



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*La interconexión de los sistemas de información EU de gran
magnitud. Enfoque holístico.*

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Juan Antonio Torres Trives

DIRECTORES: Francisco Troncoso Pastoriza

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*La interconexión de los sistemas de información EU de gran
magnitud. Enfoque holístico.*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

Europa es un continente dinámico donde millones de personas cruzan diariamente sus fronteras. Entre enero y septiembre de 2023, se registraron 380.000 cruces fronterizos ilegales, un aumento del 17% respecto al año anterior, siendo la cifra más alta desde 2016, destacando la ruta del Mediterráneo Central con un 41% de estos cruces. El panorama es preocupante debido a recientes atentados y crisis migratorias que podrían empeorar la situación si no se adoptan medidas adecuadas.

Frente a este contexto, es esencial fortalecer los controles en las fronteras exteriores para mejorar la gestión migratoria y la seguridad interna. Los ataques terroristas en París y Bruselas han resaltado la amenaza constante que enfrenta Europa. A pesar de contar con varios sistemas de información que facilitan la labor de los guardias fronterizos y la policía, la gestión de datos presenta deficiencias significativas, como la fragmentación de la información en sistemas no interconectados, lo que genera incoherencias y "puntos ciegos" en el acceso a datos críticos.

Para resolver estos problemas, se han creado diversos sistemas de información en áreas como fronteras, visados y cooperación judicial, con el objetivo de mejorar la interoperabilidad y facilitar el intercambio de información entre los Estados miembros y otras agencias. Sin embargo, esto plantea retos en la protección de datos y los derechos fundamentales de los ciudadanos, ya que involucra el manejo de grandes volúmenes de información personal.

Este trabajo se centra en los desafíos y oportunidades inherentes a la implementación de la interoperabilidad en los sistemas de la UE, como el Sistema de Información de Schengen (SIS) y el Sistema de Entrada/Salida (EES). Utilizando una metodología cualitativa con entrevistas semiestructuradas a expertos, se busca comprender las dinámicas de la interoperabilidad, identificando la colaboración interagencial y la necesidad de un marco legal coherente como claves para mejorar la seguridad y la gestión migratoria, siempre respetando la protección de datos.

PALABRAS CLAVE

Interoperabilidad, Unión Europea, Sistemas de Información, Cooperación Policial, Control de Fronteras, Seguridad Interior.

AGRADECIMIENTOS

A mi familia, por su amor, paciencia y apoyo incondicional durante todo este proceso. Su confianza en mí ha sido mi mayor fortaleza y motivación. Este trabajo es también suyo.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción y objetivos.....	5
1.1 Introducción	5
1.2 Objetivos del trabajo	8
2 Contexto y marco teórico	10
2.1 La Agencia eu-LISA y la gobernanza.....	10
2.2 Nueva estrategia de la Agencia - 3R.....	13
2.3 Necesidad de la Interoperabilidad en los sistemas de UE.....	14
2.4 Principales sistemas de información de la UE.....	17
2.4.1 El Sistema de Información de Schengen (SIS).....	17
2.4.2 El sistema Eurodac	17
2.4.3 El Sistema de Información de Visados (VIS).....	18
2.4.4 El Sistema de Entradas y Salidas (EES).....	19
2.4.5 El Sistema Europeo de Información y Autorización de Viajes (ETIAS).	19
2.4.6 El Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN).....	20
2.4.7 Otros sistemas relacionados.....	20
2.5 Costes económicos y financiación de la IO.	21
3 Normativa, principios y políticas de la agencia	23
3.1 Principios y políticas de la Agencia	23
3.2 Normativa sobre Interoperabilidad, sistemas y seguridad	24
3.3 Marco europeo de la interoperabilidad	26
4 Metodología de investigación	29
4.1 Investigación cualitativa	29
4.2 Marco teórico y el modelo de Novakouski	36
4.2.1 Niveles de interoperabilidad en el modelo de Novakouski	38
4.2.2 Factores que influyen en la Interoperabilidad	39
5 Componentes técnicos y arquitectura de la interoperabilidad.....	43
5.1 Componentes clave	43
5.1.1 Portal Europeo de Búsqueda (ESP)	43
5.1.2 Repositorio común de identidades (CIR)	43
5.1.3 Detector de identidades múltiples (MID)	44

5.1.4 Servicio de comparación biométrica compartida (sBMS).....	44
5.1.5 Repositorio Central de Informes y Estadísticas (CRRS).....	44
5.2 Arquitectura global de la IO.....	44
6 Objetivos y oportunidades de la interoperabilidad.....	48
6.1 Objetivos técnicos y de negocio.....	48
6.1.1 Interconexión y complementariedad de los sistemas.....	48
6.1.2 Enfoque modular y adaptabilidad tecnológica.....	49
6.2 Oportunidades para los actores clave.....	50
6.2.1 Para la Agencia.....	50
6.2.2 Para los sistemas de interoperabilidad.....	51
6.2.3 Para los Estados Miembros.....	52
6.2.4 Para Frontex y Europol.....	52
7 Impulsores, barreras y desafíos de la interoperabilidad.....	54
7.1 Impulsores principales.....	54
7.1.1 Grado de reutilización y uso compartido.....	54
7.1.2 Migración y planificación de la recuperación ante desastres.....	55
7.1.3 Adopción del formato de mensaje universal (UMF) y arquitectura SOA.....	56
7.2 Barreras y desafíos.....	57
8 Derechos fundamentales y protección de datos.....	60
9 Análisis.....	62
10 Conclusiones y líneas futuras.....	65
11 Bibliografía.....	67

ÍNDICE DE FIGURAS

Figura 2-1 Principales elementos de la Agencia (fuente: euLISA [13])	11
Figura 3-1 Marco Europeo de Interoperabilidad (fuente: Vernadat 2009 [32]).....	27
Figura 4-1 Métodos de Investigación (fuente: web Question Pro [45]).....	31
Figura 4-2 Diagrama de la metodología empleada (Fuente: Elaboración propia del autor)	33
Figura 4-3 Modelo de interoperabilidad de Novakouski (Fuente: elaboración propia del autor)....	38
Figura 5-1 Esquema de componentes IO (fuente: elaboración propia del autor).....	45
Figura 5-2 Conexión de sistemas relacionados con la IO (fuente: euLISA [13])	47

ÍNDICE DE TABLAS

Tabla 4-1 Análisis comparativo de la metodología (fuente: elaboración propia del autor)	32
Tabla 9-1 Oportunidades y Desafíos	62

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

En los últimos años, la Unión Europea (en adelante UE) ha venido experimentando un incremento de los cruces irregulares de fronteras, así como una amenaza continua para su seguridad interior, como ha quedado demostrado por una serie de atentados terroristas que sufrieron algunos Estados Miembros [1]. Los ciudadanos de la UE confían en que los controles de personas, tanto en las fronteras exteriores como en las interiores del espacio Schengen, sean efectivos para mejorar la gestión migratoria y fortalecer la seguridad interna. Estos desafíos han evidenciado de manera abrupta la urgente necesidad de fortalecer de forma integral las herramientas de información de la UE destinadas a la gestión de fronteras, la migración y la seguridad [2].

