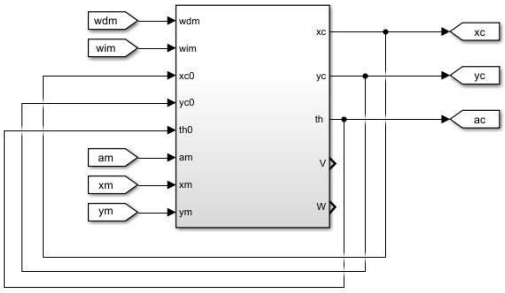

Figura 4.73: Algoritmo de Estimación de Posición

Estimación de Posición/Orientación y Control de Trayectoria

Este algoritmo calcula las coordenadas y la orientación del vehículo a partir de la velocidad angular de las ruedas, medida por los codificadores. Los resultados son las coordenadas y orientación calculadas xc, yc, ac que se utilizarán en el control de trayectoria si no hay mediciones reales disponibles.

$$V[k] = \left(wdm[k] + wim[k]\right)\frac{r}{2}$$
$$W[k] = \left(wdm[k] - wim[k]\right)\frac{r}{b}$$

$$X_{estimada}[k+1] = X_{estimada}[k] + V[k]\cdot T\cdot\cos\left(T\cdot W[k] + \theta_{estimada}[k]\right)$$
$$Y_{estimada}[k+1] = Y_{estimada}[k] + V[k]\cdot T\cdot\sin\left(T\cdot W[k] + \theta_{estimada}[k]\right)$$
$$\theta_{estimada}[k+1] = \theta_{estimada}[k] + T\cdot W[k]$$

Figura 4.74: Estimación de Posición/Orientación y Control de Trayectoria

Control de Trayectoria

Este algoritmo es responsable de generar la velocidad angular deseada para las ruedas a partir de las coordenadas xd, yd y xm, ym, am, o xc, yc, ac. Utiliza la posición medida si está disponible; de lo contrario, recurre a la odometría. Además, incluye una función para verificar si se ha alcanzado el destino.

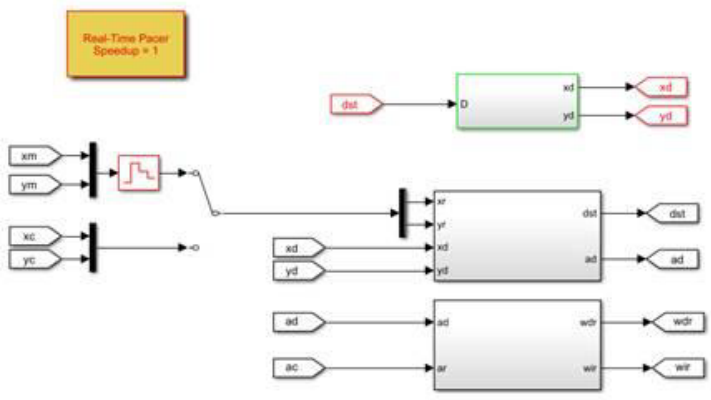

Figura 4.75: Algoritmo de Control de Trayectoria

Estimación de Posición/Orientación

Este algoritmo calcula las coordenadas y la orientación del vehículo a partir de la velocidad angular de las ruedas. Los parámetros incluyen el radio de la rueda, la distancia entre las ruedas y el período de muestreo.

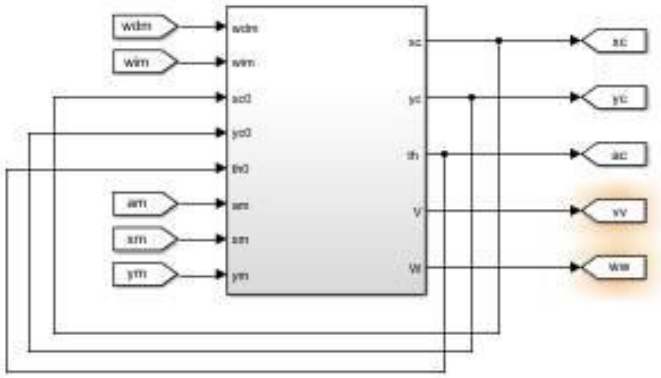

Figura 4.76: Algoritmo de Estimación de Posición/Orientación

Prototipo de Laboratorio

Se ha desarrollado un prototipo de laboratorio para pruebas funcionales, con una interfaz de usuario que permite seleccionar planes de misión y activos para la simulación.

Figura 4.77: Interfaz del Prototipo de Laboratorio

4.3.7. Servicios de adaptación de datos (CAL)

Teniendo en cuenta que los activos no tripulados que se demostrarán bajo el alcance de CAMELOT ya poseen protocolos de comunicación propietarios para intercambiar datos con sus propios GCS, el consorcio decidió implementar una solución que permita a cualquier activo, independientemente del protocolo de comunicación, conectarse al sistema CAMELOT, evitando el esfuerzo necesario para cambiar estos protocolos propietarios cada vez que se emplee un nuevo activo. En este sentido, se propuso una solución basada en la implementación de adaptadores de protocolo específicos por parte de los socios del consorcio. Esta decisión tiene, como base, la arquitectura STANAG 4817 que ya prevé el uso de adaptadores de protocolo específicos para cada activo (por ejemplo, STANAG 4586, *JANUS*, *JAUS*, *Mavlink*, *ROS*).

Así pues, es posible verificar que el sistema CAMELOT interactuará con entidades externas de dos maneras:

- A través de la Capa de Adaptador CAMELOT con los activos no tripulados, que probablemente sean productos de diferentes proveedores con protocolos propietarios.

- A través de los Servicios de Interoperabilidad CAMELOT (API REST) con sistemas C2 existentes.

Dentro del alcance del proyecto CAMELOT, la principal responsabilidad de estos adaptadores de protocolo es recibir mensajes del sistema - enviados de acuerdo con el modelo de datos de CAMELOT - y convertir estos mensajes a cada uno de los protocolos propietarios de cada proveedor de activos. Además, estos adaptadores de protocolo son responsables de enviar los mensajes traducidos a los respectivos GCS. Al mismo tiempo, se espera que estos adaptadores de protocolo tengan la capacidad de recibir mensajes de los GCS en los protocolos propietarios y ser capaces de traducir estos mensajes al modelo de datos de CAMELOT.

De la Figura 4.78, se puede verificar cómo se realizará la interfaz entre el sistema CAMELOT y los GCS locales a través de los traductores. La cantidad de adaptadores de protocolo depende del número de activos que utilizan diferentes protocolos de comunicación, por lo tanto, requieren adaptadores de protocolo específicos. Dado que cada proveedor de activos tiene un conocimiento completo de su activo y respectivo GCS, se acordó entre todos los socios que cada entidad será responsable de desarrollar el traductor de protocolo para su propio activo. Esta metodología permite a cada beneficiario detectar posibles brechas en el modelo de datos de CAMELOT en una etapa temprana.

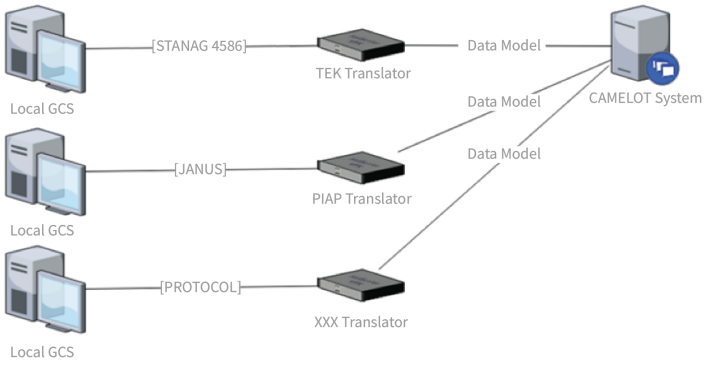

Figura 4.78: Interfaz entre el sistema CAMELOT y los GCS locales a través de los adaptadores.

4.3.8. Servicios de análisis de gestión de datos (DMA)

Esta sección detalla el componente de DMA de la plataforma CAMELOT. Este componente es responsable de recuperar información del middleware de CAMELOT, procesarla y generar alertas y advertencias basadas en las necesidades operativas del usuario final. El Motor de alerta temprana es el módulo central del DMA que facilita la evaluación de riesgos combinada con un conjunto predefinido de reglas que corresponden a requisitos operativos específicos.

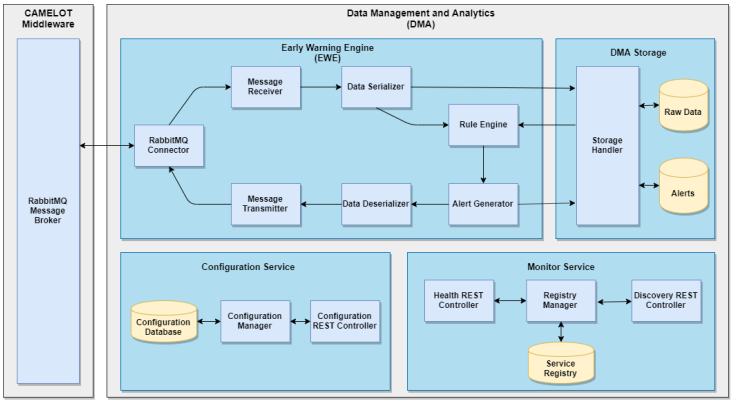

Figura 4.79: Arquitectura del componente de Gestión de Datos y Análisis (DMA) de la Plataforma CAMELOT.

El componente DMA consta de varios servicios y módulos. El EWE facilita la lógica empresarial del DMA, produciendo así información significativa en forma de alertas. Además de la funcionalidad central del DMA, se imponen un conjunto de servicios adicionales para facilitar las operaciones del EWE. La arquitectura general del DMA se ilustra en la Figura 4.79.

Motor de alerta temprana

El EWE es responsable de procesar los datos entrantes y producir información significativa como alertas y advertencias. El mecanismo implementado consta de varios módulos que se encargan de las operaciones de mensajería y extraen perspectivas situacionales valiosas. Específicamente, el EWE consta de los siguientes módulos:

- Motor de Reglas
- Generador de Alertas
- Serializador de Datos
- Deserializador de Datos
- Receptor de Mensajes
- Transmisor de Mensajes
- Conector RabbitMQ

El motor de reglas realiza verificaciones cruzadas entre los datos y las reglas para detectar posibles amenazas o actos anormales. Posteriormente, el generador de alertas consume la inteligencia producida por el motor de teglas y formula las alertas apropiadas. Los datos procesados provienen de a) el middleware de CAMELOT (datos en tiempo real) y b) el almacenamiento de DMA (datos históricos).

El resto de los módulos de EWE facilitan las operaciones de mensajería para comunicarse con el middleware de CAMELOT. La traducción de los datos entre el formato en que se almacenan y el formato en que se transmiten es facilitada por el serializador de datos y el deserializador de Datos. El receptor de mensajes y el transmisor de mensajes están interconectados con el conector RabbitMQ integrado para manejar el flujo de datos entre el EWE de DMA y el middleware de CAMELOT.

Almacenamiento DMA

El almacenamiento de DMA mantiene toda la información que es manejada por el EWE. Su base de datos consta de los siguientes tipos de datos:

- Datos Crudos: recibidos del middleware de CAMELOT
- Alertas: producidas por el generador de alertas del EWE

El módulo gestor de almacenamiento maneja las operaciones *Create, Read, Update, Delete* (CRUD) en las bases de datos. El motor de reglas del EWE recupera los datos históricos del almacenamiento de DMA y los combina con datos en tiempo real para validar las reglas impuestas. Si se detecta una anomalía, entonces el generador de alertas produce una alerta relevante que se transmite al middleware pero también se almacena en el almacenamiento de DMA para su uso futuro por el motor de reglas.

Servicio de monitorización

El servicio de monitorización ofrece funcionalidades de monitoreo del estado del servicio y descubrimiento de servicios. Es responsable de rastrear el estado de los servicios de DMA e informarles sobre los detalles de cada servicio. Esto se facilita manteniendo un registro que contiene información sobre los servicios de DMA. El registro de servicios contiene la siguiente información:

- Identificador del servicio
- Nombre del servicio
- Proveedor del servicio
- Marca de tiempo de registro
- Último estado reportado
- Marca de tiempo del último estado

Un servicio de DMA debe comunicarse con el servicio de monitorización a través de a) el controlador REST de descubrimiento y b) el controlador REST de salud. El primero es responsable de las operaciones de descubrimiento de servicios y el segundo de las operaciones de monitoreo del estado del servicio. Para ambos tipos de operaciones, se proporciona una interfaz REST separada para establecer una comunicación entre el servicio de monitorización y los demás servicios de DMA.

Servicio de configuración

El servicio de configuración contiene parámetros relacionados con la configuración de DMA. Funciona como un registro para parámetros de conexión, definiciones de reglas, configuraciones de bases de datos y otras opciones en tiempo de ejecución. El EWE, el almacenamiento de DMA y el servicio de monitorización recuperan sus respectivas configuraciones del Servicio de Configuración cuando se inicia DMA. Este enfoque ofrece un registro centralizado de parámetros, proporcionando así un método práctico para configurar DMA. El servicio de configuración consta de los siguientes módulos:

- Base de Datos de Configuración: una base de datos no relacional (NoSQL) que contiene los parámetros de configuración.
- Gestor de Configuración: gestiona las operaciones CRUD sobre la Base de Datos de Configuración.
- Controlador REST de Configuración: proporciona a los servicios solicitantes los parámetros de configuración necesarios.

Los siguientes parámetros de configuración estarán disponibles en el Servicio de Configuración:

- Parámetros de conexión del middleware de CAMELOT
- Parámetros de conexión *Virtual Private Network* (VPN)
- Parámetros de conexión RabbitMQ
- Suscripciones a mensajes del Conector RabbitMQ
- Definiciones de reglas de EWE
- Alertas activas de EWE
- Parámetros de conexión del Almacenamiento de DMA
- Parámetros de conexión del Servicio de Monitorización
- Parámetros de conexión del Servicio de Configuración

4.3.9. Servicios de comunicaciones y redes

Uno de los principales objetivos de CAMELOT es establecer una conectividad fiable y segura entre las unidades de campo, los comandantes de campo (nivel operativo) y los centros C2 (nivel táctico). La solución de comunicación global de CAMELOT se basa en un enfoque de red híbrida segura que proporcionará alta disponibilidad en áreas remotas fuera del área de cobertura de las redes de comunicación tradicionales o en áreas donde estas redes se hayan visto interrumpidas debido a un desastre. La red híbrida proporcionará la disponibilidad y las tasas de datos necesarias dentro de las restricciones de latencia para apoyar el amplio conjunto de interacciones entre las unidades de campo y los centros C2 en misiones críticas en tiempo.

Descripción de la Arquitectura de Red

Esta sección presenta una descripción detallada de la arquitectura de red de CAMELOT, con la Figura 4.80 presentando una visión general de alto nivel de los tres segmentos principales:

- La red de radio representa la red de última milla que conecta las unidades de campo y los UxVs con el centro de comunicaciones.
- Vehículo Terrestre de Viasat [111] que actúa como enlace troncal para la red de radio, es decir, el nodo de comunicación que conecta la red de radio con el centro C2. El Vehículo Terrestre de Viasat tiene tres funcionalidades principales:
  - Centro de comunicaciones - El objetivo principal de este centro de comunicaciones nómada es proporcionar cobertura de red en áreas donde los sistemas de comunicación terrestres ordinarios no están disponibles debido a la falta de cobertura, fiabilidad o interrupción.
  - Cámara a bordo - El vehículo estará equipado con una cámara *Internet Protocol* (IP) [112] que transmitirá video en tiempo real y podrá ser controlada tanto por un operador dentro del vehículo como por el Centro C2.
  - Estación de Control Terrestre - El vehículo puede albergar a un operador de la cámara, así como a un oficial que tenga conciencia situacional y pueda coordinar y brindar apoyo a las unidades en el campo.
- El C2 es la entidad que tiene una visión y control globales de todos los componentes del proyecto CAMELOT.

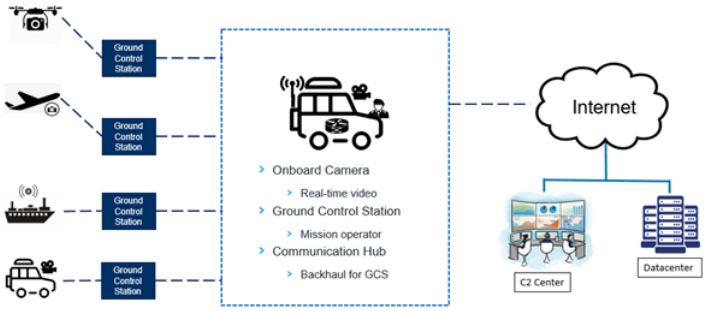

Figura 4.80: Visión general de la arquitectura de red de CAMELOT.

Red de radio

El objetivo principal de la red de radio es proporcionar conectividad a las unidades de campo y a los UxVs en áreas de operación remotas que están fuera de la cobertura de las redes de comunicación tradicionales. Además, esta red de radio debe proporcionar conectividad de alto alcance a unidades estacionarias y móviles con baja latencia para misiones críticas en tiempo.

Una solución es desplegar una Red Móvil Ad-Hoc autoformable y autoreparable, que proporciona video, voz y compartición de datos críticos para la misión sin depender de una infraestructura establecida.

Además de los canales de audio, cada módulo de radio admite transmisiones de video H.264 [113]. Dependiendo del modelo del terminal de radio y la resolución de las transmisiones de video, la red puede soportar múltiples transmisiones de video simultáneamente (por ejemplo, 4 canales de 2 Mbps cada uno). Además, el terminal de radio de Trellisware [114] puede actuar como un relevo para otras radios en rango, creando así una red de radio en malla con un gran alcance (20 km en *Line of sight* (LOS) por salto de red). Los módulos de radio (equipados en los primeros respondedores y UAVs) enviarán o retransmitirán todas las transmisiones de datos al centro de comunicaciones, donde el tráfico será enrutado al centro C2.

Centro de mando y control (C2)

El C2 es la entidad que tiene una visión y control globales de todos los componentes del proyecto CAMELOT, lo que significa que es crucial que el intercambio de datos cumpla con estrictos requisitos de seguridad. Esto se puede lograr estableciendo una conexión VPN de extremo a extremo entre el centro C2 y el centro de comunicaciones. Cada socio de CAMELOT puede

conectarse a los servicios alojados, lo que permitirá el intercambio bidireccional de datos con los componentes remotos de CAMELOT (operadores de campo y UxVs).

4.4. Logros de CAMELOT

A continuación, se presenta una lista de logros propuestos para el proyecto.

1. **Integración de Sistemas Multi-dominio:** Desarrollo exitoso de una plataforma integrada que coordina operaciones en tierra, mar, aire y ciberespacio.
2. **Avances en Inteligencia Artificial:** Implementación de algoritmos de *Inteligencia artificial* (IA) y aprendizaje automático para mejorar la toma de decisiones en tiempo real.
3. **Mejora en la Conciencia Situacional:** Creación de interfaces avanzadas para proporcionar visualización en tiempo real y aumentar la conciencia situacional en operaciones complejas.
4. **Comunicaciones Seguras:** Establecimiento de un protocolo de comunicaciones robusto y seguro, mejorando la fiabilidad en diferentes escenarios operativos.
5. **Interoperabilidad Efectiva:** Logro de una interoperabilidad completa entre diversos sistemas y plataformas, adaptándose a múltiples necesidades operativas.
6. **Capacitación y Simulación:** Desarrollo de herramientas de capacitación y simulación para entrenar al personal en el uso eficiente de las tecnologías CAMELOT.
7. **Desarrollo de Tecnologías de Realidad Aumentada:** Implementación exitosa de tecnologías AR para mejorar la orientación y el análisis en el campo.
8. **Optimización de Recursos:** Maximización de la eficiencia en la gestión y despliegue de recursos en operaciones multi-dominio.
9. **Análisis de Datos Avanzado:** Uso efectivo de análisis de grandes volúmenes de datos para anticipar y responder a situaciones dinámicas.
10. **Sostenibilidad y Escalabilidad:** Asegurar que las soluciones desarrolladas son sostenibles a largo plazo y escalables a diferentes tamaños de operaciones.

Los logros propuestos para el proyecto CAMELOT representan un esfuerzo significativo en la innovación y el avance en la coordinación y ejecución de operaciones multi-dominio. Estos objetivos establecen un camino claro hacia la mejora continua y la excelencia operativa.

Capítulo 5

Validación de la arquitectura: Caso 2 - PREVISION

5.1. Introducción

El propósito de PREVISION es dotar a los analistas e investigadores de las LEAs con herramientas y soluciones que actualmente no están disponibles comercialmente, para manejar y capitalizar las masivas corrientes de datos heterogéneos que deben procesarse durante las complejas investigaciones de crímenes y las evaluaciones de riesgo de amenazas. En un escenario donde los criminales están cada vez más determinados a utilizar tecnología nueva y avanzada para sus causas, el objetivo es establecer PREVISION como una plataforma abierta y preparada para el futuro, proporcionando apoyo práctico de vanguardia a las LEAs en su lucha contra el terrorismo, el crimen organizado y la ciberdelincuencia, que representan tres grandes desafíos de seguridad transfronterizos a menudo interconectados.

PREVISION proporcionará soporte analítico avanzado en tiempo casi real para múltiples corrientes de big data (provenientes de redes sociales en línea, la web abierta, la Darknet, sistemas de CCTV y vigilancia por vídeo, UxV, fuentes de datos de tráfico y financieros, y muchos más), permitiendo posteriormente su integración semántica en grafos de conocimiento dinámicos y autónomos que capturan la estructura, interrelaciones y tendencias de grupos e individuos terroristas, organizaciones de ciberdelincuencia y grupos de crimen organizado, dando lugar a una conciencia situacional mejorada en estos campos. Para alcan-

zar este objetivo, se integrarán muchos componentes diferentes, combinándose y complementándose entre sí para proporcionar la funcionalidad completa de PREVISION, así como para lidiar con la enorme cantidad de datos que las LEAs tienen que gestionar.