La ausencia de fronteras interiores en el espacio Schengen exige un manejo sólido y fiable de la circulación de personas por las fronteras exteriores. Esta es una condición previa para garantizar un alto nivel de seguridad interior y la libre circulación de personas dentro de este espacio. Al mismo tiempo, la ausencia de fronteras interiores significa que, como medida compensatoria, las autoridades policiales de los Estados miembros tendrán acceso a ciertos datos sobre personas. Existen varios sistemas de información a escala de la UE que proporcionan a los guardias de fronteras y agentes de policía información pertinente sobre ellas, pero la arquitectura de la gestión de estos datos es manifiestamente mejorable [3].

La utilización de los sistemas de información de la Unión Europea debería ser optimizada para ser más eficiente y efectiva, siempre respetando los derechos fundamentales, especialmente el derecho a la protección de datos personales. Esto es crucial para garantizar la protección de las fronteras externas de la UE, optimizar la gestión de los flujos migratorios y fortalecer la seguridad interna en beneficio de todos los ciudadanos. Este enfoque realza la necesidad de un manejo cuidadoso y coordinado de los datos, garantizando que las medidas de seguridad no comprometan los derechos individuales y que se logre una mejora en la operativa de los sistemas de información en el contexto de la seguridad fronteriza y la gestión migratoria.

Ya existen varios sistemas de información a nivel de la UE, y actualmente se están desarrollando otros nuevos para ofrecer información relevante a la guardia de fronteras, así como a los agentes de inmigración y de policía. Para que esta asistencia sea efectiva, la información suministrada por los sistemas de información de la UE debe ser completa, precisa y confiable; sin embargo, hay deficiencias estructurales en la arquitectura de gestión de estos sistemas.

Por otro lado, la interoperabilidad (en adelante IO), desempeña un papel cada vez más importante en el campo de las tecnologías de la información. El concepto de “interoperabilidad” se analizará con más detalle a lo largo del presente trabajo, por ahora, en el marco de este, significa la capacidad de los

sistemas y componentes para interactuar entre sí basándose en el uso de las tecnologías de la información y las comunicaciones (TIC) [4].

En este contexto, las autoridades nacionales se encuentran ante un escenario complicado de sistemas de información que se gestionan de manera diversa. Además, la arquitectura de gestión de los datos relacionados con las fronteras y la seguridad interna es fragmentada, ya que se almacenan de forma aislada en sistemas no interconectados, lo que genera áreas de opacidad. Como resultado, los sistemas de información de la UE no son interoperables, lo que impide el intercambio y la compartición de datos necesarios para que las autoridades y funcionarios competentes accedan a la información requerida en el momento y lugar adecuados [5]. La interoperabilidad de los sistemas de información a nivel de la UE puede desempeñar un papel importante en la eliminación de las actuales áreas de opacidad que permiten que cualquier persona, incluidas aquellas que podrían estar involucradas en actividades terroristas, esté registrada en diversas bases de datos que no están conectadas entre sí y que presentan diferentes identidades [6].

Para mejorar la gestión de las fronteras exteriores y la seguridad interior de la UE, la Comisión Europea presentó varias propuestas para mejorar y ampliar los sistemas europeos de información sobre fronteras y seguridad. Como parte de un proceso más amplio para maximizar su uso, la Comisión presentó propuestas legislativas para dos reglamentos en diciembre de 2017 (modificados en junio de 2018) [7], que establecen un *marco de interoperabilidad* entre los sistemas de información de la UE en el ámbito de fronteras y visados, y sobre cooperación policial y judicial, asilo y migración. Una vez finalizado el procedimiento legislativo en primera lectura en el Parlamento y en el Consejo, los colegisladores firmaron los actos finales el 20 de mayo de 2019 y se publicaron en el Diario Oficial dos días después. Ambas leyes entraron en vigor el 11 de junio de 2019. Las nuevas normas tienen como objetivo mejorar los controles en las fronteras exteriores de la UE, permitir una mejor detección de las amenazas a la seguridad y el fraude de identidad y ayudar a prevenir y combatir la migración irregular [8].

La IO es una de las principales características de los *sistemas abiertos* y se logra mediante el uso de conjuntos acordados de estándares abiertos para fomentar el uso de software de código abierto. Una de las propiedades básicas de estos sistemas es precisamente la IO, la capacidad de interactuar entre sí. Los sistemas de información abiertos tienen una serie de características comunes en diversos aspectos de su creación y aplicación. Son sistemas que constan de componentes que se comunican entre sí a través de interfaces estándar y enfatizan el aspecto sistémico de un sistema de información abierto [9].

La interacción de los sistemas de información abiertos (OIS) está determinada por la compatibilidad de los componentes de software y hardware y, por lo tanto, de los métodos y medios de intercambio de datos; por lo tanto, la IO refleja la capacidad de los sistemas para interactuar sin ninguna conversión de información adicional.

Este enfoque permite procesar, transmitir y recibir más información en menos tiempo, lo que mejora el rendimiento del sistema, aumenta la confiabilidad en su conjunto (debido al uso de tecnologías estándar y bien desarrolladas en su diseño), reduce el riesgo de pérdida y distorsión de información o aparición de errores durante su transmisión (debido a la falta de necesidad de transformaciones de información adicionales), y también facilita y acelera la instalación oportuna de protección contra amenazas externas (debido a su alto nivel de compatibilidad del sistema). Por tanto, las propiedades de IO permiten aumentar la eficiencia del funcionamiento de los sistemas.

En este sentido, muchas empresas enfrentan el desafío de garantizar la IO entre sus sistemas de información, lo que implica la capacidad de estos sistemas para comunicarse, compartir datos y operar juntos de manera eficiente. Sin embargo, el grado en que estos sistemas cumplen con esta propiedad varía considerablemente entre organizaciones. Esto se debe a la diversidad de soluciones tecnológicas disponibles en el mercado, que presentan diferentes niveles de interoperabilidad. Algunas empresas pueden implementar sistemas altamente integrados, mientras que otras pueden depender de soluciones más fragmentadas.

La aparición de una amplia gama de tecnologías de la información, cada una con su propio enfoque hacia la interoperabilidad, ha incrementado la necesidad de herramientas estandarizadas para evaluar de manera consistente la efectividad de los sistemas en este aspecto. Estas herramientas deben permitir a las empresas medir cómo sus soluciones tecnológicas cumplen con los requisitos de interoperabilidad, identificar brechas y mejorar la integración entre sistemas, lo que facilita la toma de decisiones informadas y la optimización de procesos.

Este trabajo se centrará específicamente en los sistemas operados por la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos a Gran Escala en el Espacio de Libertad, seguridad y Justicia (eu-LISA), en adelante la Agencia, que actualmente gestiona y desarrolla varios sistemas clave para la seguridad y las fronteras de la UE, incluyendo los siguientes:

- ❖ **VIS (Sistema de Información de Visados):** Este sistema permite a los Estados miembros de la UE compartir información sobre solicitudes de visado de corta duración, lo que contribuye a una gestión coordinada y eficiente en las fronteras exteriores de la Unión.
- ❖ **SIS (Sistema de Información Schengen):** Como el sistema más grande de intercambio de información en Europa para cuestiones de seguridad y fronteras, el SIS proporciona alertas sobre personas y objetos relacionados con delitos graves, mejorando la cooperación entre autoridades policiales y judiciales de los Estados miembros.
- ❖ **EURODAC (Sistema Europeo de Comparación de Huellas Dactilares):** Este sistema recolecta y compara huellas dactilares de solicitantes de asilo y de personas que cruzan ilegalmente las fronteras externas de la UE, facilitando tanto la identificación como la gestión del proceso de asilo a nivel europeo.
- ❖ **EES (Sistema de Entrada/Salida):** En operación para registrar las entradas y salidas de ciudadanos de terceros países en las fronteras externas de la zona Schengen, el EES optimiza la gestión fronteriza y mejora el control sobre los flujos migratorios.
- ❖ **ETIAS (Sistema Europeo de Información y Autorización de Viajes):** En fase de implementación, el ETIAS permitirá el control previo de visitantes exentos de visado que deseen ingresar al área Schengen, reforzando así tanto la seguridad como la gestión de movilidad dentro de la UE.
- ❖ **ECRIS-TCN (Sistema Europeo de Información de Antecedentes Penales para Nacionales de Terceros Países):** Este sistema facilita el intercambio rápido y eficaz de información sobre antecedentes penales de ciudadanos de países no pertenecientes a la UE, apoyando a las autoridades judiciales y policiales en sus tareas de seguridad.

La Agencia desempeña un papel crucial en la implementación y desarrollo de la IO de estos sistemas informáticos en el ámbito de la justicia y los asuntos de interior. Además de gestionar estos sistemas, desarrolla y mantiene los componentes de interoperabilidad, como el Portal Europeo de Búsqueda (ESP), el Repositorio de Identidades Múltiples (MID) y el Comparador Biométrico Compartido (sBMS), entre otros. Su trabajo contribuye al éxito de las políticas de la UE en seguridad y migración, apoyando a los Estados miembros en su objetivo de lograr una Europa más segura y mejor conectada. [10]

La actual falta de interoperabilidad (IO) en los sistemas genera un problema destacado tanto por los fabricantes como por la comunidad global de la información [11]. La incapacidad en la resolución de este caso puede generar una serie de consecuencias negativas. Por un lado, dificulta la aplicación y expansión de los sistemas tecnológicos, ya que los usuarios enfrentan limitaciones al intentar integrar tecnologías distintas. Esto reduce la capacidad de elegir entre diversas soluciones tecnológicas, lo que, a su vez, afecta la competitividad de las empresas de tecnología de la información (TI). La IO es clave para que las organizaciones ofrezcan productos adaptables y versátiles en un entorno tecnológico dinámico.

Uno de los impactos más graves de esta carencia se observa en el intercambio de información, que resulta ser crítico en áreas como la seguridad fronteriza y las fuerzas del orden. Para los guardias

fronterizos y la policía, que dependen de datos precisos y en tiempo real para la toma de decisiones, la falta de interoperabilidad puede retrasar la comunicación y dificultar la coordinación, lo que compromete la eficacia en situaciones urgentes.

Además, este menoscabo tendrá un impacto negativo en la organización de la transformación digital en varios países, ya que el desarrollo de un sistema de gobierno electrónico depende del uso eficiente de diversas tecnologías. La IO es fundamental para conectar sistemas de información y servicios, lo que permite que las administraciones públicas, empresas y ciudadanos interactúen de manera efectiva.

En los últimos tiempos, garantizar la IO a través del uso de normas de Tecnologías de la Información y la Comunicación (TIC) se ha convertido en un aspecto obligatorio y estratégico dentro de las políticas TIC de la Unión Europea. El Reglamento (UE) N° 1025/2012 sobre la normalización europea refuerza la necesidad de utilizar estándares TIC comunes para mejorar la interoperabilidad y asegurar que los sistemas y servicios electrónicos puedan operar de forma conjunta y sin problemas [12]. La implementación de estas normas es esencial para el desarrollo de infraestructuras digitales sólidas y para la prestación eficaz de servicios públicos electrónicos a nivel nacional y europeo.

El propósito de este trabajo es analizar en profundidad los desafíos que implica la implementación de la IO en los sistemas gestionados por la Agencia, centrándose en el contexto de la seguridad y la gestión de fronteras en la Unión Europea (UE). A través de este análisis, se busca proporcionar una comprensión más clara de los obstáculos que surgen al integrar sistemas de información dispares y fragmentados, al mismo tiempo que se identifican los beneficios que pueden derivarse de una interoperabilidad bien estructurada. Esto es especialmente importante en el ámbito de la UE, donde la colaboración entre Estados miembros y la optimización de los datos compartidos son fundamentales para mejorar la eficiencia en la seguridad y la migración.

Pretende también ofrecer soluciones técnicas y organizativas que permitan maximizar las oportunidades de los sistemas de información existentes, como el Sistema de Información Schengen (SIS) y el Sistema de Información de Visados (VIS). Estas soluciones pueden incluir medidas como el uso de estándares tecnológicos comunes, el desarrollo de interfaces compartidas o la mejora de la infraestructura de datos. Además, se propone explorar el desarrollo de nuevas acciones complementarias que aborden las carencias actuales, asegurando una integración eficaz y segura entre los diferentes sistemas de información.

El objetivo final persigue establecer un *marco de interoperabilidad* que permita a la Agencia y a los Estados miembros de la UE gestionar los sistemas de información de manera integrada, reduciendo los obstáculos al intercambio de datos y mejorando la capacidad de respuesta frente a amenazas de seguridad y desafíos migratorios.

1.2 Objetivos del trabajo

Este trabajo de investigación se centra en los retos y oportunidades asociados con la implementación de la IO en los sistemas de información gestionados por la Agencia. La cuestión central que guía este análisis es: "¿Cuáles son los retos y oportunidades que surgen con la implementación de la interoperabilidad?"

Para abordar esta pregunta principal, se explorarán dos subpreguntas fundamentales:

- ❖ ¿Qué desafíos en materia de adquisiciones, gobernanza, gestión de recursos e implementación operativa conlleva la interoperabilidad?: Esta subpregunta se centra en identificar los obstáculos que enfrenta la Agencia en la implementación de sistemas interoperables, incluyendo problemas relacionados con la adquisición de tecnología, la estructura de gobernanza, y la gestión eficiente de los recursos disponibles. Los desafíos en estos ámbitos pueden afectar la capacidad de los Estados miembros para colaborar eficazmente y asegurar la protección de datos y la seguridad de la información.