Las entradas a la plataforma PREVISION son las diversas fuentes de datos, que van desde datos geoespaciales, fuentes de datos de tráfico, datos de telecomunicaciones y fuentes de la *Darknet* [115] y la *Clearnet*. Se desarrollarán módulos apropiados para la minería de datos eficiente, apoyando la metodología general de prevención e investigación de crímenes de PREVISION. Estos datos serán procesados por las herramientas correspondientes de PREVISION, capaces de manejar tales corrientes de datos heterogéneos. Algoritmos de detección y reconocimiento facial identificarán personas específicas en imágenes/videos obtenidos de la web, redes sociales y grabaciones de cámaras estáticas/móviles. El reconocimiento de objetos se aplicará en cámaras de vigilancia portátiles y estáticas para detectar objetos sospechosos y luego se extenderá para que objetos y personas puedan ser rastreados a lo largo del vídeo. El análisis de multitudes y el reconocimiento de acciones humanas con localización espacio-temporal se aplicarán para detectar actividades sospechosas/anormales. Se utilizarán técnicas de análisis de big data sobre los datos recopilados para detectar tendencias ocultas dentro de los conjuntos de datos. La detección de patrones ocultos en los datos permitirá la predicción de actividades terroristas y criminales organizadas. Técnicas avanzadas de análisis de big data, basadas en métodos de clasificación y redes neuronales artificiales, se aplicarán a los datos recopilados para detectar anomalías, indicadores de comportamiento y revelar asociaciones y reglas previamente desconocidas que están asociadas con actividades ciberdelictivas. Además, se aplicará fusión de datos e información a los datos heterogéneos para transformar la información en conocimiento valioso. Este procesamiento y análisis de datos deberían facilitar las operaciones de las LEAs contribuyendo a operaciones más eficientes en las áreas identificadas en los casos de uso. Para facilitar esto, los resultados del análisis de datos se presentarán a los usuarios finales con herramientas de visualización innovadoras para mejorar la conciencia situacional de los tomadores de decisiones, utilizando tecnologías como la realidad virtual y aumentada.

5.2. Objetivos técnicos

El proyecto PREVISION tiene como objetivo principal desarrollar una plataforma avanzada de análisis de datos para las LEAs, incorporando una serie de requisitos técnicos específicos para garantizar seguridad, eficiencia y accesibilidad. Los objetivos técnicos derivados de estos requisitos son los siguientes:

1. **Control de Acceso:** Implementar mecanismos de control de acceso para asegurar que solo los usuarios autorizados puedan acceder a los datos y servicios de la plataforma.
2. **Perfiles de Usuario:** Soportar perfiles de usuario personalizados, permitiendo el acceso a datos y servicios específicos basados en su perfil/rol.
3. **Integración UxV:** Capacidad para integrar datos provenientes de flujos de vídeo de UxVs.
4. **Colaboración con LEAs:** Diseñar perfiles de usuario y niveles de acceso con la ayuda de las LEAs, aplicables tanto a módulos del sistema como a casos de uso y datos.
5. **Seguridad y Privacidad de Datos:** Asegurar la privacidad y seguridad de los datos mediante técnicas de anonimización/pseudonimización y mecanismos de retención de datos claros.
6. **Registro de Actividades del Usuario:** Registrar las acciones de los usuarios para garantizar la integridad de los datos y el uso adecuado de la plataforma.
7. **Comunicaciones Seguras:** Cifrar los datos intercambiados entre módulos y emplear enlaces de comunicaciones cifradas.
8. **Respaldo Automatizado:** Proporcionar mecanismos de respaldo automatizados para proteger los datos.
9. **Documentación y Manuales:** Acompañar el sistema y sus módulos con manuales de usuario para facilitar la adopción y capacitación.
10. **Integración con Bases de Datos de LEAs:** Permitir el uso de datos de bases de datos LEA existentes y de fuentes externas, restringiendo el acceso solo a usuarios autorizados.
11. **Herramientas de Crawling:** Soportar la captura de datos de fuentes de la *Darknet* y la *Clearnet*.
12. **Análisis Multilingüe:** Ofrecer análisis lingüístico en múltiples idiomas.
13. **Aprobación Operativa:** Requerir que un operador humano autorizado apruebe o modifique las recomendaciones de PREVISION antes de su transmisión a otro módulo.
14. **Interfaz de Búsqueda Eficiente:** Proveer una interfaz de búsqueda eficiente para el descubrimiento de contenido.

15. **Interfaz de Usuario Intuitiva:** Desarrollar una interfaz de usuario que facilite las investigaciones criminales, incluyendo un mecanismo de notificación inteligente y personalizable.

16. **Manejo de Datos en Streaming y Modo Independiente:** Permitir que los módulos analíticos manejen datos en streaming y que el despliegue de PREVISION soporte un modo autónomo.

Estos objetivos técnicos son fundamentales para establecer PREVISION como una plataforma abierta y preparada para el futuro, proporcionando un soporte práctico de vanguardia a las LEAs en su lucha contra el terrorismo, el crimen organizado y la ciberdelincuencia.

5.3. Arquitectura de PREVISION

La arquitectura funcional de PREVISION, que se detalla en el capítulo 3 de esta tesis, representa un enfoque innovador y avanzado en la prevención e investigación del crimen. Esta arquitectura aprovecha una diversidad de fuentes de datos, que incluyen desde información geoespacial y de tráfico hasta datos de telecomunicaciones y de las redes *Darknet* y *Clearnet*. Dentro de PREVISION, se desarrollan módulos especializados para la extracción eficiente de datos, los cuales están alineados con la estrategia global del proyecto para prevenir y analizar actividades criminales.

En el corazón de PREVISION se encuentran las herramientas de procesamiento de datos, capaces de manejar flujos heterogéneos de información. Estas herramientas aplican algoritmos de detección y reconocimiento facial para identificar individuos en una variedad de medios digitales, como imágenes y videos obtenidos de la web, redes sociales y grabaciones de cámaras estáticas o móviles. Además, se implementan técnicas de reconocimiento de objetos en cámaras de vigilancia, tanto portátiles como fijas, para detectar y rastrear objetos y personas sospechosas a lo largo de las grabaciones. El análisis de multitudes y la identificación de acciones humanas con localización espacio-temporal son fundamentales para detectar actividades anormales o sospechosas.

La aplicación de técnicas de big data y análisis predictivo es un componente crucial de PREVISION. Estas técnicas permiten descubrir tendencias ocultas en los conjuntos de datos, facilitando la predicción de actividades terroristas y criminales organizadas. Métodos avanzados basados en clasificación y redes neuronales artificiales se utilizan para detectar anomalías, indicadores de comportamiento y para revelar asociaciones y reglas relacionadas con actividades cibercriminales. Además, la fusión de datos e información transforma

estos conjuntos de datos heterogéneos en conocimiento valioso, facilitando las operaciones de las LEAs y mejorando la eficiencia en áreas críticas.

Finalmente, los resultados del análisis de datos se presentan a los usuarios finales mediante herramientas de visualización innovadoras. Estas herramientas mejoran la conciencia situacional de los tomadores de decisiones y utilizan tecnologías como la realidad virtual y aumentada para proporcionar una representación más intuitiva y detallada de la información. La arquitectura funcional de PREVISION, por tanto, no solo se centra en la integración y análisis avanzado de datos, sino también en la presentación efectiva de información para apoyar de manera proactiva la prevención e investigación del crimen.

Este análisis de la arquitectura funcional de PREVISION subraya la importancia de una integración de datos sofisticada, el análisis avanzado y una presentación efectiva de la información, demostrando su papel crucial en la prevención e investigación del crimen.

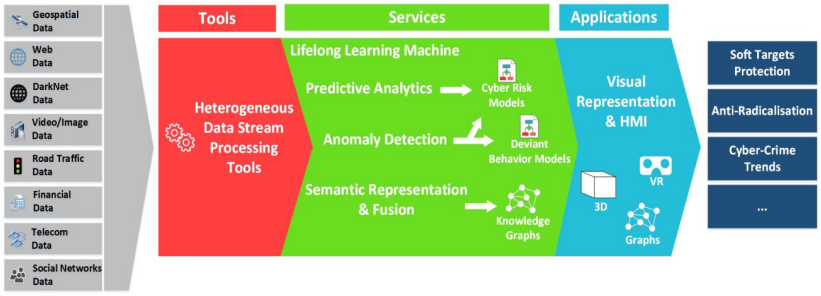

Figura 5.1: Concepto PREVISION

5.3.1. Módulos de procesamiento de flujos de datos heterogéneos a escala extrema

Herramientas de rastreo

En los últimos años, los datos obtenidos de fuentes abiertas en Internet (*Darknet y Clearnet*), incluidas las redes sociales en línea, se han convertido en una fuente valiosa de inteligencia *Open source intelligence* (OSINT) [116] para las LEAs. Combinando datos de diferentes fuentes, es posible mejorar la calidad de la inteligencia accionable que se puede obtener de ellos. Esta combinación a menudo permite obtener más información en comparación con el caso en que los datos no se combinan entre ellos. PREVISION utilizará datos de *Darknet y Clearnet*, siguiendo las directrices desarrolladas y cumpliendo con los requisitos

aplicables (respecto a la privacidad y seguridad de los datos, así como aspectos legales y éticos).

Se emplea una infraestructura de rastreo escalable para recopilar los datos necesarios, que luego son tratados en conjuntos de datos. Estos conjuntos de datos están disponibles para la búsqueda (por ejemplo, buscando entidades específicas como anuncios para el comercio ilícito de armas, etc.) y el resultado del análisis (por ejemplo, gráficos que representan las interacciones entre entidades, etc.) se pone a disposición del usuario.

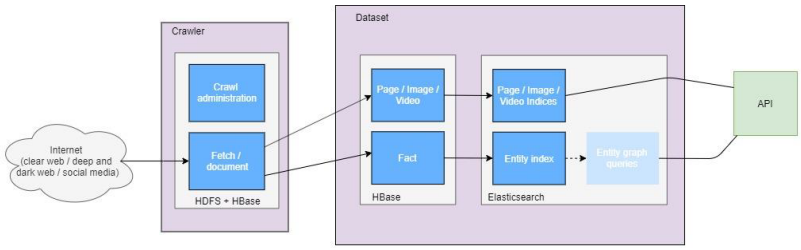

Figura 5.2: Flujo de herramienta de rastreo

La funcionalidad del rastreador se proporciona a través de una API de gestión que facilitará la configuración del rastreador para recopilar datos de fuentes abiertas de *Darknet y Clearnet*. Las características incluyen:

- Rastreo iniciado por el usuario.
- Inyectar una o muchas semillas por rastreo.
- Renderización de *JavaScript*.
- Ajustar la velocidad y profundidad del rastreo.
- Cambiar la cortesía.
- Priorizar qué enlaces seguir primero.
- Establecer tasas de actualización y retorno.
- Rastreo anónimo.
- Visualizar el progreso del rastreo.
- Captura de capturas de pantalla de páginas web.
- Devolver datos rastreados en formato de datos abiertos, Archivo HTTP.

La funcionalidad del rastreador es apoyada por características de obtención de páginas que incluyen:

- Renderizar dinámicamente una página web con un navegador real.
- Recolectar automáticamente todos los activos (por ejemplo, imágenes, etc.) incluidos en la página.
- Soporte para proxies, por ejemplo, puede obtener recursos de Servicios Ocultos de Tor [117] con el proxy de Tor.
- Soporte para scripts específicos del sitio para automatizar la interacción (por ejemplo, desplazamiento, inicio de sesión, clics en botones, etc.).
- Soporte para capturas de pantalla.

En cuanto a los datos de Darknet, se utilizarían las siguientes entidades considerando los casos de uso propuestos:

- Edad, Ciudad, País, Última Actividad, Correo Electrónico, Número de Teléfono (si lo hay), nombre de usuario, número de publicaciones, fecha de registro, Nombre Completo.

En cuanto a los datos de Clearnet, se utilizarían las siguientes entidades considerando los casos de uso propuestos:

- Edad, Ciudad, Género, País, Correo Electrónico, Número de Teléfono (si lo hay), nombre de usuario, ID de Usuario, Perfil (contiene campos mencionados anteriormente), Publicaciones, Comentarios, Eventos (asistidos por, creados por, fecha de creación), Nombre Completo, Idioma, Amigos, Seguidores, Seguidos, Hashtags.

La lista anterior de entidades será revisada frecuentemente a medida que los casos de uso y los componentes de análisis evolucionen con el objetivo de minimizar la información extraída mientras se mantienen los resultados del análisis relevantes para los usuarios finales.

Para permitir la recolección y análisis de enormes cantidades de datos, la herramienta de rastreo se implementaría sobre una infraestructura de Big Data compuesta por los siguientes componentes:

- **Hadoop (HDFS, HBase, YARN, MapReduce)**: Se utilizaría un clúster de Hadoop para ejecutar trabajos de rastreo y análisis. Esto permite escalar fácilmente para satisfacer necesidades futuras y soportar el almacenamiento y análisis de una gran cantidad de texto, imágenes y/o videos simplemente agregando hardware adicional.

- **Elasticsearch**: Para hacer que los datos sean buscables, la plataforma de rastreo realizará la indexación utilizando Elasticsearch, un motor de búsqueda de código abierto que tiene una arquitectura de sistema distribuido y se basa en la biblioteca Apache Lucene [118]. Elasticsearch proporciona una búsqueda de texto completo a través de una interfaz web siguiendo el modelo REST y utiliza archivos JSON para almacenar datos.

- **Nodos de Aplicación**: El nivel de aplicación de la plataforma está compuesto por varios componentes, como los rastreadores basados en Chrome [119], la API para búsqueda y gráficos, Elasticsearch para almacenar gráficos y el motor de rastreo y análisis. Todos ellos se ejecutan como contenedores Docker.

Esta sección ha abordado la implementación y funcionamiento de las herramientas de rastreo en PREVISION, destacando su importancia en la recolección de datos de fuentes abiertas y en la mejora de las capacidades de análisis de las LEAs.

Tráfico, telecomunicaciones y fuentes de datos financieros

El sistema PREVISION se espera que analice flujos de información heterogénea masiva, incluyendo datos de sistemas de tráfico vial, fuentes de datos de telecomunicaciones y redes, y sistemas de transacciones financieras. La recolección de esta enorme cantidad de datos debe ser rápida y segura. Por esta razón, la herramienta que se implementará será *Extract, transform and load* (ETL) [120], ya que es la tecnología más capaz de realizar dicha ingestión y transformación de datos y cargarlos en un conjunto de datos homogéneo.

Los expertos evaluaron el rendimiento de diversas opciones como *Node-Red*[121], *Apache Nifi*[122] y *Talend*[123], y concluyeron que *Node-Red* es la mejor opción de ETL para PREVISION, ya que fue el ETL que consumió la menor cantidad de recursos del sistema.

Cada una de las fuentes de datos utilizadas en PREVISION necesitará una conexión individual con el ETL, por ejemplo, una conexión para el conjunto de datos de tráfico, otra para el conjunto de datos de telecomunicaciones, otra para el conjunto de datos financieros, etc. El ETL abrirá la conexión al conjunto de datos, necesitando conocer detalles mínimos como la dirección del repositorio, el tipo de conjunto de datos y las credenciales de acceso. Luego, los datos se transformarán si es necesario y se cargarán en los siguientes módulos, estableciendo otra conexión con el siguiente componente.

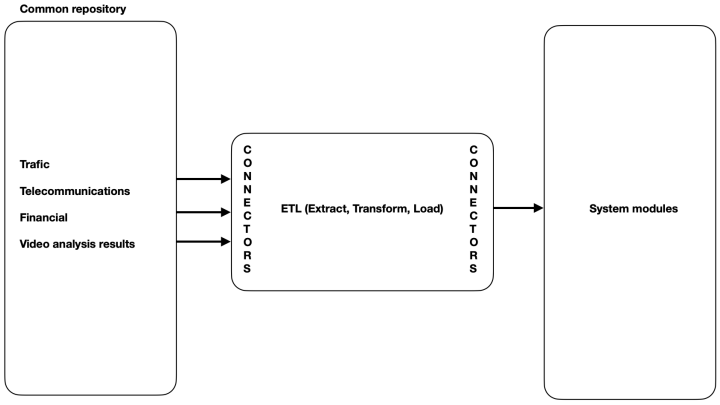

Figura 5.3: Flujo de herramientas ETL

Las etapas del proceso ETL son:

- **Extracción**: Esta fase implica establecer conexiones con el repositorio común o las fuentes de datos externas y extraer los datos proporcionados por los proveedores de datos. La sesión permanecerá abierta mientras el ETL específico de los datos esté en funcionamiento. Los archivos se leerán línea por línea para extraer los campos necesarios para los procesos subsiguientes. Actualmente, no se ha decidido si los archivos procesados se eliminarán o se moverán a un repositorio diferente.

- **Transformación**: Cuando sea necesario, los datos se transformarán o preprocesarán para verificar su integridad y calidad. El tipo de transformaciones que se pueden realizar aún no está definido. Algunos ejemplos de transformaciones incluyen la gestión de valores nulos, agregaciones o definiciones de curación. Al final de esta fase, los datos procesados estarán listos para la siguiente fase, la carga en la base de datos de PREVISION.

- **Carga**: En esta fase, el ETL cargará los datos transformados en el siguiente módulo, un *Procesador de eventos complejos* (CEP), que procesará los datos y almacenará el mínimo de datos considerados necesarios, rentables y útiles. En caso de que no se apruebe el uso de un CEP, el ETL cargará los datos en la base de datos o almacén de datos de PREVISION para que los siguientes módulos los analicen. La operación de carga para enviar los datos procesados a la base de datos de destino requerirá el uso de un conector específico de la base de datos. Aunque las decisiones técnicas

respecto al sistema de almacenamiento aún no se han tomado, se espera que no haya problemas en cuanto a los conectores.

Esta sección ha descrito el proceso ETL dentro de PREVISION, destacando su importancia en el manejo eficiente de grandes volúmenes de datos y en la preparación de estos para análisis y procesamiento posteriores.

Análisis de vídeo e imágenes en pseudo tiempo real

En la actualidad, una cantidad masiva de datos visuales se genera diariamente a través de diversas fuentes como cámaras, smartphones, UxVs y CCTV, entre otros. Estos datos visuales heterogéneos serán gestionados por las herramientas visuales de PREVISION para detectar, analizar y extraer información de interés. Con este fin, se han desarrollado cuatro herramientas discretas capaces de analizar las diversas fuentes de datos y proporcionar a las LEAs capacidades para un análisis más rápido y preciso de los mencionados flujos de datos. El objetivo de cada herramienta es realizar un análisis, considerando los datos visuales que han sido previamente extraídos o transmitidos por cámaras CCTV, para extraer detecciones/predicciones que posteriormente podrían ser reenviadas.

Herramienta de Detección de Comportamiento Anómalo

Esta herramienta es capaz de procesar y analizar continuamente contenido visual (videos, transmisiones de video) y extraer las actividades detectadas. Además, los usuarios finales podrían filtrar las actividades detectadas. Específicamente, la *Anomalous Behavior Detection* (ABD) toma como entrada un video o flujo visual y después de procesarlo, genera un archivo que incluye las actividades detectadas y la puntuación de detección para cada actividad a lo largo del tiempo.

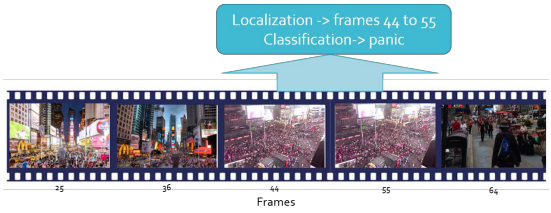

Figura 5.4: Representación de alto nivel del módulo de detección de comportamientos anómalos

Herramienta de Detección y Reconocimiento Facial

Esta herramienta es responsable de procesar flujos visuales y contenido visual en general para: 1) Identificar personas/vehículos presentes en el contenido visual y 2) reconocer los rostros detectados realizando una medida de similitud visual con los rostros almacenados en la base de datos. La salida generada de este subcomponente incluirá las coordenadas de los rostros detectados, la marca de tiempo en caso de videos, y si se aplica el proceso de reconocimiento, los identificadores de los rostros devueltos.

Herramienta de Identificación de Personas y Vehículos

Esta herramienta podrá detectar y reconocer personas y vehículos. Específicamente, la *Person and vehicle identification* (PVI) detectará personas y vehículos a partir de flujos de video y los reconocerá (cuando sea posible) realizando una comparación con los datos almacenados. El objetivo de este servicio es detectar figuras de personas/vehículos capturadas por diferentes cámaras CCTV o provenientes de UxVs. Además, los usuarios finales podrán realizar una búsqueda basada en atributos usando atributos predefinidos como altura, color de cabello, ropa, etc. La salida generada de esta herramienta será los atributos, en caso de búsqueda usando atributos, la lista clasificada de identificadores de los objetos recuperados y las puntuaciones correspondientes.