- ❖ ¿Qué oportunidades proporcionará la interoperabilidad?: Aquí se examinará cómo la interoperabilidad puede beneficiar a ciudadanos, Estados miembros e instituciones de la UE al optimizar el uso de los datos disponibles. Se explorarán las posibilidades de mejorar la seguridad, facilitar el movimiento de personas y bienes, y apoyar la toma de decisiones informadas en políticas de migración y seguridad.

Al abordar estas preguntas, se espera ofrecer una comprensión más clara de cómo la interoperabilidad no solo enfrenta desafíos, sino que también abre nuevas oportunidades para mejorar la seguridad y la eficacia en la gestión de la información en el espacio de libertad, seguridad y justicia de la UE.

2 CONTEXTO Y MARCO TEÓRICO

2.1 La Agencia eu-LISA y la gobernanza.

La creación de la Agencia en 2011 marcó un hito importante en la gestión de los sistemas de información a gran escala en el ámbito de la justicia y los asuntos de interior de la Unión Europea. Comenzó sus operaciones el 1 de diciembre de 2012, y en sus primeros años estuvo enfocada exclusivamente en tres sistemas clave: el Sistema de Información de Schengen (SIS), el Sistema de Información de Visados (VIS) y EURODAC, la base de datos europea para el procesamiento de solicitudes de asilo mediante la comparación de huellas dactilares. Estos sistemas permitieron mejorar la cooperación entre los Estados miembros, especialmente en la gestión de fronteras y en la lucha contra el crimen transfronterizo.

El Reglamento (UE) n.º 1077/2011, artículo 1, apartado 2, establece las bases legales para las funciones iniciales de la Agencia, que se limitaban a la operación y gestión técnica de estos sistemas. No obstante, a partir de 2018, la Agencia asumió nuevas responsabilidades, expandiendo su ámbito de actuación con la gestión del Sistema de Entrada/Salida (EES), que registra las entradas y salidas de nacionales de terceros países en las fronteras exteriores de la UE; el Sistema Europeo de Información de Antecedentes Penales de Nacionales de Terceros Países (ECRIS-TCN), que facilita el intercambio de información entre Estados miembros sobre condenas penales; y el Sistema Europeo de Información y Autorización de Viajes (ETIAS), diseñado para mejorar la seguridad y los controles de viajes en la UE.

Este crecimiento en su mandato ha consolidado a la Agencia como un actor crucial en la digitalización y modernización de la seguridad y gestión de fronteras dentro de la UE, permitiendo un enfoque más integrado y eficiente en el tratamiento de datos. A medida que se ampliaron las capacidades de la Agencia, también lo hicieron sus responsabilidades en términos de interoperabilidad, asegurando que todos estos sistemas puedan compartir información de manera fluida y efectiva, facilitando una respuesta coordinada y rápida a amenazas y retos en seguridad.

Uno de los aspectos más importantes de su operación es la capacidad de garantizar la disponibilidad de estos sistemas 24 horas al día, los siete días de la semana, lo que es esencial para las operaciones de control fronterizo y para el acceso a datos en tiempo real por parte de las autoridades competentes. Además, la Agencia debe garantizar que todos los sistemas operen bajo estrictas medidas de seguridad y protección de datos, lo que es clave en el contexto del Reglamento General de Protección de Datos (GDPR). Estas medidas incluyen la implementación de protocolos avanzados de encriptación, controles de acceso y auditorías regulares para proteger la integridad de los datos personales procesados.

La ubicación de las diferentes instalaciones de la Agencia también responde a su estrategia de seguridad y operatividad. Mientras que la sede administrativa está situada en Tallin, Estonia, la gestión operativa de los sistemas se lleva a cabo en Estrasburgo, Francia, con una infraestructura de respaldo en

St Johan en Pongau, Austria, lo que permite garantizar la continuidad del servicio incluso en caso de incidentes o desastres.

En términos de interoperabilidad, la Agencia ha sido un pilar esencial para garantizar la integración y cooperación entre los diferentes sistemas de información a nivel europeo, lo que permite un flujo de información más eficaz entre los Estados miembros. Esto es crucial para mejorar la coordinación en la lucha contra el terrorismo, el crimen organizado y la gestión de la inmigración irregular. Además, su labor en la protección de datos ha sido fundamental para asegurar que los derechos fundamentales de los ciudadanos se respeten, tal como establece la Carta de Derechos Fundamentales de la UE.

El progreso de la Agencia en la gestión de estos sistemas ha fortalecido la seguridad en el espacio de libertad, seguridad y justicia de la UE, contribuyendo no solo a la protección de las fronteras exteriores, sino también a la mejora de la cooperación policial y judicial en toda Europa.

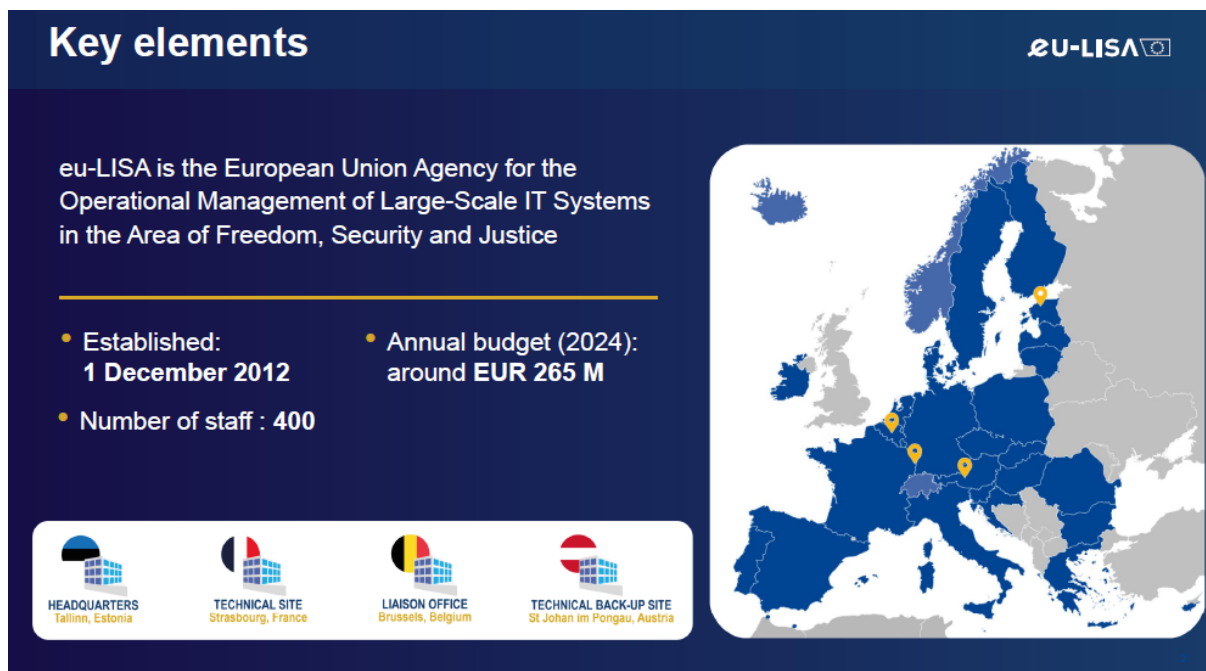


Figura 2-1 Principales elementos de la Agencia (fuente: euLISA [13])

Administrativamente, la Agencia eu-LISA, que gestiona los sistemas de información de gran escala en el ámbito de la justicia y los asuntos de interior de la Unión Europea, está organizada de la siguiente manera:

- ❖ **Sede administrativa:** La sede administrativa de eu-LISA está ubicada en Tallin, Estonia. Desde esta ubicación, se lleva a cabo la coordinación de las actividades generales de la Agencia, incluidas las tareas de gestión estratégica, la planificación y el desarrollo de políticas.
- ❖ **Sede operativa:** La sede operativa se encuentra en Estrasburgo, Francia. Aquí es donde se gestionan y supervisan directamente los sistemas de información más importantes, como el SIS, VIS, EURODAC, EES, ETIAS y ECRIS-TCN. En esta sede se realiza la administración técnica y el funcionamiento diario de los sistemas de interoperabilidad, así como la implementación de actualizaciones y mejoras tecnológicas.
- ❖ **Centro de respaldo:** El centro de respaldo de la Agencia está ubicado en St Johann im Pongau, Austria. Este centro es fundamental para garantizar la continuidad operativa de los sistemas de información gestionados por la Agencia. En caso de que haya una interrupción en la sede operativa en Estrasburgo, el centro de respaldo en Austria está diseñado para tomar el control y asegurar la disponibilidad continua de los sistemas críticos.
- ❖ **Consejo de Administración:** La Agencia está gobernada por un Consejo de Administración, compuesto por representantes de los Estados miembros de la UE y la Comisión Europea. El Consejo de Administración es responsable de definir las directrices estratégicas y operativas de

la Agencia, así como de aprobar el presupuesto, los planes de trabajo y las principales decisiones administrativas y operativas.

- ❖ **Director Ejecutivo:** El director ejecutivo es la autoridad administrativa y operativa principal de la Agencia. Es nombrado por el Consejo de Administración y es responsable de la gestión diaria de la Agencia, la implementación de sus actividades y la supervisión de los sistemas bajo su administración. El director ejecutivo actúa como representante de la Agencia y supervisa la ejecución de las estrategias y objetivos definidos por el Consejo de Administración.
- ❖ **Departamentos:** La Agencia se organiza en varios departamentos que se encargan de diferentes áreas operativas y técnicas, incluyendo:
 - Departamento de Operaciones: Responsable de la gestión técnica y operativa de los sistemas de información.
 - Departamento de Tecnología de la Información: Gestiona las infraestructuras de TI, el desarrollo de nuevos sistemas y la implementación de la interoperabilidad.
 - Departamento de Seguridad: Encargado de garantizar la seguridad de la información y la protección de los datos gestionados por los sistemas.
 - Departamento Legal y de Cumplimiento: Asegura que las actividades de la Agencia cumplan con la normativa europea, en especial en cuanto a protección de datos y derechos fundamentales.
 - Departamento de Recursos Humanos y Administración: Gestiona los recursos humanos, la formación del personal y las actividades administrativas.

La estructura administrativa de la Agencia está diseñada para operar de manera eficiente y alinearse con los objetivos de interoperabilidad, seguridad y manejo de sistemas de información a gran escala dentro de la Unión Europea. Este enfoque organizativo permite una gestión efectiva de los recursos y facilita la coordinación entre las distintas sedes y componentes operativos. Al gestionar sistemas fundamentales como SIS, VIS, EURODAC, EES y ETIAS, la Agencia asegura la continuidad operativa las 24 horas del día, los siete días de la semana, mientras implementa estrictas medidas de seguridad para proteger la integridad y la confidencialidad de los datos.

Las funciones administrativas abarcan la supervisión estratégica desde la sede en Tallin, la gestión operativa centralizada en Estrasburgo y la implementación de medidas de respaldo técnico en St. Johann im Pongau. Esta estructura descentralizada fomenta la resiliencia organizativa y asegura una rápida respuesta ante desafíos técnicos o de seguridad. La Agencia también prioriza la transparencia y la protección de datos, ofreciendo herramientas accesibles como formularios de contacto y avisos de privacidad detallados para mantener una comunicación abierta con los ciudadanos, reforzando su compromiso con los principios de protección de datos de la UE y la colaboración eficiente en el ámbito transnacional.

La Agencia gestiona sus funciones administrativas a través de una estructura descentralizada que asegura eficacia y resiliencia organizativa. Su sede en Tallin, Estonia, se encarga de la supervisión estratégica, mientras que las operaciones centrales son gestionadas desde Estrasburgo, Francia. Además, se implementan medidas de respaldo técnico desde St. Johann im Pongau, Austria, lo que garantiza una respuesta ágil ante posibles incidentes técnicos o desafíos de seguridad. Esta distribución permite optimizar recursos y coordinar esfuerzos en un marco de interoperabilidad paneuropeo.

Asimismo, la Agencia refuerza su compromiso con la transparencia y la protección de datos, pilares fundamentales en su interacción con los ciudadanos y las partes interesadas. A través de herramientas accesibles como formularios de contacto en su sitio web y avisos de privacidad claros, la Agencia facilita la comunicación abierta y la gestión responsable de los datos personales, conforme a los principios establecidos por la normativa europea de protección de datos. Este enfoque no solo asegura el cumplimiento legal, sino que también fomenta la confianza pública y la colaboración eficiente entre los

Estados miembros, consolidando su papel en la gestión operativa de los sistemas de información a gran escala en el espacio de libertad, seguridad y justicia.

2.2 Nueva estrategia de la Agencia - 3R

A finales de 2023, la Agencia junto con la CE y el Parlamento Europeo aprobó una nueva estrategia de IO y su cronograma propuesto fue aprobado por el Consejo de Justicia y Asuntos de Interior de la UE el 19 de octubre de 2023 [14]. Esta aprobación por parte de los ministros y las instituciones de la UE marca el camino a seguir por la Agencia y orienta la entrega de todos los componentes de la Arquitectura de Interoperabilidad en los próximos años. Tanto la hoja de ruta como el cronograma revisado son resultado de una estrategia de resolución propuesta por la Agencia para la implementación de la Arquitectura de Interoperabilidad general, conocida como la estrategia de las 3R: Removilizar, Resolver y Renovar [15].

Aprobada por el máximo órgano de gobierno de la Agencia, el Consejo de Administración (MB), esta estrategia se ha implementado activamente desde junio de 2023, lo que ha dado lugar a dos lanzamientos exitosos de versiones avanzadas de EES. Estos lanzamientos crearon las condiciones necesarias para que los Estados miembros y los países asociados continuaran con sus pruebas y marcaran un progreso claro en el renovado impulso hacia la interoperabilidad.