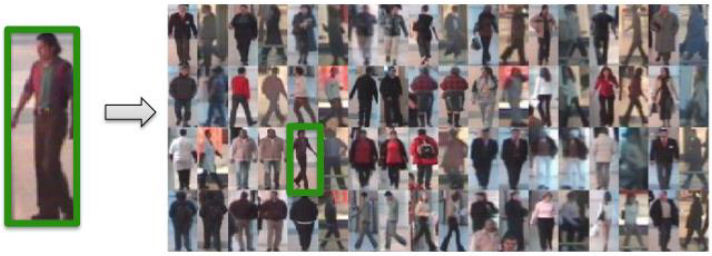

Figura 5.5: Representación de alto nivel del módulo de identificación de personas y vehículos

Herramienta de Detección de Eventos de Crisis

Esta herramienta es responsable de detectar eventos de crisis como incendios, humo e inundaciones a partir de contenido visual. El módulo realizará un análisis visual para investigar la existencia de un evento de crisis (por ejemplo, fuego, humo, inundación, etc.) dentro del medio proporcionado. Para ello, la

herramienta realizará un análisis de textura dinámica para primero detectar y posteriormente identificar el tipo de evento de crisis. El resultado de esta acción se describirá con la marca de tiempo del evento y el tipo de evento detectado.

Este análisis destaca su capacidad para manejar y procesar una gran variedad de datos visuales, proporcionando herramientas esenciales para la detección y el análisis de eventos y actividades relevantes para las LEAs.

Análisis de datos de la Darknet, la Web y las redes sociales

Los datos rastreados, recopilados con la ayuda de la herramientas desarrolladas, se analizan y procesan antes de ser indexados y estar listos para su uso. Como resultado de este análisis, se crean uno o varios conjuntos de datos indexados, dependiendo de las necesidades de los usuarios. La información extraída podría incluir:

- Direcciones de Bitcoin y números IBAN encontrados en documentos.
- Ubicaciones geográficas de los servidores que distribuyen las páginas seleccionadas.
- Ubicaciones geográficas de imágenes en un mapa (en caso de que estén disponibles datos EXIF [124]).
- Modelos de cámaras utilizados para tomar imágenes (en caso de que estén disponibles datos EXIF).
- Hashes de imágenes.
- Posibles identificadores como nombres de usuario, direcciones de correo electrónico, números de teléfono y claves *Pretty Good Privacy* (PGP) [125].
- Coincidencias con palabras clave predefinidas y disparadores.
- Marcas de tiempo.

Este análisis exhaustivo permite a PREVISION transformar los datos rastreados en información valiosa y utilizable, mejorando significativamente las capacidades de investigación y análisis de las LEAs. La indexación de estos datos facilita búsquedas rápidas y efectivas, permitiendo a los usuarios finales acceder y utilizar la información relevante de manera eficiente.

Análisis de datos de las redes sociales

En el contexto de PREVISION, se recolectarán, agregarán y analizarán los contenidos producidos en las redes sociales en línea para asistir a las LEAs en sus actividades cotidianas. Hacia este objetivo, se explotarán los últimos avances en técnicas de inteligencia artificial para realizar diversas tareas analíticas. Específicamente, el análisis de datos de redes sociales evolucionará para descubrir comunidades de usuarios basadas en interacciones en línea, para luego emplear métodos de identificación de actores clave para identificar jugadores importantes dentro de dichas comunidades. Además, los usuarios en línea que buscan difundir material ilegal (por ejemplo, contenido extremista) tienden a crear múltiples cuentas para eludir y adelantarse a las medidas de combate aplicadas por los administradores de redes sociales (por ejemplo, suspensiones de cuentas). Por lo tanto, dentro de PREVISION se desarrollará un mecanismo de resolución de identidad de actores que será responsable de detectar cuentas de usuario que probablemente pertenezcan a la misma persona natural para detener la propagación de comportamientos criminales y/o relacionados con el terrorismo a gran escala.

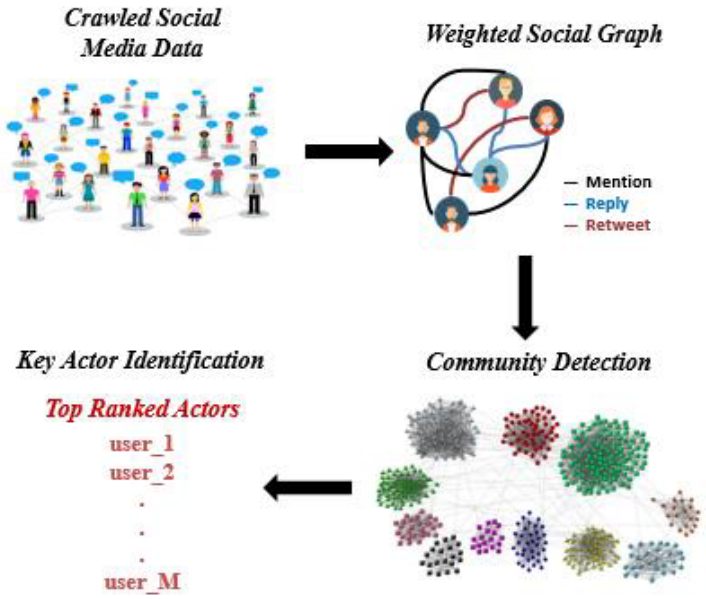

Figura 5.6: Flujo de detección de comunidades e identificación de actores clave

Centrándose en la detección de comunidades y la identificación de actores clave, la Figura 5.6 ofrece una visión general del flujo de trabajo que se seguirá dentro de PREVISION para detectar comunidades de usuarios relevantes para los dominios de PREVISION, así como actores clave. Como se presenta en la Figura 5.6, se emplearán los siguientes pasos:

- Construcción de un grafo social ponderado basado en varios tipos de relaciones derivadas de interacciones usuario-usuario o usuario-publicación;
- Identificación de grupos de usuarios (es decir, comunidades) que estén más densamente conectados entre sí que el resto de la red;
- Identificación de actores clave basada en medidas de centralidad de última generación.

Por lo tanto, la salida de este componente será una lista de actores clave (cuentas de usuario) para cada comunidad ya identificada.

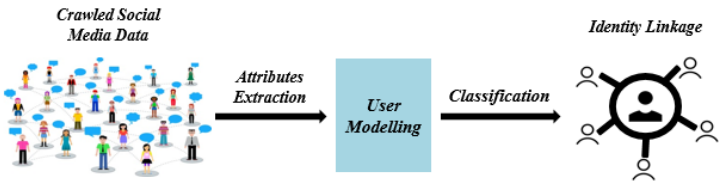

Figura 5.7: Flujo de resolución de identidades de actores

De manera similar, la Figura 5.7 ofrece una visión general del flujo de trabajo que se seguirá para detectar cuentas que probablemente pertenezcan a la misma persona natural. Se emplearán los siguientes pasos:

- Extracción de varios atributos (por ejemplo, perfil, contenido/lingüístico y basado en la red) del contenido de redes sociales rastreado;
- Modelado de usuarios que implica el modelado del comportamiento de cada cuenta en línea individual basada en los atributos ya extraídos;
- Detección de cuentas que posiblemente pertenezcan a la misma persona natural (a través de la clasificación).

En general, la salida de este componente será un conjunto de cuentas de usuario vinculadas (es decir, cuentas que probablemente pertenezcan a la misma persona).

Análisis lingüístico exhaustivo

Utilizando como datos de entrada la información generada a partir de los módulos de rastreo, así como interfaces con otras fuentes externas, el módulo de análisis lingüístico profundo generará múltiples características lingüísticas que serán utilizadas en análisis posteriores. El servicio de minería de textos de PREVISION es responsable de extraer información de texto puro en idioma inglés e instanciar nuevo conocimiento basado en esta información extraída en un almacén semántico.

Además, se proporcionará un componente de extracción de conocimiento como parte de los servicios lingüísticos.

5.3.2. Módulo de aprendizaje y capacidades cognitivas automáticas

Procesamiento de información semántica

El razonamiento en el sistema PREVISION constituye un proceso avanzado que permite incorporar semánticas complejas y enriquecidas a los conjuntos de datos. Este proceso es fundamental para el sistema, ya que facilita la recopilación automática y la utilización de información de mayor profundidad y relevancia. De manera específica, el razonamiento lógico en PREVISION juega un papel clave en la identificación y descubrimiento de hechos derivados que no están explícitamente representados en la base de conocimientos. Además, este proceso es esencial para descubrir y establecer nuevas conexiones y relaciones entre diversos objetos y elementos de datos, ampliando así el alcance del conocimiento existente.

Un componente central en este proceso es el razonador, una herramienta de software sofisticada diseñada para inferir consecuencias lógicas a partir de hechos conocidos, en línea con los axiomas establecidos por la ontología del sistema. Este razonador no solo evalúa la validez y la coherencia de los axiomas en sí, sino que también verifica su completitud y consistencia. Integrado plenamente en el sistema PREVISION, el razonador tiene la capacidad de sintetizar nuevos conocimientos a partir de los hechos ya existentes en la base de conocimientos. Esta capacidad de inferencia se nutre de datos recogidos de todas las entidades implicadas en el entorno de PREVISION, convirtiéndose en un elemento crucial para el análisis y la investigación de delitos.

El módulo de razonamiento de PREVISION se destaca por su técnica de razonamiento semántico, orientada a enriquecer la información existente y descubrir nuevos conocimientos y conexiones entre distintos objetos y elementos de datos. Esta técnica se basa en el uso de *Markov logical network* (MLN) [126], una metodología avanzada que combina los principios del modelado gráfico

probabilístico con la lógica de primer orden, permitiendo así un razonamiento probabilístico efectivo. Para que el razonador funcione de manera óptima y pueda inferir nuevos axiomas a partir de los axiomas explícitamente afirmados en la ontología, es imprescindible proporcionarle un conjunto de reglas bien definidas. Estas reglas se estructuran en forma de implicaciones lógicas, donde un antecedente (cuerpo) conduce a un consecuente (cabeza), estableciendo un marco lógico riguroso para el análisis y la deducción de nuevas inferencias.

En conclusión, el razonamiento en PREVISION representa un enfoque integral y avanzado para el análisis de datos, vital para la exploración y expansión del conocimiento dentro del sistema, y juega un papel decisivo en el fortalecimiento de las capacidades de análisis y de investigación de crímenes del sistema.

Fusión inteligente y tratamiento de datos

Los documentos NoSQL están especialmente diseñados para cargar y gestionar de manera eficiente colecciones masivas de documentos heterogéneos sin una validación estructural previa. Esta flexibilidad se convierte en un desafío serio al consultar documentos heterogéneos, ya que el usuario debe construir consultas complejas para tener en cuenta los diversos esquemas (heterogeneidad de datos). Además, el usuario debe reformular las consultas existentes cada vez que se insertan nuevos esquemas en una colección. El componente de consulta independiente del esquema tiene como objetivo consultar colecciones heterogéneas en almacenes de documentos NoSQL como MongoDB. Automatiza el proceso de reformulación de consultas mediante un conjunto de reglas que reformulan la mayoría de los operadores de almacenamiento de documentos (seleccionar, proyectar, desenrollar, agregar y buscar). El componente produce entonces consultas a través de documentos multi-estructurados, compatibles con el motor de consulta nativo (MongoDB) del almacén de documentos subyacente.

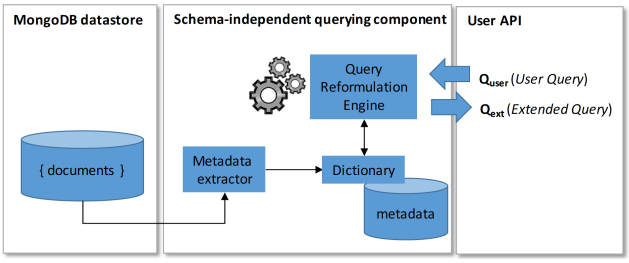

Figura 5.8: Flujo de componentes de consulta independiente del esquema

El componente de consulta independiente del esquema se organiza en dos etapas (mostradas en la Figura 5.8):

- El extractor de metadatos extrae de un almacén de datos MongoDB las estructuras de datos de las colecciones de documentos. Enriquece el diccionario con referencias a todos los caminos existentes y su derivación, inducidos por la heterogeneidad estructural en las colecciones. El diccionario se actualiza periódicamente de acuerdo con los cambios en los documentos (actualizaciones, eliminaciones o inserciones) en las colecciones.
- En la etapa de consulta, el motor de reformulación de consultas toma como entrada la consulta del usuario, denominada Quser, que se formula a través de cualquier combinación de atributos de documentos multi-estructurados. El motor de reformulación de consultas lee los metadatos del diccionario y produce una consulta enriquecida, denominada Qext, que incluye todos los caminos absolutos existentes en todos los documentos. Finalmente, la consulta enriquecida puede enviarse al almacén de documentos MongoDB.

Las funcionalidades del componente de consulta independiente del esquema son:

- Extraer periódicamente estructuras de datos de colecciones de documentos heterogéneos,
- Almacenar metadatos que describen documentos heterogéneos,
- Generar consultas de usuario reformuladas según cualquier combinación de atributos de los documentos heterogéneos almacenados.

Para reescribir una consulta de usuario, el motor de reformulación de consultas admite varios operadores de consulta del lenguaje de consulta MongoDB: selección, proyección, agregación y desenrollar. Cada consulta de usuario se descompone internamente en una combinación de estos operadores. Cada operador se reescribe según los documentos multi-estructurados; los operadores se componen luego para producir la consulta enriquecida que el componente proporciona como salida.

Pruebas basadas en AI

El módulo de estimación de densidad de probabilidad y predicción en PREVISION representa una herramienta avanzada para el análisis y modelado de patrones delictivos. Utilizando una nube de puntos avanzada, cada punto,

representando un incidente criminal, se etiqueta con una categoría específica de delito y se asocia con una marca de tiempo precisa. Estos puntos están geográficamente codificados con coordenadas de longitud y latitud, ofreciendo una representación espacial detallada de los incidentes. Este enfoque se utiliza primordialmente para identificar y analizar los puntos calientes de criminalidad en una región determinada a lo largo del tiempo, lo que permite una asignación estratégica de recursos, como el despliegue de patrullas policiales en áreas críticas.

El análisis de tendencias temporales y la detección de patrones emergentes son fundamentales en este módulo. Al acumular un volumen significativo de datos a lo largo del tiempo, el módulo utiliza algoritmos avanzados para revelar tendencias y movimientos de estos puntos calientes, proporcionando predicciones fundamentadas sobre la evolución futura de la criminalidad. Además, este módulo incorpora técnicas predictivas sofisticadas que se basan en observaciones históricas para estimar la densidad de probabilidad de futuros incidentes delictivos, lo que permite una planificación proactiva y la prevención de delitos.

El componente de Árbol de Decisión en PREVISION introduce una metodología de clasificación de datos basada en principios de aprendizaje automático y análisis de datos avanzados. Este componente es alimentado por conjuntos de entrenamiento específicos proporcionados por el usuario, los cuales contienen valores de clase y datos representativos. La tarea principal del componente es clasificar eficientemente conjuntos de datos nuevos y no etiquetados en categorías predeterminadas, basándose en los patrones aprendidos de los conjuntos de entrenamiento.

El resultado de este proceso es doble: por un lado, se obtienen conjuntos de datos clasificados de manera precisa, y por otro, se genera un árbol de decisión explicativo. Este árbol de decisión actúa como una herramienta interpretativa, ofreciendo una visión clara y lógica de cómo se han tomado las decisiones de clasificación, lo que es esencial en aplicaciones donde la transparencia y la explicabilidad son cruciales. El componente maneja una variedad de operadores de consulta del lenguaje de MongoDB, incluyendo selección, proyección, agregación y desenrollado, lo que le permite descomponer y reformular internamente las consultas de usuario en una serie de operaciones lógicas, adaptándose así a la estructura multifacética de los documentos y datos almacenados.

Esta versión avanzada del módulo y del componente en PREVISION pone de relieve su capacidad para manejar y analizar grandes conjuntos de datos complejos, proporcionando herramientas esenciales para la toma de decisiones informadas y basadas en datos en el ámbito de la seguridad y la prevención del crimen.

Analíticas predictivas y análisis de modelos

El módulo de predicción de difusión de información en redes sociales online se centra en el análisis y la modelización de la propagación de información, especialmente en el contexto de la detección de actividades criminales en redes sociales. Modelar la difusión de información en estos medios de comunicación en crecimiento es crucial tanto para comprender la propagación de información como para controlarla mejor. Nuestro módulo tiene como objetivo predecir si un mensaje de Twitter [127] será difundido o no, y el nivel de dicha difusión.

El modelo se basa en técnicas de aprendizaje automático, utilizando un algoritmo de aprendizaje supervisado para predecir la popularidad de los mensajes en redes sociales (inicialmente desarrollado para tweets, luego extendido a otros formatos), medida por el número de reposts futuros. Para predecir la popularidad de las publicaciones, estas se clasifican en:

i) **Clasificación binaria:** para predecir si una publicación será reenviada o no, se clasifica en dos clases: '0' (no reenviada) y '1' (reenviada).

ii) **Clasificación multiclase:** para predecir el nivel de difusión, las publicaciones se clasifican en cuatro clases: '0' (no reenviada), '1' (reenviada de 1 a 100 veces), '2' (reenviada de 101 a 10,000 veces), '3' (reenviada más de 10,000 veces).

En nuestro modelo, las publicaciones se representan mediante características que incluyen:

- **Características basadas en el usuario** (valores numéricos): total de publicaciones anteriores, número de seguidores y seguidos, antigüedad de la cuenta, número de favoritos, número de grupos participantes, promedio de publicaciones por día, promedio de favoritos por día, longitud del nombre del usuario.

- **Características basadas en el tiempo** (valores binarios): si una publicación se hizo al mediodía, en la tarde, durante el fin de semana o en días festivos.

- **Características basadas en el contenido** (binarias o numéricas): si contiene ubicación, programa de *Television* (TV), organización, imagen, video, número, exclamación, sugerencia de retweet, *Uniform Resource Locator* (URL) [128], hashtag, longitud del texto, tiene longitud óptima.

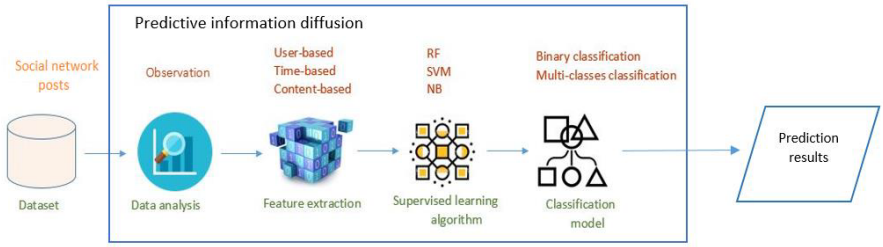

Figura 5.9: Flujo del modelo de difusión de información predictiva

Se utiliza un conjunto de entrenamiento para aprender el modelo antes de aplicarlo en el conjunto de prueba o en nuevas publicaciones. El flujo del modelo se describe en la Figura 5.9.

Las funcionalidades del módulo predictivo de difusión de información incluyen:

- Aprender el modelo en un conjunto de entrenamiento.
- Clasificar publicaciones de otro conjunto.
- Predecir la popularidad de nuevas publicaciones, ya sea de manera binaria o de forma más detallada.

Para predecir la popularidad de los mensajes, utilizamos técnicas como:

- **Librerías de Python:** Las características representativas de los mensajes o publicaciones se extraen mediante un programa escrito en Python [129], utilizando varias librerías como *time*, *holiday*, JSON, *scikit-learn* [130], etc.
- **Algoritmos de aprendizaje supervisado:** Para clasificar las publicaciones en clases, utilizamos varios algoritmos de aprendizaje supervisado como Naive Bayes [131], Máquina de Soporte Vectorial [132] y Bosque Aleatorio [133], implementados en la biblioteca Java Weka [134].

Detección de anomalías y comportamientos multivariantes

En el ámbito de PREVISION, los oficiales de la LEA enfrentan el desafío de gestionar y analizar grandes volúmenes de datos heterogéneos en sus tareas diarias. Para abordar esta complejidad, PREVISION implementará una serie de servicios avanzados que dotarán a los oficiales de LEA con capacidades automatizadas y sofisticadas para detectar cambios de comportamiento, anomalías,

y valores atípicos. Estas herramientas también están diseñadas para identificar señales débiles y cambios tempranos que podrían indicar la emergencia de nuevas tendencias. Utilizando técnicas de aprendizaje automático aplicadas a los datos recopilados, estas herramientas realizarán un análisis conductual multivariante, crucial para la detección de anomalías y la identificación de nuevas tendencias emergentes. Los resultados obtenidos serán fundamentales para mejorar la conciencia operacional y situacional de los oficiales de LEA.

El análisis de asociación y correlación constituye un pilar central en este conjunto de herramientas, con el objetivo de descubrir conexiones intrincadas entre diversas características presentes en los conjuntos de datos. Esta capacidad de análisis es esencial para comprender las complejas interacciones y relaciones subyacentes en los datos relacionados con la seguridad.

Por otro lado, el análisis de clustering facilitará la agrupación de instancias de datos en grupos que compartan similitudes ocultas. Esta funcionalidad es particularmente valiosa para identificar patrones y tendencias que no son inmediatamente evidentes para un analista humano, permitiendo así una comprensión más profunda de los datos.

La identificación de patrones, incluyendo el uso de algoritmos de regresión y clasificación, será otra característica clave de estas herramientas. Estos modelos se enfocarán en descubrir patrones y regularidades ocultas en los datos, lo que es vital para anticipar y responder a las dinámicas delictivas y de seguridad.

El análisis de patrones frecuentes jugará un papel crucial en la identificación de eventos o crímenes que presenten asociaciones. Este aspecto del análisis proporcionará insights sobre la secuencia y la probabilidad de ocurrencia de ciertos eventos o crímenes, basándose en la ocurrencia previa de otros.

Finalmente, el análisis de valores atípicos permitirá la detección de comportamientos anómalos y no esperados basándose en la situación actual descrita por los datos. Esta función es especialmente crítica para identificar amenazas emergentes o actividades inusuales que podrían pasar desapercibidas sin un análisis profundo.

En conjunto, estas herramientas integrarán y aplicarán metodologías avanzadas de análisis de datos y modelos predictivos. Esta integración permitirá a los oficiales de LEA no solo un entendimiento más profundo de los datos a su disposición, sino también una capacidad mejorada para responder de manera efectiva a las diversas situaciones de seguridad y crimen que enfrentan en su trabajo cotidiano.

5.3.3. Análisis de Herramientas de Conciencia Situacional para su Uso en la Plataforma PREVISION

En el desarrollo de la plataforma PREVISION, se ha llevado a cabo un análisis exhaustivo de diversas herramientas de conciencia situacional. Este análisis tiene como objetivo identificar y evaluar las herramientas más adecuadas que pueden ser integradas en la plataforma para mejorar la eficiencia y efectividad de los procesos de toma de decisiones de los oficiales de LEA. La conciencia situacional es crucial en el ámbito de la seguridad y la aplicación de la ley, ya que permite a los oficiales comprender y anticipar eventos en su entorno operativo, basándose en la recopilación y análisis de datos en tiempo real.

Las herramientas seleccionadas para análisis abarcan un amplio espectro de funcionalidades, incluyendo, pero no limitándose a, la visualización avanzada de datos, el seguimiento en tiempo real de eventos y actividades, el análisis predictivo y la modelización de escenarios, y la integración de múltiples fuentes de datos para una perspectiva holística. Estas herramientas están diseñadas para proporcionar a los usuarios una comprensión profunda de su entorno operativo, facilitando así la identificación rápida de patrones, anomalías y tendencias emergentes.

El análisis se centra en evaluar la capacidad de cada herramienta para integrarse de manera efectiva en la infraestructura existente de PREVISION, su facilidad de uso, escalabilidad, y cómo pueden contribuir a mejorar los procesos de toma de decisiones. Además, se consideran aspectos como la seguridad de los datos, la privacidad y el cumplimiento normativo, que son de suma importancia en el contexto de la aplicación de la ley.

Este análisis detallado es un paso crucial en el desarrollo de PREVISION, asegurando que la plataforma esté equipada con las herramientas más avanzadas y efectivas para mejorar la conciencia situacional de los oficiales de LEA, lo que a su vez mejora su capacidad para responder a situaciones de seguridad de manera rápida y efectiva.

Herramientas para el conocimiento operativo y situacional

En PREVISION, el diseño de la HMI se aborda con un enfoque modular y detallado, enfatizando la flexibilidad y la eficiencia. Este enfoque permite una adaptación y expansión fluidas de la interfaz en respuesta a las necesidades cambiantes y la integración de nuevas herramientas y funcionalidades. La HMI se estructura en componentes modulares clave para una interacción intuitiva y eficiente:

1. **Área de Navegación Principal:** Basada en un diseño de navegación con pestañas, esta área permite a los usuarios seleccionar rápidamente

entre las diversas herramientas disponibles en PREVISION, proporcionando una interfaz de usuario clara y accesible.

2. **Área de Submenú:** Aquí, los usuarios pueden elegir entre las funciones preferidas de una herramienta seleccionada, permitiendo un acceso rápido a funcionalidades específicas y una personalización de la experiencia del usuario.
3. **Área de Componentes:** Es el espacio dedicado a la visualización y manejo de las funciones seleccionadas. Esta área puede subdividirse para incluir tanto una zona de navegación adicional como un espacio principal para la interacción directa con los datos y herramientas.
4. **Caja de Notificaciones:** Diseñada para mostrar notificaciones personalizadas y alertas, esta sección juega un papel crucial en mantener a los usuarios informados sobre eventos críticos o actualizaciones en tiempo real.

Funciones adicionales como autenticación de usuarios, ajustes de configuración y alertas de sistema se ubican de manera estratégica en la parte superior de la HMI para garantizar un acceso fácil y rápido.

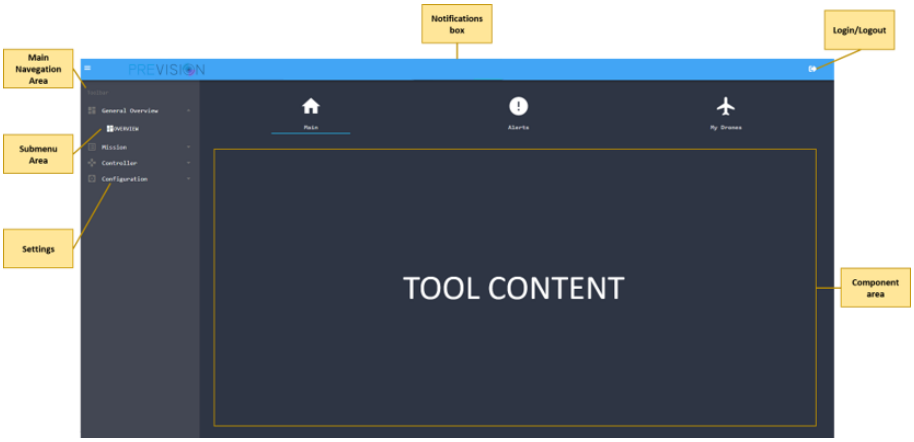

Figura 5.10: Mockup de distribución de la pantalla principal

Integración Avanzada de Web GIS y Dispositivos Hápticos en PREVISION

El Web-GIS en PREVISION se centra en una representación avanzada y enriquecida de datos geoespaciales. Utilizando un motor GIS 3D de múltiples

capas, esta herramienta visualiza información georreferenciada y datos procedentes de diversas fuentes, mejorando significativamente la conciencia situacional de los usuarios.

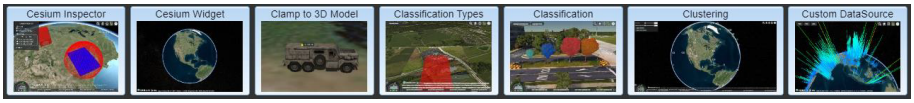

Figura 5.11: Capacidades CESIUM

La integración de un dispositivo háptico, como LEAP Motion [135], ofrece una experiencia de usuario profundamente inmersiva y natural, permitiendo una interacción intuitiva con los datos geoespaciales a través de movimientos y gestos manuales. Esta sinergia entre el Web-GIS y la tecnología háptica abre nuevas posibilidades para la navegación y el análisis de datos en un entorno virtual tridimensional.

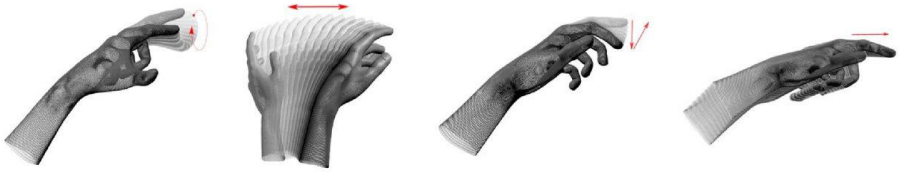

Figura 5.12: Gestos de círculo, barrido, toque de tecla y toque de pantalla con el controlador LEAP Motion

Innovaciones en Visualización de Realidad Virtual (VR) para PREVISION

La adopción de técnicas de visualización inmersiva como la VR representa un avance significativo en la representación y análisis de datos en el campo de la seguridad. La VR facilita la visualización de gráficos y estructuras de datos tridimensionales en un entorno envolvente, mejorando la capacidad del usuario para interactuar y comprender complejas estructuras de datos. Los dispositivos VR varían desde sistemas conectados físicamente a PCs hasta soluciones móviles integradas y dispositivos VR independientes, ofreciendo un espectro de posibilidades para diferentes aplicaciones y necesidades de usuario.

	VR atada (tethered)	VR móvil
Ventajas	- Movimiento de muy alta precisión (6 grados de libertad). - Mejor fidelidad de imagen.	- Mayor comodidad y libertad de movimiento (3 grados de libertad). - No se requiere hardware adicional.
Desventajas	- Menor comodidad. - Requiere equipo de alto nivel. - Precios altos (600-800$)	- Seguimiento de movimiento menos preciso. - Calidad de imagen reducida.
Productos	- Oculus Rift (Xbox y controladores de mano) - HTC Vive (Controladores de mano)	- Samsung Gear VR (Trackpad) - Google Daydream (Movimiento) - Google Cardboard (Botón)

Tabla 5.1: Comparación entre VR Atada y VR Móvil

La integración de soluciones GIS con dispositivos VR, como Oculus Rift, a través de desarrollos específicos o plugins, permite a los usuarios de PREVISION explorar y analizar datos en un entorno virtualmente realista. Además, la colaboración con plataformas como Unity facilita la creación de entornos inmersivos personalizados para una navegación y análisis de datos más intuitivos y efectivos.

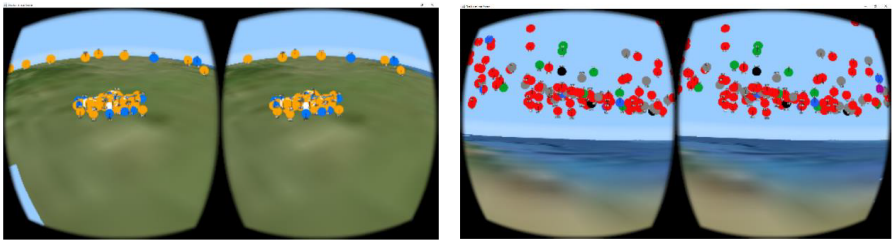

Figura 5.13: Ejemplos de visualización inmersiva

Estos desarrollos representan un paso crucial en la evolución de PREVISION, mejorando no solo la interacción del usuario con la plataforma, sino también proporcionando herramientas avanzadas para el análisis y la toma de decisiones en el campo de la seguridad y la aplicación de la ley.

5.3.4. Identificación de Procesos de Radicalización y Propaganda Terrorista en la Comunicación Online

La identificación de procesos de radicalización y propaganda terrorista en la comunicación online es un objetivo importante de PREVISION. La enorme cantidad de datos proporcionados por sitios web y la comunicación online en redes sociales, blogs y salas de chat representa un gran desafío para las agencias de aplicación de la ley. Por esta razón, a menudo se utilizan instrumentos de análisis y seguimiento automatizados para gestionar la evaluación y el análisis de estos datos.

Un enfoque prometedor es el uso de instrumentos basados en palabras clave. Con su ayuda se pueden identificar sitios web radicales y propaganda terrorista en internet, especialmente en redes sociales [136]. Los algoritmos se basan en listas de palabras clave y suponen que los sitios web en los que se discute contenido radical a menudo están vinculados entre sí o establecen una conexión con el tiempo y forman una especie de comunidad virtual. Se pueden utilizar listas de palabras predefinidas, que pueden ser complementadas por bases de datos léxicas para evitar la exclusión de términos relevantes debido al uso de catálogos de palabras clave estáticamente predefinidos.

Además de la identificación de contenido radical en sitios web, el uso de herramientas basadas en palabras clave permite la evaluación del riesgo de individuos o grupos basada en su comportamiento online. De esta forma, la comunicación de un individuo puede proporcionar información sobre el riesgo individual que emana de él o ella: 'Diferentes señales podrían ser [...] los términos relevantes de ciertos ámbitos políticos [...], pero también formulaciones que suenan violentas [...] o una expresión que enfatiza la diferencia con otros grupos sociales [...]'.

Sin embargo, en este contexto, cabe señalar que la identificación de personas (posiblemente) relevantes basada en análisis de palabras clave puede ser problemática. Si, por ejemplo, ciertos actores se refieren a enlaces o artículos con contenido extremista o radical en su comunicación online, esto puede ser una expresión tanto de actitudes negativas como positivas hacia este contenido. Un enfoque exclusivo en el nivel lingüístico de tales corrientes de comunicación puede conducir a errores.

Además de la calidad de la comunicación, los enfoques basados en palabras clave también deben permitir considerar la cantidad de lo que se comunica. Si individuos o grupos expresan fantasías concretas de violencia o intenciones de cometer delitos, posiblemente varias veces, aumenta el riesgo de actos concretos de violencia. Si la comunicación en redes sociales se interrumpe, también se pue-

de asumir un riesgo aumentado. Información de este tipo representa enfoques concretos de investigación para las agencias de aplicación de la ley.

La información sobre la calidad y cantidad de contenido radical en sitios web y la comunicación radical de individuos permite el cálculo de puntuaciones de riesgo. Esto debería incluir una clasificación de sitios web y personas según su potencial peligro para la sociedad en 'potencial de riesgo bajo', 'potencial de riesgo medio' y 'potencial de riesgo alto'.

Los catálogos de palabras clave en diferentes idiomas son indispensables para una monitorización nacional y completa de la comunicación online para identificar contenido radical y propaganda terrorista; por ejemplo, el fenómeno del terrorismo islamista requiere el uso de catálogos de palabras clave en árabe. En el contexto de PREVISION, se recomienda utilizar catálogos de palabras clave en inglés durante un período de prueba.

Además de la variación del idioma, también se debe tener en cuenta la variación del vocabulario de los comunicadores. En el contexto de la comunicación dinámica en plataformas de redes sociales, blogs, etc., los términos están en constante modificación o se utilizan expresiones completamente nuevas. Una forma de abordar este problema en el contexto del monitoreo online 'es utilizar técnicas de aprendizaje automático no supervisadas que pueden aprender a identificar términos semánticamente similares en los datos simplemente leyendo grandes cantidades de texto'. También se debe tener en cuenta que la comunicación en redes sociales es contenido generado por los usuarios, que puede ser no estructurado y gramaticalmente incorrecto y puede contener errores de ortografía, lenguaje coloquial, abreviaturas o emoticonos. Además, el lenguaje de aquellas personas que están en redes radicales a menudo puede tener peculiaridades subculturales. Los instrumentos de reconocimiento de texto deben ser capaces de lidiar con estos desafíos y aprender ciertas ortografías o usos de términos en contextos específicos.

Además del análisis lingüístico de los datos en línea, el reconocimiento de imágenes, para determinar si existen imágenes radicales y/o símbolos criminales en sitios web o perfiles de redes sociales, puede ser de gran importancia para identificar la radicalización y la propaganda terrorista. Los algoritmos de análisis de imágenes pueden utilizarse, por ejemplo, después de análisis de redes. Si los individuos son identificados como miembros de una red radical a través del análisis de redes, los algoritmos de reconocimiento de imágenes pueden utilizarse para verificar esto, aplicando descriptores de imágenes para determinar imágenes radicales o símbolos de organizaciones terroristas, como el ISIS, en imágenes y videos en los perfiles de redes sociales de estos individuos.

En general, se puede decir que los rastreadores web, los módulos de reconocimiento de texto y los sistemas de reconocimiento de imágenes representan un valor añadido significativo para las agencias de aplicación de la ley para

la identificación de contenido radical, procesos de radicalización y propaganda terrorista en internet en general y en las redes sociales en particular. Estos métodos pueden implementarse utilizando inteligencia artificial, aprendizaje automático y aprendizaje profundo.

Lucha contra el tráfico ilícito y el blanqueo de dinero

La lucha contra el tráfico ilícito de bienes culturales requiere nuevas tecnologías para ayudar a las LEAs en el terreno y aumentar su confianza al enfrentarse con artefactos culturales.

En esta perspectiva, el equipo de PREVISION en el caso de uso desarrolló múltiples microservicios, como una herramienta de detección y reconocimiento automático de artefactos para analizar imágenes de objetos supuestamente ilícitos tomadas por las fuerzas policiales en búsquedas, incautaciones o controles aduaneros. Esta herramienta estará accesible como una aplicación en smartphones y tabletas.

Los servicios integran una capacidad de escaneo web para buscar a través de las numerosas páginas web de los comerciantes para detectar artefactos robados o elementos de listas rojas.

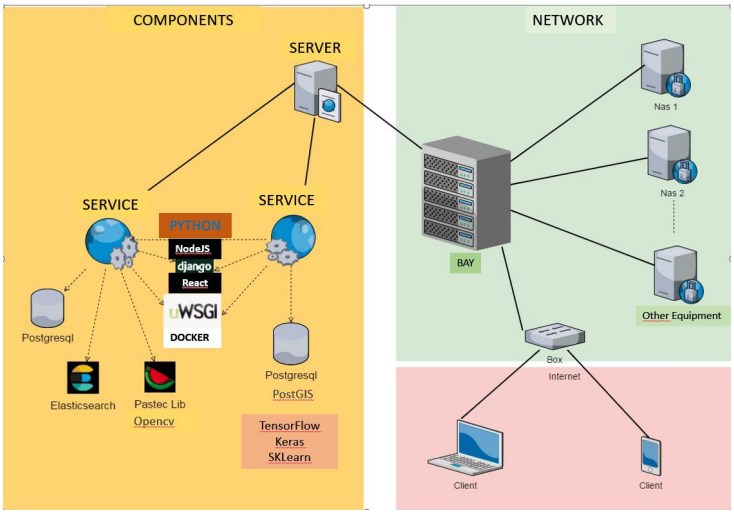

Figura 5.14: Organización de herramientas para el tráfico ilícito

Los servicios están respaldados por una base de datos que integra datos heterogéneos y los clasifica, normalizándolos en una clasificación *International*

Organization for Standardization (ISO) para objetos culturales conocida como *CIDOC Conceptual Reference Model* (CIDOC CRM) [137]. Esto con el fin de hacer coincidir el objeto con las categorías de la Lista Roja de artefactos. Una Base de Datos Central es necesaria para clasificar y organizar todos los datos bajo la misma norma y para reducir la velocidad de las consultas y el tiempo de respuesta.

El sitio web y el navegador accesibles para LEA se ha desarrollado de acuerdo con cada ventaja específica. Finalmente, los datos serán tratados en la base de datos bajo OBJECT ID y organizados con la ontología de objetos culturales bajo la norma ISO 21127 conocida como CIDOC CRM y adoptada por el *International Council of Museums* (ICOM) [138].

5.4. Logros de PREVISION

Durante su ejecución, el proyecto PREVISION ha alcanzado múltiples logros significativos, los cuales han contribuido a su éxito y a la mejora de las capacidades operativas de las LEAs. A continuación, se presentan algunos de los más destacados:

1. Implementación de una arquitectura robusta de microservicios que ha permitido una mayor flexibilidad y escalabilidad en las operaciones de las LEAs.

2. Desarrollo de algoritmos avanzados para el reconocimiento de patrones y la detección automática de actividades sospechosas en diferentes entornos y contextos.

3. Integración exitosa de sistemas de comunicación que aseguran la interoperabilidad entre dispositivos y plataformas, facilitando así una respuesta coordinada y eficiente.

4. Adopción de estándares de seguridad cibernética de vanguardia para proteger la integridad y confidencialidad de los datos críticos manejados por la plataforma.

5. Establecimiento de una infraestructura de base de datos centralizada que proporciona un acceso rápido y seguro a información relevante para la toma de decisiones.

6. Integración de sistemas UxV para la mejora de la captación de datos en el terreno.

7. Creación de interfaces de usuario intuitivas que permiten a los operadores de las LEAs interactuar de manera efectiva con la plataforma y sus herramientas analíticas.

8. Contribución al desarrollo de protocolos de entrenamiento y manuales de operación que mejoran la formación y preparación de los usuarios finales.

9. Avances significativos en el desarrollo de tecnologías de realidad virtual y aumentada para la visualización de datos y la simulación de escenarios complejos.

Estos logros reflejan el compromiso del proyecto PREVISION con la innovación tecnológica y su contribución continua a la seguridad y eficacia de las operaciones de las LEAs.

Capítulo 6

Evaluación de los sistemas

6.1. Introducción

Este capítulo de la tesis se dedica a llevar a cabo una evaluación exhaustiva de la arquitectura que se ha desarrollado e implementado en los proyectos CAMELOT y PREVISION, cuyos detalles se han descrito en los Capítulos 4 y 5. El enfoque se sitúa en la validación de los resultados obtenidos tras el desarrollo en estos proyectos, procediendo a un análisis detallado de su funcionalidad y eficacia.

En este capítulo, se examinarán los diferentes contextos y escenarios en los que se han efectuado las pruebas de cada caso de uso. Se expondrá el procedimiento operativo adaptado a las particularidades de cada contexto y, finalmente, se realizará una evaluación de los resultados, centrándose en la eficiencia y el impacto de las soluciones implementadas.

Adaptación y Desafíos en el Proyecto CAMELOT

El proyecto CAMELOT, enfocado en la gestión de misiones multidominio, afrontó retos únicos debido a las restricciones de la pandemia de COVID-19. Las evaluaciones en este proyecto se realizaron a través de demostraciones simuladas ejecutadas de forma remota, superando el desafío de llevar a cabo pruebas sin contacto físico. Este enfoque garantizó la continuidad y la calidad del proceso evaluativo y proporcionó una visión integral de las actividades desarrolladas durante el proyecto.

Evaluaciones Contextualizadas en el Proyecto PREVISION

En contraste, el proyecto PREVISION permitió la implementación y evaluación de los desarrollos en entornos controlados y situaciones simuladas en terreno. Esto posibilitó una evaluación más práctica y contextual de las aplicaciones en escenarios de amenaza real, brindando una valoración completa de la funcionalidad y la operatividad de las herramientas y sistemas desarrollados.

La evaluación de las arquitecturas implementadas en los proyectos CAMELOT y PREVISION representa un paso crítico para medir su eficacia y viabilidad. Este capítulo detalla cómo se adaptaron y evaluaron estas implementaciones en diferentes contextos, destacando tanto los desafíos como los éxitos logrados en cada uno de los proyectos.