Sobre la base de estos éxitos iniciales, la Agencia ha ampliado el modelo ágil desarrollado a través de la estrategia de resolución de las 3R a todas las áreas de los Programas de Interoperabilidad, creando así un enfoque operativo y una hoja de ruta concretos y sólidos para la entrega y la implementación de todo el programa.

Principales Puntos de la nueva estrategia:

- ❖ Aprobación y Colaboración
 - La hoja de ruta fue respaldada por el Consejo de Administración de la Agencia (MB), destacando la colaboración cercana con los Estados miembros, la Comisión Europea y otros cuerpos de gobernanza para asegurar un entendimiento y apoyo completos de la nueva propuesta.
- ❖ Implementación Activa
 - Desde junio de 2023, la estrategia 3R ha llevado a dos lanzamientos exitosos de versiones avanzadas del Sistema de Entrada/Salida (EES), creando condiciones necesarias para que los Estados miembros y países asociados avancen en sus pruebas y logren un progreso claro hacia la interoperabilidad.
- ❖ Modelo Ágil
 - Basándose en estos éxitos iniciales, eu-LISA ha ampliado el modelo ágil desarrollado a través de la estrategia 3R a todas las áreas de los Programas de Interoperabilidad, estableciendo un enfoque operativo robusto y una hoja de ruta para la entrega e implementación de toda la Arquitectura de Interoperabilidad.
- ❖ Enfoque en las Necesidades de los Interesados
 - La implementación de la estrategia se basa en un enfoque de olas claro durante los próximos tres años, con entregables del sistema alineados con los objetivos comerciales centrales. Se destaca la importancia de entender y abordar las necesidades de todos los interesados, desde transportistas hasta operadores de puntos de control fronterizo.
- ❖ Compromiso con la Transformación Digital
 - eu-LISA está comprometida a alcanzar la "línea de meta" de la hoja de ruta de interoperabilidad, apoyando a la zona Schengen en sus aspiraciones de transformación digital. Esto implica un enfoque estratégico y una determinación constante para gestionar

y desarrollar sistemas informáticos a gran escala que simplifiquen el trabajo de los profesionales y sirvan a los ciudadanos de manera efectiva.

Esta nueva estrategia y el enfoque colaborativo establecido son fundamentales para avanzar en la interoperabilidad y el desarrollo, así como la implementación de sistemas de información eficaces en el contexto de la seguridad y justicia en la Unión Europea.



Figura 2-2 Imágenes institucionales de la Agencia (fuente: euLISA [13])

2.3 Necesidad de la Interoperabilidad en los sistemas de UE

Se entiende por interoperabilidad la capacidad de dos o más sistemas de intercambiar información y de utilizar la información obtenida como resultado del intercambio [16]. Para lograr la IO, debe garantizarse la accesibilidad a los datos a través de cualquier otro sistema de datos electrónicos interoperables. Todos los estándares, términos, valores de campo y documentos utilizados deben entenderse de la misma manera y transmitirse sin pérdidas ni distorsiones entre los dispositivos/sistemas electrónicos. La IO en los sistemas de la UE debe garantizarse no sólo a nivel técnico mediante el uso de protocolos de comunicación estándar, sino también a niveles superiores (semántico y organizativo). Se debe proporcionar una visión común para armonizar los estándares semánticos para la recopilación y el acceso a metadatos. Los sistemas pertinentes deben contar con servicios de comparación biométrica compartidos, un depósito de datos común, una interfaz de búsqueda única e interconectividad de los sistemas [17].

A raíz de una solicitud de Países Bajos en el año 2016 [18], durante su presidencia de turno de la UE, en 2019, se estableció un nuevo marco jurídico entre los sistemas de la Agencia en el ámbito de las fronteras y los visados (Reglamento (UE) 2019/817) y la policía, la migración, el asilo y la cooperación judicial (Reglamento (UE) 2019/818). El objetivo de estas regulaciones es crear mejores comunicaciones entre sistemas, prevenir la inmigración ilegal, crear una mayor seguridad y mitigar las lagunas de información.

Existe preocupación, como no puede ser de otra manera, por la protección de los datos personales y los derechos fundamentales, y se garantiza que las organizaciones encargadas de hacer cumplir la ley y sus miembros accedan a la información necesaria a su disposición [19]. Si bien existen sistemas que ayudan a los guardias fronterizos con información relevante, estos sistemas tienen varias deficiencias asociadas que pueden afectar a las autoridades nacionales. Las principales deficiencias son: funcionalidades deficientes de los sistemas de información actuales, lagunas en la arquitectura de gestión de datos de la UE, un panorama dinámico de sistemas de información regulados y una arquitectura de

gestión de datos fragmentada para el control y la protección de fronteras. Los actuales sistemas de información de control fronterizo y seguridad interior dentro de la UE cubren una amplia variedad de funcionalidades; sin embargo, las funcionalidades de los sistemas actuales tienden a tener puntos débiles e inconvenientes. Al observar los procedimientos de control fronterizo aplicados a varios viajeros, hay deficiencias en algunos procedimientos y en los sistemas de información de control fronterizo utilizados. Además, es necesario optimizar la eficiencia de los nuevos sistemas de aplicación de la ley. Y por eso, es necesaria una mejora de estos sistemas nuevos y actuales.

Otro problema crítico en la arquitectura de gestión de datos de la UE es la persistencia de lagunas que afectan los controles fronterizos, particularmente para ciertos grupos de pasajeros, como los titulares de visas de larga duración de terceros países. Esta fragmentación dificulta el seguimiento eficiente de estas personas, lo que puede generar situaciones en las que falte información crucial para las autoridades fronterizas. Además, existe una disparidad en la información disponible antes de la entrada en la frontera para ciertos nacionales de terceros países, especialmente aquellos a quienes se les ha denegado la visa, creando brechas significativas en la seguridad. Esto plantea la cuestión de si es necesario abordar dichas lagunas a través de la creación de sistemas de información adicionales o, alternativamente, mejorar los existentes para optimizar el flujo de datos y garantizar controles más robustos y eficientes.

A nivel de la UE, los guardias de fronteras y los agentes de policía en particular se enfrentan a un panorama dinámico de sistemas de información regulados de manera diferente. Tal complejidad crea dificultades prácticas explícitas sobre qué bases de datos en una situación determinada deben revisarse. Además, los Estados miembros no están interconectados a todos los sistemas existentes actualmente. Esto se puede solucionar creando una interfaz de búsqueda única que permita a diferentes nacionales acceder a los sistemas.

Actualmente, debido a contextos legales, institucionales y políticos, la arquitectura de gestión de datos de la UE está fragmentada, ya que toda la información necesaria está dispersa en múltiples sistemas, en su mayoría no interconectados. Las bases de datos son inconsistentes y las diferentes autoridades tienen acceso divergente a los datos. Todo eso genera puntos ciegos, especialmente para las autoridades encargadas de hacer cumplir la ley, ya que las asociaciones entre fragmentos de datos pueden ser muy difíciles de identificar. Por lo tanto, es importante trabajar hacia soluciones integradas para mejorar la transparencia y la accesibilidad para la gestión y la seguridad de las fronteras. Por otro lado, era necesario avanzar hacia la interoperabilidad de los sistemas de información actuales.