6.2. CAMELOT

6.2.1. Entorno de pruebas

La verificación de la efectividad y aplicabilidad de la plataforma se ha efectuado utilizando el prototipo de arquitectura desarrollada en el Capítulo 3, la cual ha sido específicamente configurada para ajustarse a las necesidades del proyecto CAMELOT, tal como se detalla en el Capítulo 4. Para las pruebas, se eligió un ejercicio de simulación de una operación de vigilancia y control con dispositivos de varios dominios en la frontera portuguesa. La demostración implicó la implementación integral de los servicios de CAMELOT en la infraestructura *CLOUD* suministrada por la *Universidad Politécnica de Valencia* (UPV) [139]. En esta infraestructura *CLOUD*, se estableció un nodo central, crucial para permitir el intercambio de información relevante para la misión y las condiciones ambientales actuales entre todas las partes involucradas en la simulación. Este nodo central aseguró una coordinación efectiva y una respuesta rápida a la situación simulada.

Implementación de la Infraestructura

La infraestructura completa se estableció dentro del servidor de la Universidad, donde se virtualizaron todas las máquinas y servicios para crear un ambiente controlado y seguro. Esta medida se tomó para prevenir cualquier posible intrusión o acceso no autorizado a información confidencial, que aunque simulada, incluía tácticas operativas y datos de naturaleza sensible.

La virtualización se realizó utilizando el entorno de VMware vSphere [140] y un servidor *Elastic Sky X integrated* (ESXI) [141], conforme a la configuración mostrada en la Figura 6.1.

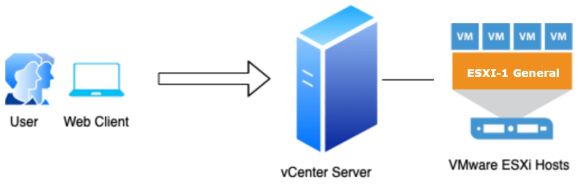

Figura 6.1: Configuración de Infraestructura Virtualizada en VMware vSphere

En el corazón de la arquitectura propuesta para CAMELOT, el nodo principal (ESXI-1) fue designado para alojar todos los servicios esenciales de la plataforma. En este nodo, se establecieron varias máquinas virtuales, cuyos detalles y configuraciones se expondrán más adelante.

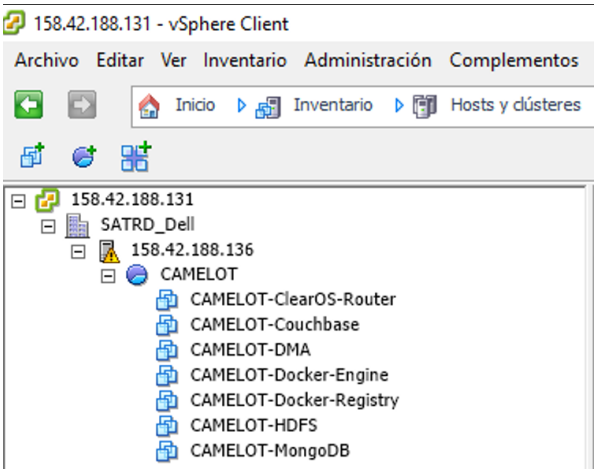

Figura 6.2: Distribución de Máquinas Virtuales en el Nodo Principal - CAMELOT

Profundizando más, la Figura 6.2 ilustra la disposición y el papel de las máquinas virtuales desplegadas. Estas máquinas no solo fueron cruciales para las etapas finales de integración, sino que también desempeñaron un papel vital en las actividades de validación, pruebas y demostraciones. En la figura, se destaca que dentro del entorno de trabajo de CAMELOT se desplegaron un total de 7 máquinas virtuales en el servidor.

A continuación, se detallarán los servicios y recursos asignados a cada una de estas máquinas virtuales, así como las funcionalidades específicas que cada una tenía el objetivo de cumplir en el contexto del piloto de pruebas.

Servidor ESXI-1

- **CAMELOT-ClearOS-Router:** Utilizando ClearOS [142] basado en GNU/Linux, esta máquina virtual actúa como un router avanzado, controlando el tráfico de red en CAMELOT y proporcionando servicios críticos como DHCP [143] y DNS [144] para una operación fluida.
- **CAMELOT-Mongodb:** Esta instancia aloja el motor de base de datos MongoDB, ofreciendo una solución de almacenamiento NoSQL ideal para manejar datos heterogéneos y complejos, típicos en escenarios de gestión de misiones.
- **CAMELOT-Couchbase:** Operando con CouchDB [145], esta máquina se enfoca en la gestión de datos en tiempo real, crucial para el seguimiento efectivo de dispositivos y sus posiciones.
- **CAMELOT-HDFS:** Implementa HDFS de Hadoop, proporcionando un sistema de archivos distribuidos para el almacenamiento y análisis eficiente de grandes volúmenes de datos.
- **CAMELOT-Docker-Registry:** Funciona como el repositorio central para la gestión de imágenes de Docker, facilitando la distribución y el almacenamiento de contenedores.
- **CAMELOT-Docker-Engine:** Este nodo principal para Docker Engine permite la creación y administración de contenedores, mejorando la escalabilidad y distribución de aplicaciones.
- **CAMELOT-DMA:** Gestiona datos diversos, desde información en bruto hasta alertas generadas, y juega un papel crucial en la combinación de datos históricos y en tiempo real para la generación de alertas y el análisis de reglas.

El servidor ESXI-1, equipado con especificaciones técnicas de alto rendimiento, fue esencial para soportar las operaciones de estas máquinas virtuales en CAMELOT.

- **Hardware:** Servidor PowerEdge T640 [146]
- **CPU:** 2x Intel Xeon Gold 5120, 2.2GHz, 14 núcleos/28 hilos
- **Memoria RAM:** 128GB, 2666 MT/s, Dual Rank
- **Almacenamiento:** 12TB SAS 12Gb/s 7,2K rpm

6.2.2. Caso de uso: Gestión de misiones de vigilancia en múltiples ámbitos de actuación en zonas fronterizas

En el marco del proyecto CAMELOT, el caso de uso específico se desarrolla en la costa portuguesa, en la región del Puerto de Setúbal [147]. Se ha identificado una serie de zonas vulnerables a actividades ilícitas, como la inmigración no regulada, el tráfico de drogas y bienes culturales.

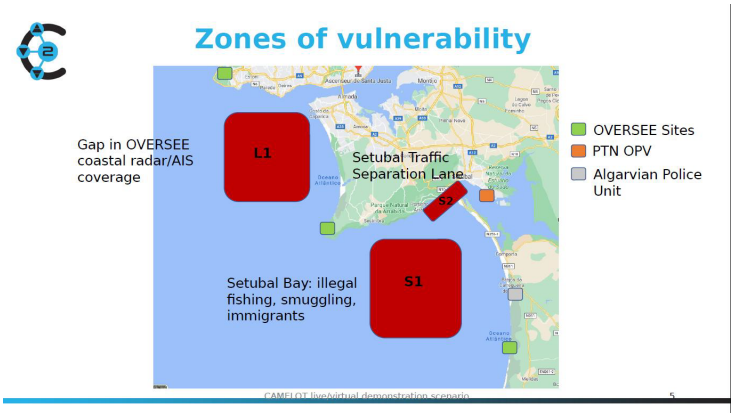

Figura 6.3: Zona con áreas vulnerables

Implementación de Soluciones de Vigilancia

Para abordar estos desafíos, se desplegaron una serie de UxV de dominio múltiple como se puede observar en la Figura 6.4, proporcionando una cobertura completa y eficaz de todas las zonas críticas.

Figura 6.4: Disponibilidad de UxVs

Con este despliegue e implementación, se asegura una vigilancia integral del área, permitiendo detectar y responder a amenazas potenciales.

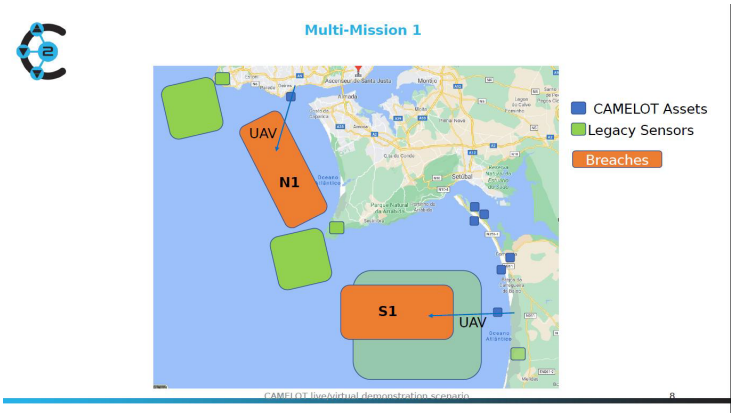

Figura 6.5: Punto de partida misión 1

Demostración de Caso de Uso: Timeline Detallado

El caso de uso se compone de varios escenarios simulados, cada uno representando una situación potencial en el área de vigilancia. A continuación, se detallan los pasos de la demostración, como se observa en la Figura 6.6:

1. **Inicio del Simulador de NMEA:** Para esta demostración remota, se inicia un simulador de *National Marine Electronics Association* (NMEA) [148], estableciendo el escenario virtual para los eventos simulados.

2. **Transferencia de Drogas:** Se simula una operación donde se transfiere una remesa de drogas del barco Linux al Ennui.

3. **Desvío de Barco de Inmigrantes:** Un barco cargado de inmigrantes altera su curso, dirigiéndose hacia la costa portuguesa, representando un escenario de inmigración irregular.

4. **Aparición de Contrabandistas:** Se detecta la presencia de lanchas rápidas de contrabandistas en la zona, introduciendo un nuevo nivel de amenaza.

5. **Encuentro en el Mar:** Las lanchas de contrabandistas llegan al Ennui para recoger la mercancía ilegal, ilustrando la interacción entre diferentes actores ilícitos.

6. **Reporte de Polución:** Se reporta un incidente de contaminación en la zona, añadiendo complejidad al escenario operativo.

7. **Movimiento hacia la Playa:** La lancha de inmigrantes se dirige a una playa específica, indicando una posible situación de desembarco.

8. **Llegada de Contrabandistas a la Costa:** Las lanchas de contrabandistas alcanzan la costa, completando una parte de su operación.

9. **Desembarco de Inmigrantes:** La lancha de inmigrantes llega a la playa, representando un evento crítico en el escenario de inmigración.

10. **Conclusión del Trayecto de Contrabandistas:** Los contrabandistas completan su ruta, representando el fin de su operación ilícita.

11. **Detención de Inmigrantes:** Se simula la detención de los inmigrantes tras llegar a la costa, mostrando la capacidad de respuesta de las autoridades.

12. **Finalización del Caso de Uso:** Se concluye la demostración, proporcionando una visión general de cómo la plataforma CAMELOT puede manejar múltiples situaciones de forma simultánea y eficaz.

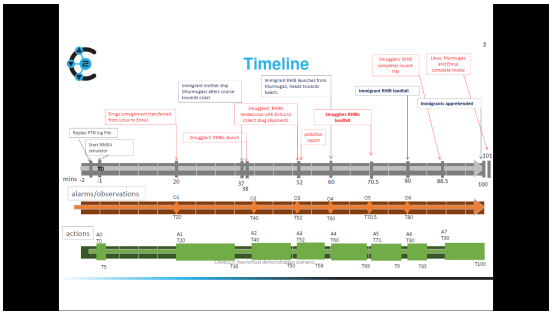

Figura 6.6: Línea temporal del caso de uso

Adaptabilidad y Eficacia de la Plataforma CAMELOT

Este caso de uso demuestra la adaptabilidad y la capacidad de la plataforma CAMELOT para manejar situaciones complejas y dinámicas. La tecnología UxV y las estrategias de vigilancia implementadas permiten un control efectivo y simultáneo de múltiples eventos, asegurando una respuesta adecuada a cada situación. La demostración en el proyecto CAMELOT en la costa portuguesa resalta la versatilidad y eficacia de la plataforma en escenarios de seguridad y vigilancia.

6.2.3. Demostraciones

Dada la situación única creada por la pandemia global, el proyecto CAMELOT adoptó un enfoque innovador al realizar una demostración híbrida, combinando elementos físicos y virtuales.

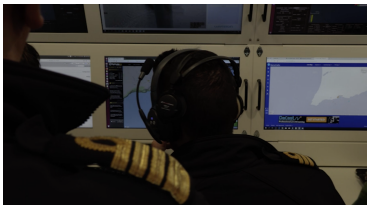

Figura 6.7: Seguimiento de la misión

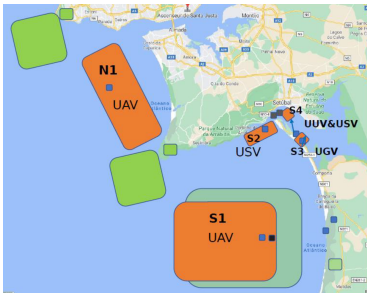

Figura 6.8: Esquema situacional misión

Esta estrategia permitió superar las limitaciones impuestas por el distanciamiento social y las restricciones de viaje, asegurando así la continuidad y el éxito del proyecto.

Monitorización y Tecnología Avanzada en la Costa Portuguesa

La demostración se llevó a cabo en la zona costera de Portugal, donde se monitoreó la misión en tiempo real a través de la plataforma CAMELOT. Este seguimiento continuo demostró los avances significativos y la vanguardia tecnológica que el proyecto incorpora. Como se puede observar en las Figuras 6.9, 6.10, 6.11 y 6.12, se realizó un despliegue de múltiples dispositivos en campo.

Figura 6.9: Despliegue operario con sensor AR

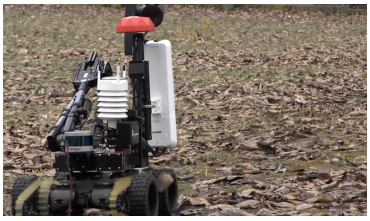

Figura 6.10: Despliegue campo UGV

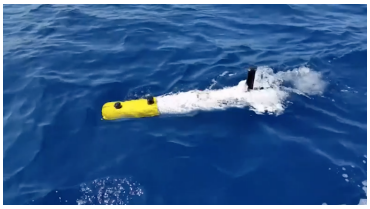

Figura 6.11: Despliegue marítimo UUV

Figura 6.12: Despliegue campo UAV

Casos de Uso Específicos: Tráfico Ilegal de Inmigrantes y Drogas

Durante la demostración, se puso especial atención en un caso concreto de tráfico ilegal de inmigrantes. Con la ayuda de dispositivos como un UUV, un

UGV, un UAV, un operario equipado con gafas de AR y múltiples de sensores de campo se realizó un seguimiento exhaustivo de la situación.

Figura 6.13: Seguimiento inmigrantes llegando a la costa

Los operarios encargados de la misión llevaron a cabo un análisis situacional detallado, utilizando los sensores desplegados para obtener una comprensión clara de los eventos en el terreno.

Figura 6.14: Seguimiento de la misión inmigrantes 1

Figura 6.15: Seguimiento de la misión inmigrantes 2

Esta supervisión meticulosa permitió establecer un perímetro de seguridad efectivo, culminando en la interceptación exitosa de los inmigrantes y asegurando el cumplimiento de los objetivos de la misión.

Figura 6.16: Seguimiento de la misión inmigrantes 3

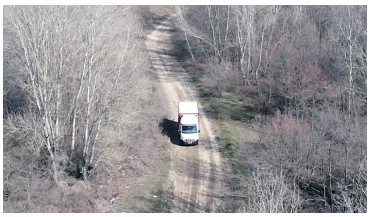

Figura 6.17: Seguimiento de la misión inmigrantes 4

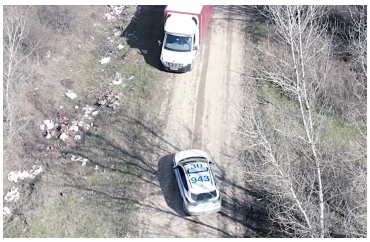

Figura 6.18: Intercepción en la misión inmigrantes

Figura 6.19: Detención de los inmigrantes

Además de la situación de inmigración, se llevaron a cabo demostraciones centradas en el tráfico e intercambio de drogas. Estas actividades ilustraron la capacidad multifacética de la plataforma CAMELOT para abordar una variedad de escenarios de seguridad complejos y dinámicos.

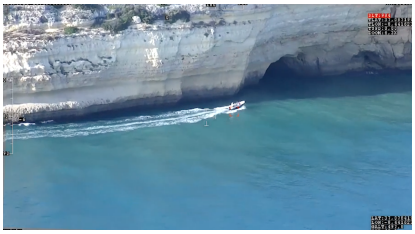

Figura 6.20: Misión tráfico de drogas

Figura 6.21: Persecución misión tráfico de drogas

La demostración híbrida del proyecto CAMELOT resalta la integración efectiva de tecnologías avanzadas y operaciones estratégicas, incluso en el con-

texto desafiante de una pandemia. Con una combinación de innovación y adaptabilidad, CAMELOT demostró ser una herramienta esencial para la vigilancia y la gestión de situaciones de seguridad críticas en la costa portuguesa.

6.3. Respuesta de los usuarios finales

A pesar de los desafíos impuestos por la pandemia, la implementación del proyecto CAMELOT se llevó a cabo en un entorno híbrido simulado. El proceso de validación se ejecutó conforme a lo planificado en cada fase establecida, demostrando un valor agregado significativo en comparación con las soluciones existentes.

Evaluación Operacional y Resultados

La evaluación operativa de la plataforma CAMELOT se basó en índices de rendimiento como *Métricas de Efectividad Operativa* (MOE), *Key performance indicator* (KPI)s y otros. Los resultados, analizados en detalle, muestran una satisfacción adecuada de las necesidades de los usuarios, destacando la eficiencia de la plataforma en el contexto de vigilancia fronteriza.

La plataforma CAMELOT fue diseñada para ser intuitiva, reduciendo la carga de trabajo de los usuarios finales y cumpliendo con las normativas éticas, legales y de protección de datos. Las características clave incluyen:

- Monitoreo y control centralizado de todos los subsistemas a nivel de Comando y Control.
- Herramientas para crear, actualizar y visualizar un Cuadro Operacional Común, facilitando la toma de decisiones.
- Disponibilidad de Información Táctica/Situacional a través de dispositivos portátiles para unidades de patrulla.
- Integración y coordinación de dispositivos portátiles en la cadena de mando y control.
- Herramientas para la Planificación de Misiones y la Gestión de Operaciones acorde a los requisitos operacionales.

Capacidades Específicas y Comunicación Interfaz

El sistema demuestra una capacidad sobresaliente para mostrar y manejar información de sensores y plataformas, apoyando la conciencia situacional y la predicción de capacidades y limitaciones. Esto incluye:

- Visualización de eventos detectados en un sistema GIS, con un registro único para cada evento.
- Procesamiento de pistas con capacidades como seguimiento de información, filtros y reproducción comprimida en tiempo.
- Manejo y generación de alarmas automáticas basadas en el análisis y fusión de datos de sensores.
- Presentación flexible de alarmas y verificación de objetos de interés.
- Representación de zonas de amortiguamiento para apoyar actividades de patrulla superficial.

El sistema incluye un Sistema de Gestión de Contenido para el almacenamiento, manejo, archivo y registro eficiente de contenido multimedia y heterogéneo. La selección y duración del almacenamiento de datos es ajustable, y los datos se almacenan tanto local como remotamente.

Conclusiones Generales

Los resultados obtenidos de la plataforma CAMELOT han sido positivos, demostrando un valor añadido excepcional en el ámbito de la vigilancia fronteriza. La plataforma no solo ofrece una experiencia intuitiva y reduce la carga de trabajo, sino que también cumple con las regulaciones de privacidad y protección de datos, lo que la hace una solución integral y adaptable para el futuro.

6.4. PREVISION

6.4.1. Entorno de pruebas

Al igual que en la fase final del proyecto CAMELOT, la evaluación de la eficacia y aplicabilidad de PREVISION se realizó a través de la arquitectura prototipo desarrollada en el Capítulo 3 y ajustada específicamente para PREVISION, cuyos detalles se encuentran en el Capítulo 5. Dada la variedad de aplicaciones potenciales del prototipo, se establecieron tres escenarios de prueba distintos para demostrar sus capacidades.

El primer escenario se llevó a cabo en Bilbao, España, donde se simuló la prevención de un ataque terrorista en un lugar crítico, en este caso, el Teatro Arriaga [149]. El segundo escenario se desarrolló en Moldavia, enfocado en la simulación de un caso de radicalización y prevención de amenazas terroristas. Finalmente, el tercer escenario tuvo lugar en Munich, Alemania, simulando un incidente de ataque terrorista.

Implementación de la Infraestructura

Siguiendo un enfoque similar al utilizado en CAMELOT, todos los servicios de PREVISION se alojaron virtualmente en una serie de servidores dentro de la infraestructura de la UPV.

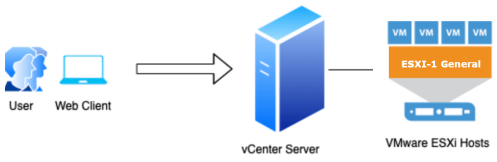

Figura 6.22: Entorno CLOUD VMware

Para los servicios en la nube, se optó por una virtualización en el entorno VMware vSphere, utilizando dos servidores ESXI configurados como se muestra en la Figura 6.22. Estos servidores estaban interconectados mediante una red segura protegida por VPN, garantizando la seguridad y la privacidad de los datos.

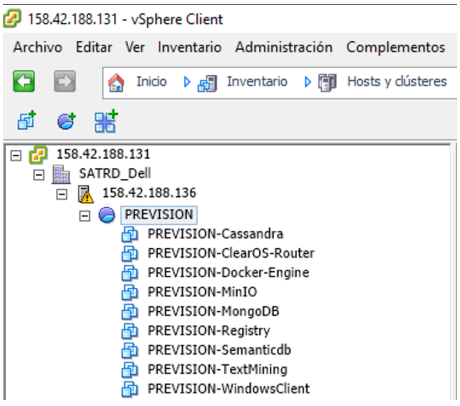

Figura 6.23: Detalle de las Máquinas Virtuales en los Servidores PREVISION

La Figura 6.23 detalla la distribución de las máquinas virtuales empleadas en las diversas demostraciones, así como en las fases de desarrollo, pruebas y

validación. En esta configuración, se observa que el servidor alojó un total de 9 máquinas virtuales dentro del espacio de trabajo PREVISION.

En este documento se presentan los servicios y recursos asignados a cada servidor, así como sus funciones específicas en distintos escenarios de prueba.

Servidor ESXI-1

- **PREVISION-ClearOS-Router:** Utiliza GNU/Linux ClearOS, derivado de CentOS, para funcionar como un router virtual. Su principal tarea es la administración del tráfico de red de PREVISION, incluyendo la asignación de direcciones IP mediante un servidor *Dynamic Host Configuration Protocol* (DHCP) y la resolución de nombres de dominio a través de un servidor *Domain Name System* (DNS), lo que optimiza la eficiencia de la red dentro de PREVISION.

- **PREVISION-Mongodb:** Aloja la base de datos MongoDB, una solución NoSQL basada en documentos. Esta plataforma es reconocida por su rendimiento, disponibilidad y escalabilidad. Con su estructura de datos flexible, es ideal para el manejo de datos complejos y variados, característicos en la prevención de incidentes.

- **PREVISION-Semanticdb:** Se basa en Apache Jena Fuseki, un servidor de base de datos semántica que proporciona funciones avanzadas para el almacenamiento y la consulta de datos estructurados siguiendo los estándares de la web semántica, como RDF y SPARQL. Este servidor es clave para consultas complejas y el razonamiento lógico sobre los datos.

- **PREVISION-MinIO:** Un sistema de archivos distribuidos que se destaca por su alta disponibilidad y tolerancia a fallos. En PREVISION, se emplea para el almacenamiento y procesamiento eficiente de grandes conjuntos de datos.

- **PREVISION-Docker-Registry:** Sirve como el repositorio central para almacenar y gestionar imágenes Docker en el entorno de PREVISION. Funciona como un punto crítico para la distribución y almacenamiento seguro de contenedores, facilitando el acceso y manejo de imágenes de aplicaciones y servicios.

- **PREVISION-Docker-Engine:** Representa el principal nodo de la plataforma Docker Engine, permitiendo la creación y gestión de contenedores Docker. En PREVISION, facilita la encapsulación y distribución de aplicaciones y servicios, posibilitando una replicación y escalabilidad eficientes.

- **PREVISION-Cassandra:** Incorpora el motor de base de datos NoSQL Cassandra, especializado en el manejo de datos tabulares orientados a columnas. Su elección se debe a su robustez y escalabilidad, ideal para el almacenamiento y procesamiento de grandes volúmenes de datos.
- **PREVISION-TextMining:** Conjunto de herramientas para el procesamiento y análisis de texto. Utiliza técnicas de minería de texto avanzadas para extraer información y patrones de grandes volúmenes de datos textuales, crucial para la identificación de tendencias y correlaciones en la prevención de amenazas.
- **PREVISION-Windows-client:** Se trata de una máquina virtual en windows capaz de ejecutar servicios no accesibles desde otros sistemas operativos.

Se observa que el servidor ESXI-1 *CLOUD* virtualiza la mayoría de los servicios críticos de PREVISION, requiriendo especificaciones técnicas de alto rendimiento para gestionar las diversas 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

6.4.2. Caso de uso 1: Bilbao

La sección describe un caso de uso detallado de la Policía *Ertzaintza* (ERTZ) [150] en Bilbao, enfocado en la utilización de tecnologías avanzadas y análisis de datos para la identificación y gestión de amenazas de seguridad.

1. **Análisis Histórico de Datos:** La ERTZ inicia un estudio detallado de datos históricos para identificar anomalías indicativas de amenazas de seguridad en Bilbao.
2. **Amenaza en el Teatro Arriaga:** Se detecta una posible amenaza en el Teatro Arriaga. Personas radicalizadas están bajo vigilancia, incluyendo el análisis de sus actividades en redes sociales.
3. **Solicitud de Información Adicional:** Se solicita información a operadores de red para enriquecer la base de conocimientos de PREVISION, vinculando sospechosos con IPs y actividades de red.

4. **Análisis de Redes Sociales:** Se analizan datos de redes sociales para detectar comunidades y vínculos entre individuos.
5. **Detección de Múltiples Identidades:** Se analiza el dataset de redes sociales para identificar múltiples identidades de individuos.
6. **Vigilancia de Vehículos Sospechosos:** Se realiza vigilancia sobre vehículos de sospechosos y se analizan imágenes de estos en diferentes cámaras.
7. **Análisis de Detección de Actividades:** Se inicia la detección de actividades en las mismas cámaras donde se identificaron vehículos sospechosos.
8. **Detección de Accesos Ilícitos:** Se identifican accesos ilícitos en cámaras cerca del área del estadio, incluyendo intentos de ataque a puertos *Secure Shell* (SSH).
9. **Identificación de Sospechosos en Cámaras:** Se crea una galería de sospechosos y se inicia un análisis para identificarlos en cámaras cercanas al área de interés.
10. **Análisis de Reconocimiento de Actividades:** Se realiza un análisis para identificar actividades en cámaras donde se detectaron sospechosos.
11. **Detección y Reconocimiento Facial:** Se lleva a cabo detección y reconocimiento facial en áreas cercanas al estadio para identificar a los sospechosos.

Este escenario describe las operaciones llevadas a cabo por la ERTZ en Bilbao, utilizando un enfoque integrado de análisis de datos, vigilancia, y tecnología avanzada para manejar amenazas de seguridad.

Figura 6.24: Sede de la Ertzaintza, Bilbao - Demostración

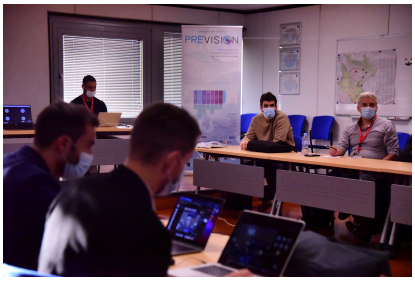

Figura 6.25: Trabajo conjunto en la sede de la Ertzaintza

Respuesta de los usuarios finales

Los resultados del Cuestionario 6.1 se centran en aspectos como la facilidad de uso y la necesidad de soporte técnico, el Cuestionario 6.2 evalúa el valor añadido, utilidad en el trabajo diario, y la percepción de su coste y eficacia.

Pregunta	**Total. desacuerdo**	**Desacuerdo**	**Neutral**	**De acuerdo**	**Total. acuerdo**
Q1. Me gustaría usarlo con frecuencia:	0	1	0	2	3
Q2. Me pareció que era fácil de usar:	0	0	2	4	0
Q3. Creo que no necesitaría el apoyo de una persona técnica para usar este sistema:	0	2	1	3	0
Q4. Encontré que las funciones en este sistema estaban bien integradas:	0	1	1	4	0
Q5. Me pareció que había demasiada consistencia:	0	1	4	2	0
Q6. La mayoría aprendería a usarlo rápidamente:	0	1	1	4	0
Q7. Creo que es compatible con procedimientos ya existentes en mi organización:	0	0	1	5	0
Q8. Me sentí muy seguro usándolo:	1	0	2	3	0
Porcentaje:	4	11	25	55	5

Tabla 6.1: Respuestas al Cuestionario de Usabilidad del Sistema

Pregunta	**Total. desacuerdo**	**Desacuerdo**	**Neutral**	**De acuerdo**	**Total. acuerdo**
Q1. Creo que esta herramienta tendrá un gran impacto positivo en nuestro trabajo:	0	0	1	3	2
Q2. Encontré que este sistema aporta valor agregado respecto a las herramientas actuales:	0	1	0	4	1
Q3. Creo que este sistema será de gran ayuda para nuestro trabajo:	0	0	1	3	2
Q4. Espero que este sistema no sea costoso:	1	0	1	3	0
Q5. Recomendaría encarecidamente a mi organización pagar por tener esta funcionalidad:	0	1	1	4	0
Q6. Recomendaría el uso de esta herramienta a un colega:	0	1	0	2	3
Q7. Creo que sería posible transferir esta tecnología a otro dominio de la aplicación de la ley:	0	1	1	1	3
Porcentaje:	2	10	12	49	27

Tabla 6.2: Respuestas al Cuestionario de Impacto

Los comentarios adicionales de las Agencias de Aplicación de la Ley ofrecen una visión más profunda sobre la plataforma PREVISION, su aplicabilidad y

las expectativas para su mejora. Las siguientes conclusiones resumen los aspectos más destacados:

- **Aplicabilidad y Fiabilidad en Diferentes Organizaciones:** Se reconoce que algunas herramientas de PREVISION podrían ser aplicables en otras organizaciones, pero es esencial que sean fiables, ofrezcan resultados previstos y se adapten a diferentes contextos.
- **Interconexión con Soluciones Existentes:** Es crucial que PREVISION se interconecte con soluciones de C2, mecanismos de comunicación y soluciones GIS existentes en los entornos de las LEAs.
- **Interés Operativo y Necesidad de Mejoras:** Las herramientas demostradas generan interés operativo y han mejorado significativamente desde las últimas demostraciones. Sin embargo, se destaca la necesidad de mantener la coherencia en investigaciones largas y la importancia de permitir a los operadores seleccionar, guardar o extraer resultados específicos.
- **Preocupaciones sobre Rendimiento y Uso Simultáneo:** A pesar de los avances, persisten preocupaciones sobre el rendimiento de la plataforma, especialmente en cuanto al uso simultáneo por varios investigadores y la recuperación de datos.
- **Cumplimiento con el GDPR y Facilidad de Uso:** Los usuarios finales buscan herramientas que sean compatibles con el *General Data Protection Regulation* (GDPR) [151], destacando la importancia del rendimiento, la rapidez y la facilidad de uso. La plataforma tiene un potencial de uso significativo en diferentes servicios de la policía nacional, municipal, gendarmería, DGSI, etc.

Estas conclusiones reflejan el reconocimiento del potencial de la plataforma PREVISION, al mismo tiempo que subrayan la importancia de su desarrollo continuo y adaptación a las necesidades legales y operativas de las LEAs y otras organizaciones relevantes.

6.4.3. Caso de uso 2: Escenario de la Cumbre Rumano-Moldava

Aquí se detalla un caso práctico de prevención de amenazas de radicalización y terrorismo durante una importante cumbre entre Rumania y Moldavia. El storyline presenta las etapas clave de la operación llevadas a cabo por los servicios de seguridad, utilizando avanzadas herramientas de análisis y prevención proporcionadas por la plataforma PREVISION.

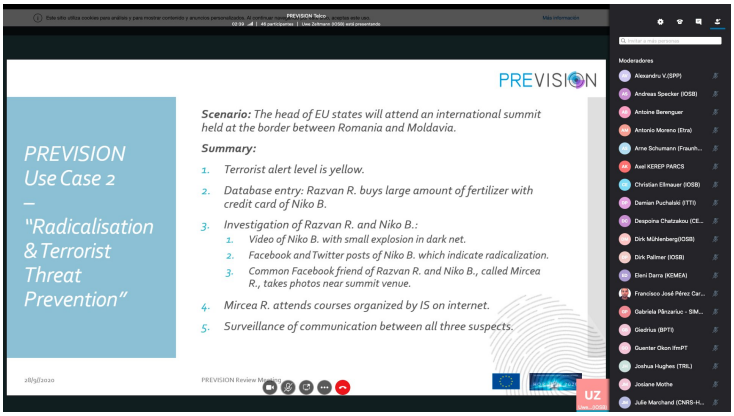

Figura 6.26: Vista general del caso de uso

1. **Inicio del Análisis de Información:** Antes de la cumbre, los servicios de seguridad comienzan un análisis detallado de datos para identificar amenazas potenciales.

2. **Rastreo en Redes Sociales y Darknet:** Se realiza un rastreo en redes sociales y foros de darknet para recopilar publicaciones sospechosas.

3. **Evaluación de Sospechosos:** Se carga información biográfica y fotos de sospechosos en la base de conocimientos y en Hadoop para su evaluación.

Figura 6.27: Evaluación de sospechosos

4. **Análisis de Texto y Nivel de Radicalización:** Se efectúa un análisis de texto detallado para determinar el grado de radicalización de los sospechosos.

5. **Visualización de Resultados con TVT:** Los resultados se visualizan a través de la Herramienta de Visualización de Texto para facilitar la interpretación.

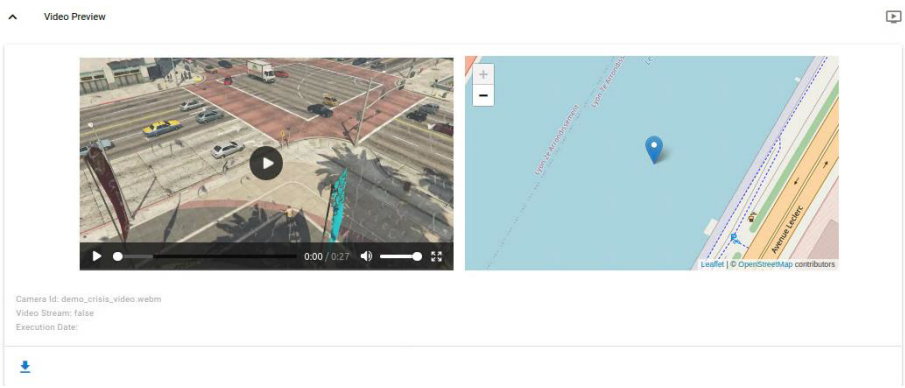

Figura 6.28: Supervisión grabaciones

6. **Conclusión sobre la Radicalización de Niko B.:** Se concluye que Niko B. está radicalizado y se inicia la identificación de todos los involucrados.

7. **Identificación de Cómplices:** Se descubre que Niko B. tiene contactos directos con otros sospechosos, incluidos Razvan R. y Mircea R.

Figura 6.29: Identificación de otros sospechosos

8. **Aplicación de Herramientas de Análisis de Video:** Se emplean herramientas de análisis de video para monitorizar las actividades de los sospechosos.

9. **Revisión de Grabaciones de CCTV y vídeo de UxVs:** Se revisan videos de CCTV, así como grabaciones de los UxVs cerca del lugar de la cumbre para identificar a los sospechosos.

10. **Análisis de Actividades y Reconocimiento de Incidentes:** Se determinan actividades sospechosas y se identifican incidentes potenciales cerca de la cumbre.

11. **Clasificación y Respuesta a Eventos de Crisis:** Tras identificar un evento de crisis, se clasifica y se coordina una respuesta rápida para contener el incidente.

12. **Conclusión y Prevención de Acciones:** Con la ayuda de las herramientas de PREVISION, se identifica un ataque planeado en la cumbre y se previenen acciones contra los dignatarios protegidos.

Se detalla las operaciones llevadas a cabo para prevenir amenazas de radicalización y terrorismo durante la cumbre Rumano-Moldava, demostrando la eficacia de las herramientas de análisis y prevención de PREVISION.

Respuesta de los usuarios finales

A continuación se presentan los resultados de dos cuestionarios clave diseñados para evaluar la usabilidad y el impacto de una herramienta tecnológica innovadora. El primero, el Cuestionario 6.3, se centra en aspectos como la facilidad de uso, la integración de funciones y la necesidad de soporte técnico. El segundo, el Cuestionario 6.4, evalúa el valor añadido de la herramienta, su utilidad en el trabajo diario, y la percepción de su costo y eficacia. Ambos cuestionarios son instrumentos esenciales para comprender cómo los usuarios perciben la herramienta y cuál es su potencial impacto en el ámbito operativo.

Pregunta	**Total. desacuerdo**	**Desacuerdo**	**Neutral**	**De acuerdo**	**Total. acuerdo**
Q1. Creo que me gustaría usar este sistema con frecuencia:	0	0	0	1	4
Q2. Me pareció que el sistema era fácil de usar:	0	0	2	3	0
Q3. Creo que no necesitaría el apoyo de una persona técnica para usar este sistema:	0	1	1	3	0
Q4. Encontré que las funciones en este sistema estaban bien integradas:	0	0	0	4	5
Q5. Me pareció que había demasiada consistencia en este sistema:	0	0	3	2	0
Q6. Imagino que la mayoría de las personas aprenderían a usar este sistema rápidamente:	0	0	3	2	0
Q7. Creo que esta herramienta es compatible con procedimientos ya existentes en mi organización:	0	0	1	3	1
Q8. Me sentí muy seguro usando el sistema:	0	0	2	2	1
Porcentaje:	3	9	29	40	19

Tabla 6.3: Respuestas al Cuestionario de Usabilidad del Sistema

Pregunta	**Total. desacuerdo**	**Desacuerdo**	**Neutral**	**De acuerdo**	**Total. acuerdo**
Q1. Creo que esta herramienta tendrá un gran impacto positivo en nuestro trabajo:	0	0	0	3	2
Q2. Encontré que este sistema aporta valor agregado respecto a las herramientas actuales:	0	0	0	3	2
Q3. Creo que este sistema será de gran ayuda para nuestro trabajo:	0	0	0	2	2
Q4. Espero que este sistema no sea costoso:	0	0	0	2	2
Q5. Recomendaría encarecidamente a mi organización pagar por tener esta funcionalidad:	0	0	0	2	2
Q6. Recomendaría el uso de esta herramienta a un colega:	0	0	0	2	2
Q7. Creo que sería posible transferir esta tecnología a otro dominio de la aplicación de la ley:	0	0	0	2	2
Porcentaje:	3	8	8	43	38

Tabla 6.4: Respuestas al Cuestionario de Impacto

Los comentarios recibidos de las LEAs respecto a la plataforma PREVISION ofrecen una perspectiva valiosa sobre su utilidad, capacidades

y áreas de mejora. Las siguientes conclusiones resumen los aspectos más destacados de estos comentarios:

- **Utilidad en la Prevención de Radicalización y Ataques Terroristas:** Las LEAs reconocen que la plataforma es especialmente útil para la prevención de radicalización y ataques terroristas, siempre que la situación legal permita el uso completo de los componentes de la plataforma.

- **Capacidades Adicionales a las Herramientas Actuales:** La plataforma agrega diversas capacidades útiles a las herramientas existentes, ampliando el alcance y la eficiencia de las operaciones actuales.

- **Aplicación en Diversas Fases de Investigación:** La plataforma es útil tanto al inicio como durante las investigaciones, y en las investigaciones de seguimiento, ofreciendo una forma compacta de agrupar y mostrar toda la información necesaria.

- **Reconocimiento y Bloqueo Rápido de Peligros:** La plataforma permite un reconocimiento y bloqueo más rápido de peligros, con medidas basadas en el riesgo que representa una persona.

- **Necesidad de Mejoras y Calibración:** Si bien algunos de los prototipos de herramientas aún necesitan mejoras o calibración para reducir falsos positivos y aumentar la tasa de detección y precisión, la plataforma muestra un potencial significativo.

- **Priorización de Información Relevante:** Es esencial que la plataforma pueda mostrar solo información relevante y prioritaria para evitar sobrecargar a los analistas con grandes volúmenes de datos.

- **Posibilidad de Transferencia a Varias Organizaciones:** La variedad de tecnologías detrás de PREVISION podría ser utilizada por múltiples organizaciones, aunque es crucial considerar cómo se realiza esta transferencia, si incurre en costos y si solo algunas de las herramientas pueden ser incluidas según la línea de trabajo de estas organizaciones.

Estas conclusiones reflejan el potencial y los desafíos de la plataforma PREVISION, subrayando la importancia de su desarrollo continuo y adaptación a las necesidades específicas de las LEAs y otras organizaciones relevantes.

6.4.4. Caso de uso 3: Escenario de la Conferencia de Seguridad de Múnich

Se describe el despliegue operativo para la prevención de amenazas terroristas durante la Conferencia de Seguridad de Múnich, donde líderes políticos de alto nivel se reúnen bajo medidas de seguridad intensivas.

1. **Identificación de una Amenaza Potencial:** La policía bávara centra su atención en Ibraim Jafari, clasificado como una posible amenaza por otra agencia europea de aplicación de la ley. Su actividad en redes sociales es monitoreada y analizada.

2. **Análisis de Redes Sociales y Foros del Darknet:** Tras analizar datos de redes sociales, Ibraim Jafari es identificado como actor clave en una comunidad. Se encuentran interacciones frecuentes con Guenter Seifert, otro actor clave. Se analizan datos recopilados de foros del darknet asociados a ambos.

3. **Evaluación del Nivel de Radicalización:** Se estima que Ibraim Jafari está radicalizado basándose en el análisis de las actividades en línea.

4. **Consulta con la Oficina Estatal de Protección de la Constitución:** Se descubre que Ibraim Jafari estuvo supuestamente involucrado en la creación o distribución de material propagandístico islamista. El material recopilado se examina en busca de menciones a la *Munich Security Conference* (MSC) y pistas sobre posibles métodos de ataque terrorista.

5. **Detección y Reconocimiento Facial Cerca del Evento:** Se lleva a cabo la detección y reconocimiento facial en grabaciones de video cerca del lugar de la MSC. Además, se utiliza el reconocimiento de actividades durante el evento. Se descubre que Ibraim Jafari observó detenidamente la escena frente a la entrada principal antes del inicio de la MSC.