Los objetivos perseguidos con la interoperabilidad de los sistemas de información de la Unión Europea en el ámbito de la justicia y los asuntos de interior son varios y buscan fortalecer la gestión de fronteras, la seguridad interna y el acceso a la información. Los principales objetivos incluyen fortalecer la protección de las fronteras exteriores, mejorando la capacidad de las autoridades fronterizas para implementar controles efectivos mediante el acceso a información compartida y actualizada entre los diferentes sistemas. Esto ayuda a gestionar mejor los flujos migratorios y las amenazas de seguridad. También se busca mejorar la seguridad interna de la UE, garantizando que las fuerzas policiales y las autoridades judiciales puedan acceder de manera eficiente a los datos necesarios para prevenir, detectar y responder ante delitos graves, terrorismo o amenazas de seguridad.

Otro objetivo es aumentar la eficiencia y reducir duplicidades, optimizando el uso de los sistemas de información existentes evitando la repetición de entradas de datos y proporcionando una visión completa y coherente de la información disponible. Esto ahorra tiempo y mejora la calidad de los datos procesados. Además, se pretende facilitar el intercambio de información en tiempo real, permitiendo que los distintos sistemas se comuniquen entre sí para ofrecer una visión integrada de las personas que cruzan las fronteras o que están bajo vigilancia, asegurando que los datos estén disponibles de forma rápida y accesible para las autoridades pertinentes.

Cumplir con la normativa de protección de datos es otro objetivo importante, asegurando que los sistemas interoperables respeten plenamente las normativas europeas de protección de datos, como el Reglamento General de Protección de Datos (RGPD), y garanticen la privacidad de los ciudadanos. La interoperabilidad también busca optimizar el uso de datos en múltiples contextos, garantizando que la

información esté disponible no solo para los controles fronterizos, sino también para la cooperación policial, la gestión de visas, la lucha contra el crimen organizado y la gestión de crisis, entre otros. Finalmente, se pretende apoyar la transformación digital del espacio Schengen, facilitando la digitalización de los procesos fronterizos y administrativos, reduciendo la dependencia de procedimientos manuales y optimizando la gestión de datos. Estos objetivos buscan una mayor coherencia y eficiencia operativa en toda la UE, mejorando tanto la seguridad como la protección de los derechos fundamentales de las personas.

Los actuales sistemas de información de control fronterizo y seguridad interior dentro de la UE cubren una amplia variedad de funcionalidades, pero a pesar de ello, todavía existen inconvenientes que deben tenerse en cuenta para optimizar su funcionalidad [19].

Cuando los guardias fronterizos verifican información en el Sistema de Información Schengen, solo pueden buscar el nombre y la fecha de nacimiento. El inconveniente de este sistema parece ser el hecho de que los guardias fronterizos sólo pueden verificar la identidad de una persona con sus huellas dactilares después de buscar y encontrar su nombre. Esto permite a los delincuentes potenciales utilizar documentos falsificados para evitar la identificación del SIS, de hecho, se han encontrado personas con más de 20 identidades que han ido cruzando las fronteras interiores del espacio Schengen sin ser detectados. Para eliminar ese inconveniente del sistema SIS, el Consejo Europeo propuso y decidió [20]mejorar la búsqueda de huellas dactilares añadiendo un Sistema Automatizado de Identificación de Huellas Dactilares (AFIS).

La CE tenía previsto mejorar la funcionalidad del VIS mediante la aplicación del AFIS mencionado anteriormente, la creación de imágenes faciales de mejor calidad para facilitar el uso de la comparación biométrica, la recogida de huellas dactilares de niños más pequeños de entre 6 y 12 años [21] y el fomento del uso de la base de datos de documentos de viaje robados y perdidos (SLTD) de Interpol.

La CE propuso también mejorar y potenciar la funcionalidad de solicitudes de asilo y refugio [22]. Realizará un seguimiento de los inmigrantes irregulares y su movimiento entre Estados miembros, así como identificar y verificar la documentación de los inmigrantes irregulares, lo que les permitirá mejorar la eficacia de los procesos de retorno y readmisión. La legislación también cubriría los intercambios de información almacenada en EURODAC con terceros países, teniendo en cuenta las salvaguardias de protección de datos.

La financiación de los programas de interoperabilidad está asegurada principalmente a través de diversos fondos europeos y programas específicos de la UE, como el Fondo de Seguridad Interior (FSI), que apoya a los Estados miembros en la implementación de medidas de interoperabilidad y seguridad fronteriza. La interoperabilidad de los sistemas es una prioridad de financiación para mejorar la capacidad de gestionar la migración y combatir el crimen transfronterizo. También está el Fondo de Asilo, Migración e Integración (FAMI), que aporta financiación para la mejora de los sistemas de información relacionados con la gestión de las fronteras y la migración. Este fondo financia acciones de interoperabilidad que buscan mejorar la eficiencia en la gestión de los flujos migratorios en la UE. Por otro lado, el programa de trabajo anual de eu-LISA recibe financiación a través del presupuesto de la UE para la gestión de grandes sistemas informáticos a nivel europeo. El presupuesto está destinado a garantizar el desarrollo continuo de sistemas interoperables, como el EES, ETIAS y ECRIS-TCN. Además, el Fondo Europeo de Desarrollo Regional (FEDER) también puede asignar recursos para mejorar infraestructuras tecnológicas que contribuyan a la interoperabilidad de los sistemas informáticos de los Estados miembros, en especial aquellos que facilitan el intercambio de información transfronterizo. La UE ha proporcionado un sólido marco legislativo y financiero que sustenta el desarrollo de la interoperabilidad, lo que permite a los sistemas de control fronterizo y seguridad interior funcionar de manera integrada y eficiente, garantizando una gestión de datos más efectiva y mejorando la seguridad dentro del espacio Schengen.

2.4 Principales sistemas de información de la UE.

La interoperabilidad de sistemas se enfoca en los sistemas de información de la UE, gestionados centralmente, que apoyan la seguridad, el control fronterizo y la gestión migratoria. Tres de estos sistemas ya están en funcionamiento, mientras que otros tres se encuentran en desarrollo. Cada uno tiene metas específicas, propósitos propios, fundamentos legales, normas aplicables, grupos de usuarios y un contexto institucional único.

Bajo este escenario de sistemas y antes de profundizar en la interoperabilidad, conviene definir brevemente que hace cada uno de ellos.

Los tres sistemas de información centralizados en operaciones hasta el momento son los siguientes:

2.4.1 El Sistema de Información de Schengen (SIS)

Las autoridades policiales de toda la UE utilizan el Sistema de Información de Schengen para introducir o consultar las descripciones de personas y objetos buscados o desaparecidos. El sistema contiene 91 millones de descripciones y en 2023 registró casi 16 billones de consultas de las autoridades [23].