6. **Registro y Análisis de Vehículos:** Durante el evento, se graban varios vehículos que pasan por la entrada del hotel donde tiene lugar la MSC.

En el presente caso de uso se detalla las medidas de seguridad y análisis llevados a cabo para prevenir amenazas terroristas en la Conferencia de Seguridad de Múnich, destacando la eficacia de las herramientas de análisis y vigilancia.

Respuesta de los usuarios finales

A continuación se presentan los resultados del Cuestionario 6.5, que se centra en aspectos como la facilidad de uso, la integración de funciones y la necesidad de soporte técnico, y el Cuestionario 6.6 que evalúa el valor añadido de

la herramienta, su utilidad en el trabajo diario, y la percepción de su costo y eficacia.

Pregunta	**Total. desacuerdo**	**Desacuerdo**	**Neutral**	**De acuerdo**	**Total. acuerdo**
Q1. Creo que me gustaría usar este sistema con frecuencia:	0	1	0	4	1
Q2. Me pareció que el sistema era fácil de usar:	0	0	3	2	1
Q3. Creo que no necesitaría el apoyo de una persona técnica para usarlo:	0	1	3	2	0
Q4. Encontré que las funciones en este sistema estaban bien integradas:	0	1	0	2	3
Q5. Me pareció que había demasiada consistencia en este sistema:	0	0	4	2	0
Q6. Imagino que la mayoría aprendería a usarlo rápidamente:	0	1	2	3	0
Q7. Creo que es compatible con procedimientos ya existentes en mi organización:	0	1	1	3	0
Q8. Me sentí muy seguro usándolo:	1	0	2	2	1
Porcentaje:	4	9	30	43	13

Tabla 6.5: Respuestas al Cuestionario de Usabilidad del Sistema

Pregunta	**Total. desacuerdo**	**Desacuerdo**	**Neutral**	**De acuerdo**	**Total. acuerdo**
Q1. Creo que esta herramienta tendrá un gran impacto positivo en nuestro trabajo:	0	0	1	4	1
Q2. Encontré que este sistema aporta valor agregado respecto a las herramientas actuales:	0	1	0	4	1
Q3. Creo que este sistema será de gran ayuda para nuestro trabajo:	0	0	1	4	1
Q4. Espero que este sistema no sea costoso:	0	1	3	1	1
Q5. Recomendaría encarecidamente a mi organización pagar por tener esta funcionalidad:	0	1	2	2	1
Q6. Recomendaría el uso de esta herramienta a un colega:	0	1	0	3	2
Q7. Creo que sería posible transferir esta tecnología a otro dominio de la aplicación de la ley:	0	0	1	3	2
Porcentaje:	0	10	19	50	21

Tabla 6.6: Respuestas al Cuestionario de Impacto

Los comentarios de las Agencias de Aplicación de la Ley brindan percepciones valiosas sobre la operatividad y funcionalidad de la plataforma

PREVISION. Las siguientes conclusiones resumen los puntos clave destacados por las LEAs:

- **Complejidad y Operatividad:** Desde el punto de vista del observador, el sistema no parece demasiado complejo, pero se anticipa que podrían surgir problemas durante la operación real. Las opciones de filtrado y clasificación requieren conocimientos programáticos, lo que puede ser una barrera para algunos usuarios.

- **Conocimiento Específico para Funciones Avanzadas:** Algunas características de la plataforma, como la programación en *Language for querying databases stored as RDF* (SPARQL) [152] para filtrar resultados, requieren conocimientos específicos, lo que podría limitar su accesibilidad a usuarios sin estas habilidades.

- **Integración y Conexión de Herramientas:** Existe la necesidad de mejorar la integración de las herramientas para asegurar una interconexión eficiente y reducir la necesidad de interacción manual por parte de los desarrolladores.

- **Consistencia y Rendimiento con Datos Nuevos:** La consistencia observada en las demostraciones se debe a ensayos previos y al uso de conjuntos de datos conocidos. Surge la curiosidad sobre cómo funcionaría la plataforma con información recién recopilada.

- **Presentación de Herramientas y Complejidad:** En la demostración actual, se presentaron un número limitado de herramientas, mostrando una complejidad manejable. Sin embargo, PREVISION ofrece muchas más funcionalidades que requerirán un mayor esfuerzo por parte de los usuarios para familiarizarse con todas ellas.

- **Aplicabilidad en Organizaciones:** En general, los procedimientos dentro de PREVISION son aplicables también en las organizaciones de las LEAs. Dependiendo de la herramienta y las actividades específicas, algunas podrían no ser ejecutadas por los oficiales si están fuera del alcance de su actividad.

Estas conclusiones proporcionan una visión crítica del estado actual de la plataforma PREVISION y subrayan áreas clave para su mejora y adaptación a las necesidades de los usuarios finales y las organizaciones de aplicación de la ley.

6.4.5. Demostraciones

Las demostraciones de casos de uso en el proyecto PREVISION desempeñan un papel crucial en la validación y el desarrollo de sus herramientas y tecnologías. Estas demostraciones no solo proporcionan una oportunidad para probar la plataforma en escenarios realistas y desafiantes, sino que también permiten a los desarrolladores y a los usuarios finales, incluidas las LEAs, interactuar directamente con el sistema, evaluando su eficacia, usabilidad y impacto operativo.

Figura 6.30: Demostración en Lyon - Herramientas

Figura 6.31: Demostración en Lyon - Herramientas - Demo

Figura 6.32: Demostración en Karlsruhe

Figura 6.33: Demostración en Toulouse

Colaboración con Proyectos Hermanos

Una faceta destacada de las demostraciones de PREVISION ha sido la colaboración con proyectos hermanos como *Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs* (LETSCROWD) [153]. Estas colaboraciones enriquecen el proceso de desarrollo, permitiendo que las herramientas y tecnologías se prueben en un contexto más amplio y se beneficien de diferentes perspectivas y experiencias. La inte-

gración con proyectos como LETSCROWD amplía el alcance de las demostraciones, ofreciendo una visión más comprensiva del rendimiento de la plataforma en distintos escenarios operativos.

Figura 6.34: Colaboración con el Proyecto LETSCROWD

Las demostraciones de PREVISION son fundamentales para garantizar que la plataforma cumpla con las necesidades y expectativas de los usuarios finales. A través de estas pruebas prácticas y la colaboración con otros proyectos, PREVISION continúa perfeccionando sus herramientas para proporcionar soluciones efectivas en el ámbito de la seguridad y la prevención del crimen.

Capítulo 7

Conclusiones y líneas futuras

7.1. Conclusiones

La presente tesis ha explorado en profundidad los desafíos asociados con la coordinación efectiva en la gestión de misiones multidominio y el manejo de amenazas, enfatizando la importancia de la colaboración entre diferentes corporaciones. Se ha elaborado una arquitectura general innovadora, diseñada para afrontar eficazmente los obstáculos relacionados con la falta de coordinación interagencial, y esta ha sido aplicada y probada en dos contextos de proyecto distintos.

Implementación y Evaluación en Proyectos CAMELOT y PREVISION

En el marco de los proyectos CAMELOT y PREVISION, se llevaron a cabo pruebas en una variedad de escenarios, lo que proporcionó una oportunidad única para evaluar la arquitectura propuesta. Estas demostraciones han sido fundamentales para extraer aprendizajes valiosos y conclusiones pertinentes sobre la eficacia y la viabilidad de las estrategias desarrolladas. A continuación, se presentan las conclusiones finales derivadas de este trabajo de investigación, que sintetizan los resultados obtenidos y las lecciones aprendidas a lo largo del proceso de desarrollo y evaluación de la arquitectura en los mencionados proyectos multidominio.

Este capítulo concluye la tesis proporcionando una visión integrada y una reflexión sobre los esfuerzos y resultados alcanzados, subrayando las contribu-

ciones significativas de la investigación en el campo de la gestión de misiones multidominio y la prevención y gestión de amenazas.

7.1.1. Conclusiones generales

Estado del Arte en la Gestión de Misiones Multidominio y Prevención de Amenazas

- **Integración en Sistemas Complejos:** La adopción de tecnologías emergentes en sistemas complejos presenta retos técnicos que necesitan soluciones innovadoras y adaptativas.
- **Retos y Oportunidades con Big Data:** Si bien las tecnologías de Big Data ofrecen oportunidades para mejorar el análisis de datos variados, enfrentan desafíos en cuanto a integración, seguridad y procesamiento de información.
- **Importancia de la Respuesta Rápida en Situaciones Críticas:** Las emergencias exigen respuestas rápidas y coordinadas, desafiando la colaboración interagencial debido a la diversidad en tecnologías y procedimientos.
- **Desafíos en Interoperabilidad y Trabajo Conjunto:** La colaboración efectiva entre agencias se ve obstaculizada por sistemas heterogéneos, afectando el intercambio fluido de información.
- **Manejo de Información en la Era de la Big Data:** En un mundo inundado de datos digitales, la gestión de información se ha vuelto un desafío crítico, especialmente en áreas como la gestión de misiones multidominio y prevención de amenazas, donde el procesamiento efectivo de información es crucial.
- **Gestión de Datos Diversos:** El manejo de grandes volúmenes de datos variados, especialmente en la lucha contra actividades ilícitas, plantea desafíos en almacenamiento y análisis.
- **Barreras de Recursos y Formación:** La limitación de recursos, infraestructuras anticuadas y falta de formación en tecnologías emergentes son barreras clave para una gestión eficiente en situaciones de crisis.
- **Reto de los Grandes Volúmenes de Datos:** La necesidad de procesar grandes cantidades de datos, en especial en tiempo real, demanda soluciones más allá de las tecnologías convencionales, enfrentando retos de escalabilidad y rendimiento.

- **Problemas de Integración y Silos de Datos:** La falta de integración y los silos de datos impiden lograr una perspectiva comprensiva y actualizada, crucial en la gestión de misiones multidominio y prevención de amenazas.
- **Desarrollo de Herramientas de Análisis y Visualización:** Aunque las herramientas de análisis y visualización han avanzado, persisten desafíos para adaptar estas tecnologías a las necesidades específicas de distintos contextos operativos.
- **Uso de Adaptadores para Dispositivos Externos:** Los adaptadores juegan un papel vital en la transformación de datos de dispositivos externos a formatos compatibles con el proyecto. Facilitan la interoperabilidad y la integración efectiva de sistemas heterogéneos, permitiendo que la información recolectada sea procesada y utilizada eficientemente. Esta función es esencial para una toma de decisiones precisa y la ejecución exitosa de operaciones multidominio.
- **Integración de dispositivos UxV:** Se ha preparado el sistema para poder gestionar múltiples UxV, ya sea para la supervisión de misiones, así como para el control y vigilancia a nivel preventivo.

Avances y Soluciones en la Arquitectura

- **Avance Frente a Sistemas Tradicionales:** La arquitectura sugerida ofrece soluciones avanzadas para mejorar la eficacia y la interoperabilidad en la gestión de misiones multidominio y prevención de amenazas, enfocándose en una integración efectiva y el intercambio de información entre múltiples entidades.
- **Satisfacción de Necesidades Específicas de Usuarios:** Se ha prestado especial atención a las demandas de los usuarios de los proyectos CAMELOT y PREVISION, personalizando la arquitectura para cumplir con sus requisitos exclusivos.
- **Estructura Innovadora y Flexibilidad:** La propuesta introduce una estructura altamente innovadora, adecuada para una variedad de entornos, desde oficinas hasta situaciones de campo, con un enfoque en la interoperabilidad y la mejora de la comunicación interagencial.
- **Integración Eficiente de Software:** La arquitectura propuesta se beneficia de la integración de una diversidad de componentes software, aplicando tecnologías como SOAP y API REST.

- **Adopción de Microservicios y API Gateway:** Resalta la transición hacia arquitecturas de microservicios, con un API Gateway que mejora la modularidad, escalabilidad y la elección de tecnología.
- **Gestión de la Complejidad en Software:** Se aborda la complejidad inherente a sistemas integrados, con un enfoque en la combinación de diversas tecnologías para el manejo eficiente de grandes volúmenes de datos.
- **Desarrollo en la Adquisición de Datos:** Se establece una infraestructura robusta para adquisición y almacenamiento de datos, aplicando tecnologías como Apache Kafka y bases de datos especializadas.
- **Innovaciones en la Fusión de Datos:** Los datos se transforman en formatos accesibles mediante ontologías y bases de conocimiento, facilitando el acceso y la organización eficiente de la información.
- **Profundización en el Análisis de Datos:** Se implementa un rango extenso de análisis de datos a través de microservicios dockerizados, optimizando la utilización de recursos.
- **Visualización Clara y Operativa:** Se pone énfasis en transformar los análisis en visualizaciones entendibles, consolidando estas en un dashboard unificado, así como propuestas innovadoras como AR y VR.
- **Priorización de Seguridad y Resiliencia:** La propuesta subraya la importancia de reforzar la seguridad y la resiliencia en escenarios críticos, con una comunicación y análisis de datos mejorados.
- **Flexibilidad y Escalabilidad en la Implementación:** La arquitectura diseñada es adaptable a diferentes contextos, ofreciendo flexibilidad y posibilidad de escalar según las necesidades.
- **Mejora en la Gestión de Misiones Multidominio:** Se apunta a una gestión más eficiente en misiones multidominio, permitiendo una mejor coordinación y respuesta rápida.
- **Optimización de la Toma de Decisiones Basada en Datos:** Se busca mejorar la capacidad de análisis de información para una toma de decisiones efectiva.
- **Escalabilidad y Mantenimiento:** La arquitectura propuesta destaca por su escalabilidad, permitiendo la expansión o modificación de componentes sin afectar el funcionamiento global del sistema. Este aspecto

es crucial para adaptarse a las necesidades cambiantes y para facilitar el mantenimiento continuo.

- **Seguridad y Protección de Datos:** Se ha puesto un énfasis especial en la seguridad y en la protección de datos dentro de la arquitectura, implementando protocolos avanzados para garantizar la integridad y confidencialidad de la información, un aspecto esencial en operaciones sensibles.
- **Integración de Inteligencia Artificial:** La incorporación de tecnologías de inteligencia artificial y aprendizaje automático dentro de la arquitectura permite un análisis más profundo y predictivo de los datos, abriendo nuevas posibilidades para la anticipación y respuesta a situaciones complejas.
- **Soporte para Decisiones Basadas en Datos:** La arquitectura facilita un enfoque de toma de decisiones basado en datos, proporcionando a los usuarios finales herramientas analíticas y predictivas que ayudan en la identificación de patrones y en la toma de decisiones informadas.
- **Compatibilidad y Conectividad:** Se ha asegurado que la arquitectura sea compatible con una amplia gama de sistemas y tecnologías, facilitando una conectividad robusta y reduciendo las barreras para la integración de diferentes plataformas y herramientas.

7.1.2. Sistema CAMELOT

- **Plataforma Unificada para la Gestión de Misiones y Toma de Decisiones:** CAMELOT ha establecido un sistema integrado que centraliza la gestión de misiones y facilita la toma de decisiones. Este enfoque unificado ha demostrado ser crucial para una respuesta coordinada y efectiva en situaciones de emergencia y operaciones de seguridad.
- **Innovación en Gestión de Misiones Multidominio:** El proyecto ha marcado un hito en la gestión de operaciones multidominio, implementando soluciones vanguardistas que han revolucionado la manera de abordar desafíos complejos en distintos ámbitos de seguridad.
- **Eficiencia en la Coordinación de Múltiples Recursos:** La habilidad de CAMELOT para coordinar de manera eficiente una amplia gama de recursos, incluyendo personal, tecnologías y equipamiento, ha mejorado notablemente la ejecución de las misiones.
- **Uso Efectivo de Tecnologías Emergentes:** CAMELOT ha integrado con éxito tecnologías emergentes, como UxV y sistemas de inteligencia

artificial, optimizando la recolección de datos y el análisis situacional, lo que ha permitido tomar acciones más informadas y oportunas.

- **Desarrollo de Interfaces Intuitivas para Usuarios:** Se han creado interfaces de usuario intuitivas y fáciles de manejar, permitiendo a los operadores interactuar eficientemente con el sistema y acceder a información crítica de manera rápida y sencilla.
- **Arquitectura Basada en Microservicios y Escalable:** La adopción de una arquitectura de microservicios ha proporcionado a CAMELOT una notable escalabilidad y flexibilidad, permitiendo la incorporación o modificación de servicios sin interrupciones ni impactos negativos en el sistema global.
- **Cumplimiento de Normativas y Protección de Datos:** CAMELOT ha dado prioridad al cumplimiento de las normativas vigentes, incluyendo la protección de datos, asegurando así que la operación del sistema se alinee con los más altos estándares éticos y legales.
- **Avances en Visualización de Datos:** Se han logrado avances significativos en la visualización de datos, facilitando la comprensión y el análisis de información compleja, lo que es fundamental para la toma de decisiones informadas en situaciones críticas.
- **Impacto Positivo en la Seguridad y Vigilancia:** CAMELOT ha tenido un impacto positivo y tangible en los campos de la seguridad y la vigilancia, mejorando la capacidad de respuesta y la efectividad operativa en diversos escenarios.
- **Validación y Satisfacción de Usuarios:** La validación del sistema CAMELOT por parte de los usuarios finales ha sido extremadamente positiva, reflejando una alta satisfacción con la funcionalidad, usabilidad y los resultados obtenidos, lo que subraya el éxito del proyecto en su conjunto.

7.1.3. Sistema PREVISION

- **Plataforma Integral para Prevención y Gestión de Amenazas:** PREVISION ha desarrollado una plataforma completa que integra la prevención, detección y gestión de amenazas, utilizando tecnologías avanzadas para mejorar la respuesta y coordinación en escenarios de seguridad.
- **Implementación de Servicios Big Data:** El proyecto ha incorporado servicios Big Data para el procesamiento y análisis de grandes volúmenes

de información, lo que ha sido fundamental para identificar patrones y tendencias en datos de seguridad.

- **Ingestión de flujo de vídeo:** La plataforma está preparada para el tratamiento y procesado de flujo de vídeo a partir de cámaras CCTV y dispositivos UxV.

- **Servicios Avanzados de Detección Facial:** Se han integrado tecnologías de detección facial, permitiendo la identificación rápida y precisa de individuos en diversos entornos, lo que ha reforzado significativamente las capacidades de vigilancia y reconocimiento.

- **Aplicación de Servicios de Crawling:** PREVISION ha utilizado servicios de crawling para recolectar datos de múltiples fuentes en línea, mejorando la capacidad de recopilar información relevante para la seguridad y prevención de amenazas.

- **Detección de Personas y Comportamientos Anómalos:** El sistema integra algoritmos avanzados para detectar comportamientos anómalos y actividades sospechosas, lo que aumenta la eficacia en la identificación y prevención de posibles incidentes.

- **Análisis de Datos en Redes Sociales:** La plataforma realiza un análisis exhaustivo de datos en redes sociales, proporcionando información valiosa sobre las tendencias y las posibles amenazas que emergen en estas plataformas digitales.

- **Procesamiento de Texto y Análisis Predictivos:** Se han implementado técnicas de procesamiento de texto y análisis predictivos, permitiendo una interpretación más profunda de los datos recopilados y facilitando la anticipación a eventos de seguridad.

- **Arquitectura Flexible y Adaptable:** La arquitectura de PREVISION es altamente flexible y adaptable, lo que permite su aplicación en una variedad de contextos de seguridad, garantizando eficacia en diferentes escenarios operativos.

- **Cumplimiento de Normativas de Seguridad y Protección de Datos:** El proyecto ha mantenido un enfoque riguroso en el cumplimiento de normativas de seguridad y protección de datos, asegurando la integridad y confidencialidad de la información.

- **Avances en Visualización y Análisis de Datos:** PREVISION ha implementado innovaciones en la visualización y análisis de datos, mejorando significativamente la comprensión y el manejo de información compleja.
- **Impacto Positivo en la Seguridad Pública:** El proyecto ha contribuido de manera significativa a la seguridad pública, mejorando las capacidades de prevención, detección y respuesta a situaciones de riesgo.
- **Validación Exitosa y Reconocimiento de Usuarios:** La plataforma PREVISION ha sido validada y altamente valorada por los usuarios finales, destacando su utilidad, eficacia y mejoras en la gestión y respuesta ante diversas amenazas.

7.2. Líneas de investigación futuras

Tras la culminación de esta tesis, se han identificado varias oportunidades para ampliar la investigación en direcciones multifacéticas. Una observación clave ha sido la importancia crítica de las herramientas Big Data y su interoperabilidad en el ámbito de la gestión de misiones, destacando el potencial para su aplicación en contextos más amplios que la mera prevención de amenazas. En particular, la plataforma CAMELOT, diseñada para la gestión eficiente de múltiples dispositivos en entornos multidominio, muestra una adaptabilidad notable. Esta característica sugiere su aplicabilidad en entornos alternativos con modificaciones mínimas, abriendo puertas para su uso en escenarios novedosos, como aquellos que se exploran en el proyecto europeo *Smart Maritime and Underwater Guardian* (SMAUG) [154], beneficiándose del conocimiento y experiencia adquirida durante el desarrollo de CAMELOT.

En términos de interoperabilidad, la plataforma CAMELOT tiene el potencial de ser útil en una variedad de escenarios más allá de los que se han investigado en los proyectos CAMELOT y PREVISION. Aunque los adaptadores específicos podrían requerir ajustes para su aplicación en otras herramientas, las funcionalidades centrales de la plataforma general desarrollada en esta tesis tienen un valor considerable en una gama diversa de entornos. Una línea de investigación futura podría enfocarse en la adaptación de la arquitectura a nuevas bases de datos distribuidas y modelos avanzados de inteligencia artificial para optimizar el rendimiento en el almacenamiento, indexación y análisis de información en varios ámbitos.

Además, sería provechoso investigar la integración de escenarios adicionales en contextos similares a los abordados en PREVISION. Ampliar el espectro de prevención de amenazas mediante la incorporación de servicios variados y

la exploración de nuevas tecnologías como el *Internet of things* (IoT) podría enriquecer significativamente la gestión y respuesta ante amenazas. Esta idea ha sido considerada en la elaboración de una nueva propuesta coordinada por la UPV para el programa Horizonte Europa. Entre las propuestas, destaca el proyecto europeo *Fight against large-scale corruption and organised crime networks* (FALCON) [155], que se enfoca en la investigación e identificación de corrupción criminal.

Para finalizar, la integración de sistemas de mensajería modernos y tecnología de comunicaciones 5G, junto con la conexión con un amplio rango de sensores IoT, podría dotar a la plataforma de una capacidad aún mayor y versatilidad. La inclusión de estas tecnologías avanzadas abriría nuevas posibilidades para la optimización y eficiencia en la gestión de misiones multidominio, reforzando la utilidad y aplicabilidad de la plataforma en una diversidad de contextos operativos.

Referencias

[1] Inmigración en la ue: cruce de frontera ilegal por tierra 2013 — statista. [Online]. Available: https://es.statista.com/estadisticas/637634/cruce-de-frontera-ilegal-por-tierra-a-la-ue-por-pais-de-origen/

[2] P. Stalker, "Migration trends and migration policy in europe," *International Migration*, vol. 40, pp. 151–179, 2002.

[3] Statistics – maoc. [Online]. Available: https://maoc.eu/statistics/

[4] European drug report 2020: Key issues. [Online]. Available: https://www.emcdda.europa.eu/publications/edr/key-issues/2020_en

[5] M. R. Kenwick, B. A. Simmons, and R. J. McAlexander, "Infrastructure and authority at the state's edge: The border crossings of the world dataset," *Journal of Peace Research*, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:258394736

[6] S. Durmus, S. Uzumcu, A. A. Mert, and A. Ozturk, "Modernization challenges of command and control systems," *INCOSE International Symposium*, vol. 30, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:225621628

[7] C2 advanced multi-domain environment and live observation technologies — camelot — cordis — european commission. [Online]. Available: https://cordis.europa.eu/project/id/740736/es

[8] H. J. Cho *et al.*, "Study on control system of integrated unmanned surface vehicle and underwater vehicle," *Sensors*, 2020.

[9] A. Mihailovic *et al.*, "A framework for incorporating a national maritime surveillance system into the european common information sharing environment," in *2021 25th International Conference on Information Technology (IT)*, 2021, pp. 1–6.

[10] L. Alawneh, M. H. Said, and Z. Al-Sharif, "Towards hierarchical cooperative analytics architecture in law enforcement agencies," *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, pp. 1–6, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:3907284

[11] D. v. Wietlisbach, O. Terror in europa: : In the 70s and 80s, terrorists left a trail of blood across europe. [Online]. Available: https://www.watson.ch/wissen/schweiz/982459207-terror-in-europa-und-der-schweiz-seit-1970-diese-fakten-sollte-man-kennen

[12] Prevision – prediction and visual intelligence for security information. [Online]. Available: http://www.prevision-h2020.eu/

[13] Y. Y. Haimes and T. A. Longstaff, "The role of risk analysis in the protection of critical infrastructures against terrorism," *Risk Analysis*, vol. 22, 2002. [Online]. Available: https://api.semanticscholar.org/CorpusID:11270120

[14] W. L. Perry, B. McInnis, C. C. Price, S. Smith, and J. S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND Corporation, 2013.

[15] M. Brandt. Infographic: Between raf and is— statista. [Online]. Available: https://de.statista.com/infografik/5378/terrorattacken-in-westeuropa/

[16] C. R. Westphal, "Data mining for intelligence, fraud & criminal detection: Advanced analytics & information sharing technologies," 2008.

[17] P. de Hert and G. Boulet, "Cloud computing and trans-border law enforcement access to private sector data. challenges to sovereignty, privacy and data protection," 2013.

[18] G. Gkioka, B. Magoutas, E. Bothos, and G. Mentzas, "A hybrid data model for the assessment of border control technologies," *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*, pp. 1–8, 2022.

[19] O. Farion, A. Balendr, O. Androshchuk, A. Mostovyi, and V. Grinchenko, "Methods of extraction and analysis of intelligence to combat threats of organized crime at the border," *Journal of Human, Earth, and Future*, 2022.

[20] N. R. Adam *et al.*, "Agency interoperation for effective data mining in border control and homeland security applications," in *Digital Government Research*, 2004.

[21] K. Tomaszycki, "The interoperability of european information systems for border and migration management and for ensuring security," *Facta Universitatis, Series: Law and Politics*, 2019.

[22] T. A. Quintel, "Interoperable data exchanges within different data protection regimes: The case of europol and the european border and coast guard agency," *European Public Law*, 2020.

[23] H. Duan and S. Liu, "Unmanned air/ground vehicles heterogeneous cooperative techniques: Current status and prospects," *Science China Technological Sciences*, vol. 53, pp. 1349–1355, 2010.

[24] R. V. Hauck, "Coplink: Exploring usability of a multimedia database application for law enforcement," 1999.

[25] H. H. Abraha, "Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives," *Int. J. Law Inf. Technol.*, vol. 29, pp. 118–153, 2020.

[26] R. G. Smith, "Impediments to the successful investigation of transnational high tech crime," *Trends and issues in crime and criminal justice*, p. 1, 2005.

[27] C.-C. Chiang, "The use of adapters to support interoperability of components for reusability," *Inf. Softw. Technol.*, vol. 45, pp. 149–156, 2003.

[28] J. Potter *et al.*, "The janus underwater communications standard," in *2014 Underwater Communications and Networking (UComms)*, 2014, pp. 1–4.

[29] M. M. Marques, "Stanag 4586—standard interfaces of uav control system (ucs) for nato uav interoperability."

[30] NATO - STANAG 4748, "DIGITAL UNDERWATER SIGNALLING STANDARD FOR NETWORK NODE DISCOVERY & INTEROPERABILITY," North Atlantic Treaty Organization, Standard STANAG 4748, 2017.

[31] K. Rein, "Re-thinking standardization for interagency information sharing," 2013.

[32] Emergency data exchange language (edxl) distribution element version 2.0. [Online]. Available: https://docs.oasis-open.org/emergency/edxl-de/v2.0/edxl-de-v2.0.html

[33] Niem. [Online]. Available: https://www.niem.gov/

[34] Xml - explicación del lenguaje de marcado extensible (xml) - aws. [Online]. Available: https://aws.amazon.com/es/what-is/xml/

[35] Json. [Online]. Available: https://www.json.org/json-es.html

[36] Rest. [Online]. Available: https://www.codecademy.com/article/what-is-rest

[37] J. Tekli, E. Damiani, and R. Chbeir, "Differential soap multicasting," in *2011 IEEE International Conference on Web Services*, 2011, pp. 1–8.

[38] G. Mulligan and D. Gracanin, "A comparison of soap and rest implementations of a service based interaction independence middleware framework," *Proceedings of the 2009 Winter Simulation Conference (WSC)*, pp. 1423–1432, 2009.

[39] Data lakes ibm. [Online]. Available: https://www.ibm.com/es-es/topics/data-lake

[40] R. Hai, C. Quix, and M. Jarke, "Data lake concept and systems: a survey," *ArXiv*, vol. abs/2106.09592, 2021.

[41] Hdfs apache hadoop — ibm. [Online]. Available: https://www.ibm.com/es-es/topics/hdfs

[42] Minio — high performance, kubernetes native object storage. [Online]. Available: https://min.io/

[43] Mongodb. [Online]. Available: https://www.mongodb.com/es

[44] Apache cassandra documentation. [Online]. Available: https://cassandra.apache.org/_/index.html

[45] Nosql databases explained. [Online]. Available: https://www.mongodb.com/es/nosql-explained

[46] Sql server 2022 — microsoft. [Online]. Available: https://www.microsoft.com/es-es/sql-server/sql-server-2022

[47] Oracle — aplicaciones y plataforma en la nube. [Online]. Available: https://www.oracle.com/es/

[48] Z. Xu, Z. Yan, L. Mei, and H. Zhang, "The big data analysis of the next generation video surveillance system for public security," in *Web*, 2015.

[49] Apache kafka. [Online]. Available: https://kafka.apache.org/

[50] Apache storm. [Online]. Available: https://storm.apache.org/

[51] Elasticsearch: Motor de búsqueda y analítica distribuido oficial. [Online]. Available: https://www.elastic.co/es/elasticsearch

[52] Kibana: Explora, visualiza y descubre datos — elastic. [Online]. Available: https://www.elastic.co/es/kibana

[53] Rabbitmq. [Online]. Available: https://www.rabbitmq.com/

[54] Eclipse mosquitto. [Online]. Available: https://mosquitto.org/

[55] F. Pop, R. Prodan, and G. Antoniu, "Rm-bdp: Resource management for big data platforms," *Future Gener. Comput. Syst.*, vol. 86, pp. 961–963, 2018.

[56] Apache spark™. [Online]. Available: https://spark.apache.org/

[57] Hadoop mapreduce. [Online]. Available: https://hadoop.apache.org/docs/r1.2.1/mapred_tutorial.html

[58] Kubernetes. [Online]. Available: https://kubernetes.io/es/docs/concepts/overview/what-is-kubernetes/

[59] P. Yermalovich, "Dashboard visualization techniques in information security," *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, 2020.

[60] Grafana: The open observability platform — grafana labs. [Online]. Available: https://grafana.com/

[61] Javascript — mdn. [Online]. Available: https://developer.mozilla.org/es/docs/Web/JavaScript

[62] React. [Online]. Available: https://es.react.dev/

[63] Angular. [Online]. Available: https://angular.io/

[64] Vue.js. [Online]. Available: https://vuejs.org/guide/introduction.html#what-is-vue

[65] N. Bikakis, "Big data visualization tools," *ArXiv*, vol. abs/1801.08336, 2018.

[66] I. Drofova, M. Adamek, A. Malatinský, and M. Karhankova, "The potential of using virtual reality in the field of security control in public space," *2022 26th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, pp. 51–55, 2022.

[67] Oculus rift: Gafas de juegos de realidad. [Online]. Available: https://www.oculus.com/rift-s/?locale=es_ES

[68] Htc vive - vr, ar, and mr headsets, glasses, experiences. [Online]. Available: https://www.vive.com/us/

[69] Apple vision pro - apple. [Online]. Available: https://www.apple.com/apple-vision-pro/

[70] Microsoft hololens — tecnología de realidad mixta. [Online]. Available: https://www.microsoft.com/es-es/hololens

[71] P. N. Day, G. Ferguson, P. O. Holt, S. Hogg, and D. Gibson, "Wearable augmented virtual reality for enhancing information delivery in high precision defence assembly: an engineering case study," *Virtual Reality*, vol. 8, pp. 177–184, 2005.

[72] Unity — motor de 3d, 2d, vr y ar. [Online]. Available: https://unity.com

[73] Unreal engine. [Online]. Available: https://www.unrealengine.com/es-ES

[74] Arkit 6 - augmented reality - apple developer. [Online]. Available: https://developer.apple.com/augmented-reality/arkit/

[75] Arcore — google for developers. [Online]. Available: https://developers.google.com/ar?hl=es-419

[76] Vuforia— engine developer portal. [Online]. Available: https://developer.vuforia.com/

[77] Mixed reality toolkit. [Online]. Available: https://learn.microsoft.com/windows/mixed-reality/mrtk-unity/mrtk3-overview/

[78] D. Akila, V. R. Elangovan, R. S. Batth, D. Balaganesh, and R. Padmavathi, "The software component reusability: An efficient strategy to develop an enhanced software through using service-oriented architecture (soa)," *2022 International Mobile and Embedded Technology Conference (MECON)*, pp. 259–262, 2022.

[79] K. Bakshi, "Microservices-based software architecture and approaches," *2017 IEEE Aerospace Conference*, pp. 1–8, 2017.

[80] Docker. [Online]. Available: https://www.docker.com/

[81] A. Alanda, H. Mooduto, and R. Hadelina, "Continuous integration and continuous deployment (ci/cd) for web applications on cloud infrastructures," *JITCE (Journal of Information Technology and Computer Engineering)*, 2022.

[82] A. Elfatatry, "Microservices: A review of the costs and the benefits," 2019.

[83] L. D. Magnoni, "Modern messaging for distributed sytems," *Journal of Physics: Conference Series*, vol. 608, 2015.

[84] D. Hercog, "Tcp protocol," *Communication Protocols*, null.

[85] A. Ćatović, N. Buzađija, and S. Lemes, "Microservice development using rabbitmq message broker," *Science, Engineering and Technology*, 2022.

[86] Amqp. [Online]. Available: https://www.amqp.org/

[87] Stomp. [Online]. Available: https://stomp.github.io/

[88] Mqtt - the standard for iot messaging. [Online]. Available: https://mqtt.org/

[89] G. Castellano *et al.*, "A model-based abstraction layer for heterogeneous sdn applications," *International Journal of Communication Systems*, vol. 32, 2019.

[90] M. Doerr, C.-E. Ore, and S. Stead, "The cidoc conceptual reference model - a new standard for knowledge sharing," in *International Conference on Conceptual Modeling*, 2007.

[91] D. Q. Nguyen, "An overview of embedding models of entities and relationships for knowledge base completion," *ArXiv*, vol. abs/1703.08098, 2017.

[92] D. Liu and L. Zhao, "The research and implementation of cloud computing platform based on docker," *2014 11th International Computer Conference on Wavelet Actiev Media Technology and Information Processing(ICCWAMTIP)*, pp. 475–478, 2014.

[93] S. C. Carroll, "Mission impact analysis visualization for enhanced situational awareness," 2012.

[94] T. Rakha and A. Gorodetsky, "Review of unmanned aerial system (uas) applications in the built environment: Towards automated building inspection procedures using drones," *Automation in Construction*, 2018.

[95] G. Nugroho, M. Satrio, A. A. Rafsanjani, and R. R. T. Sadewo, "Avionic system design unmanned aerial vehicle for disaster area monitoring," *2015 International Conference on Advanced Mechatronics, Intelligent Manufacture, and Industrial Automation (ICAMIMIA)*, pp. 198–201, 2015.

[96] J. J. Ackley, R. L. Wade, and D. G. Gehring, "Future of unmanned systems interoperability," in *SPIE Defense + Commercial Sensing*, 2006.

[97] F. J. Pérez, A. García, V. Garrido, M. Esteve, and M. Zambrano, "C2 advanced multi-domain environment and live observation technologies," *Int. J. Comput. Commun. Control*, vol. 16, 2021.

[98] J. D. Pfautz *et al.*, "The role of meta-information in c2 decision-support systems," 2006.

[99] N. Li, W. Huai, and S. Wang, "The solution of target assignment problem in command and control decision-making behaviour simulation," *Enterprise Information Systems*, vol. 11, pp. 1059 – 1077, 2017.

[100] D. Bein, W. W. Bein, A. Karki, and B. B. Madan, "Optimizing border patrol operations using unmanned aerial vehicles," *2015 12th International Conference on Information Technology - New Generations*, pp. 479–484, 2015.

[101] Nato shipping centre - ais (automatic identification system) overview. [Online]. Available: https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview

[102] Y. R. Pétillot *et al.*, "Acoustic-based techniques for autonomous underwater vehicle localization," *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment*, vol. 224, pp. 293 – 307, 2010.

[103] M. A. Khalighi *et al.*, "Underwater wireless optical communication; recent advances and remaining challenges," *2014 16th International Conference on Transparent Optical Networks (ICTON)*, pp. 1–4, 2014.

[104] D. Fortun, P. Bouthemy, and C. Kervrann, "Optical flow modeling and computation: A survey," *Comput. Vis. Image Underst.*, vol. 134, pp. 1–21, 2015.

[105] Nato. [Online]. Available: https://www.nato.int/nato-welcome/

[106] Stanag 4609 imágenes de movimiento digital otan. [Online]. Available: https://www.eurolab.net/es/sektorel/askeri-testler/stanag-4609-nato-dijital-hareket-goruntuleme/

[107] Motion imagery standards board (misb) — geospatial-intelligence standards working group. [Online]. Available: https://gwg.nga.mil/gwg/focus-groups/Motion_Imagery_Standards_Board_(MISB).html

[108] App-6 nato joint military symbology. [Online]. Available: https://www.cimic-coe.org/resources/external-publications/app-6-c.pdf

[109] Luciad developer platform. [Online]. Available: https://dev.luciad.com/portal/welcome/

[110] Kml — keyhole markup language. [Online]. Available: https://developers.google.com/kml/documentation/kml_tut?hl=es

[111] Global communications — services, solutions & satellite internet — viasat. [Online]. Available: https://www.viasat.com/

[112] Protocolo internet (internet protocol) - documentación de ibm. [Online]. Available: https://www.ibm.com/docs/es/aix/7.2?topic=protocols-internet-protocol

[113] A. Sofokleous, "Review: H.264 and mpeg-4 video compression: Video coding for next-generation multimedia," *The Computer Journal*, vol. 48, no. 5, pp. 563–563, 01 2005. [Online]. Available: https://doi.org/10.1093/comjnl/bxh117

[114] Trellisware technologies, inc. [Online]. Available: https://www.trellisware.com/

[115] Darknet: definition, how it works and who uses it — myra. [Online]. Available: https://www.myrasecurity.com/en/knowledge-hub/darknet/

[116] Osint — incibe. [Online]. Available: https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder

[117] Tor project. [Online]. Available: https://www.torproject.org/es/

[118] Apache lucene. [Online]. Available: https://lucene.apache.org/

[119] Navegador web google chrome. [Online]. Available: https://www.google.com/intl/es_es/chrome/

[120] Extracción, transformación y carga de datos (etl) - microsoft learn. [Online]. Available: https://learn.microsoft.com/es-es/azure/architecture/data-guide/relational-data/etl

[121] Node-red. [Online]. Available: https://nodered.org/

[122] Apache nifi. [Online]. Available: https://nifi.apache.org/

[123] Talend — a complete, scalable data management solution. [Online]. Available: https://www.talend.com/

[124] Exif — adobe. [Online]. Available: https://www.adobe.com/es/creativecloud/file-types/image/raster/exif-file.html

[125] Pgp encryption (pretty good privacy) — fortinet. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/pgp-encryption

[126] M. Richardson and P. Domingos, "Markov logic networks," *Machine learning*, vol. 62, pp. 107–136, 2006.

[127] Twitter. [Online]. Available: https://twitter.com

[128] 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.

[129] Python. [Online]. Available: https://www.python.org/

[130] scikit-learn: machine learning in python documentation. [Online]. Available: https://scikit-learn.org/stable/

[131] A. McCallum and K. Nigam, "A comparison of event models for naive bayes text classification," *AAAI Conference on Artificial Intelligence*, 1998.

[132] I. Steinwart and A. Christmann, "Support vector machines," *Information Science and Statistics*, 2008.

[133] V. Radhika, C. Prasad, C. R. Prasad, and A. Chakradhar, "Smartphone-based human activities recognition system using random forest algorithm," 2022.

[134] Weka 3 - data mining with open source machine learning software in java. [Online]. Available: https://waikato.github.io/weka-site/index.html

[135] Ultraleap. [Online]. Available: https://www.ultraleap.com/

[136] A. I. Kapitanov, I. I. Kapitanova, V. M. Troyanovskiy, V. F. Shangin, and N. O. Krylikov, "Approach to automatic identification of terrorist and radical content in social networks messages," *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 1517–1520, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:3928904

[137] Cidoc crm. [Online]. Available: https://www.cidoc-crm.org/

[138] International council of museums. [Online]. Available: https://icom.museum/en/

[139] Upv universitat politècnica de valència. [Online]. Available: https://www.upv.es/

[140] Vmware vsphere. [Online]. Available: https://www.vmware.com/es/products/vsphere.html

[141] Esxi— hipervisor bare metal. [Online]. Available: https://www.vmware.com/es/products/esxi-and-esx.html

[142] Clearos. [Online]. Available: https://www.clearos.com/

[143] Protocolo de configuración dinámica de host (dhcp). [Online]. Available: https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

[144] Dns. [Online]. Available: https://aws.amazon.com/es/route53/what-is-dns/

[145] Apache couchdb. [Online]. Available: https://couchdb.apache.org/

[146] Servidor de torre poweredge t640 — dell españa. [Online]. Available: https://www.dell.com/es-es/shop/ipovw/poweredge-t640

[147] Yilport. [Online]. Available: https://www.yilport.com/es/puertos/default/Setubal-Portugal/716/0/0

[148] National marine electronics association. [Online]. Available: https://www.nmea.org/

[149] Teatro arriaga antzokia. [Online]. Available: https://www.teatroarriaga.eus/

[150] Ertzaintza. [Online]. Available: https://www.ertzaintza.euskadi.eus/lfr/web/ertzaintza

[151] General data protection regulation (gdpr) – official legal text. [Online]. Available: https://gdpr-info.eu/

[152] Sparql query language for rdf. [Online]. Available: https://www.w3.org/TR/rdf-sparql-query/

[153] Letscrowd – law enforcement agencies human factor methods and toolkit for the security and protection of crowds in mass gatherings. [Online]. Available: https://letscrowd.eu/

[154] Smaug eu— linkedin. [Online]. Available: https://www.linkedin.com/company/smaug

[155] Fight against large-scale corruption and organised crime networks — falcon — cordis. [Online]. Available: https://cordis.europa.eu/project/id/101121281/es