El SIS también facilita instrucciones a las autoridades sobre la manera de actuar cuando se localiza una persona o un objeto, por ejemplo:

- ❖ la detención de una persona buscada,
- ❖ la protección de una persona vulnerable desaparecida,
- ❖ la confiscación de un objeto ilegal o robado.

En noviembre de 2018, la UE adoptó nuevas normas para mejorar el Sistema de Información de Schengen.

La versión actualizada entró en funcionamiento en marzo de 2023 e incluye:

- ❖ nuevas categorías de descripciones,
- ❖ biometría, como impresiones palmares,
- ❖ huellas dactilares,
- ❖ registros de ADN de personas desaparecidas.

2.4.2 El sistema Eurodac

La base de datos Eurodac contiene las impresiones dactilares de los solicitantes de asilo registrados en los Estados miembros de la UE y los países asociados. Esta base de datos se utiliza para la aplicación del Reglamento de Dublín. Ayuda a:

- ❖ verificar si un solicitante ha solicitado previamente asilo en otro Estado miembro;
- ❖ comprobar si un solicitante ha sido detenido previamente al entrar irregularmente en el territorio europeo;
- ❖ determinar qué Estado miembro es responsable del examen de una solicitud de asilo.

En mayo de 2016, la Comisión propuso una reforma del sistema Eurodac como parte de las propuestas legislativas de reforma de las normas de asilo de la UE. La reforma propuesta tiene como finalidad:

- ❖ mejorar el sistema recogiendo más datos como, por ejemplo, imágenes faciales;
- ❖ ampliar su ámbito de aplicación incluyendo datos sobre los nacionales de terceros países que se encuentren en situación irregular en la UE y que no hayan solicitado asilo;

- ❖ simplificar el acceso de las autoridades policiales.

El 22 de junio de 2022, el Consejo aprobó un mandato de negociación con el Parlamento Europeo sobre esta propuesta legislativa.

El nuevo reglamento de Eurodac se centra en aumentar su interoperabilidad con otros sistemas de información de la UE, como el Sistema de Entrada/Salida (EES) y el Sistema Europeo de Información y Autorización de Viajes (ETIAS). Este rediseño facilita una mejor identificación de las personas que cruzan las fronteras y apoya a las autoridades en la lucha contra el fraude de identidad y la migración irregular. Además, la nueva versión de Eurodac ahora permite almacenar más datos biométricos, como imágenes faciales, y también recoge más información sobre las personas que se encuentran en situación irregular, no solo solicitantes de asilo en las mejoras es su capacidad para identificar a personas con múltiples identidades, asegurando así que las autoridades tengan una visión más clara y completa de los registros. Esto, junto con el acceso ampliado para agencias como Europol y FRONTEX, permite una mejor cooperación en la lucha contra el crimen organizado y el terrorismo.

Uno de los principales objetivos del nuevo Eurodac es combatir el fraude de identidad y garantizar que las autoridades puedan identificar a personas que puedan estar utilizando múltiples identidades. Esto se logra al permitir el cruce de datos biométricos con otros sistemas de información de la UE, lo que fortalece la cooperación en la lucha contra el crimen organizado y el terrorismo. El reglamento también extiende el acceso a agencias como Europol y FRONTEX, ampliando así su capacidad de actuar en áreas de seguridad y migración.

La propuesta de reforma del Eurodac forma parte de la política más amplia de la UE sobre migración y asilo, que busca abordar los retos del incremento de los cruces fronterizos irregulares y mejorar la seguridad interior frente a amenazas como el terrorismo [2].

2.4.3 El Sistema de Información de Visados (VIS)

El Sistema de Información de Visados, en funcionamiento desde 2011, es una base de datos que facilita el procedimiento de expedición de visados de corta duración.

Este sistema ayuda a las autoridades de migración, asilo, fronteras y visados a realizar comprobaciones sobre los nacionales de terceros países que necesitan un visado de corta duración para entrar en el espacio Schengen. Las autoridades pueden utilizar el VIS para comprobar las correspondencias biométricas de identificación de personas e impedir la usurpación o el fraude de identidad.

En respuesta a la evolución de los retos en materia de migración y seguridad, en mayo de 2021 la UE adoptó un nuevo Reglamento para mejorar el sistema. Las nuevas normas son las siguientes:

- ❖ seguir reforzando la seguridad del procedimiento de obtención de los visados de corta duración;
- ❖ incluir en la misma base de datos los visados de larga duración y los permisos de residencia;
- ❖ garantizar la interoperabilidad entre el VIS y otros sistemas y bases de datos pertinentes de la UE.

El nuevo VIS, que está en proceso de actualización, incluirá varias mejoras clave diseñadas para aumentar la seguridad y mejorar la capacidad de control fronterizo y la detección de fraudes. Algunas de las actualizaciones más importantes son:

- ❖ Ampliación del rango de datos biométricos: El nuevo sistema VIS podrá almacenar más tipos de datos biométricos, como imágenes faciales, lo que facilitará la identificación precisa de los viajeros y ayudará a evitar el fraude de identidad.
- ❖ Interoperabilidad mejorada: La nueva versión del VIS será interoperable con otros sistemas de la UE, como el Sistema de Entrada/Salida (EES), el Sistema Europeo de Información y Autorización de Viajes (ETIAS), y el Sistema de Información de Schengen (SIS). Esto permitirá

una mejor coordinación y colaboración entre los Estados miembros en materia de control de fronteras y seguridad.

- ❖ *Mayor acceso para Europol y otras agencias:* En línea con las necesidades de seguridad interior de la UE, las agencias como Europol tendrán un acceso más amplio al VIS para ayudar en la prevención de delitos graves, incluidos el terrorismo y el crimen organizado.
- ❖ *Cobertura más amplia:* Se ampliará el alcance del sistema para incluir no solo visados de corta duración, sino también visados de larga duración y permisos de residencia, lo que mejorará la visibilidad y el control sobre todas las personas que ingresan a la UE.

El nuevo VIS también mejorará la capacidad de las autoridades de realizar verificaciones cruzadas y compartir información en tiempo real, lo que facilitará la detección de riesgos y la gestión eficiente de los flujos migratorios [24].

Todos estos sistemas se encuentran operativos en la actualidad, los siguientes se encuentran en fase de desarrollo, algunos más avanzados que otros ya que son interdependientes, es decir, irán entrando en producción sucesivamente.

2.4.4 El Sistema de Entradas y Salidas (EES)

En noviembre de 2017, el Consejo adoptó el Reglamento por el que se establece un Sistema de Entradas y Salidas. Este sistema registrará los datos de las entradas, salidas y denegaciones de entrada de los nacionales de terceros países que crucen las fronteras exteriores del espacio Schengen.

El Sistema de Entradas y Salidas contribuirá a:

- ❖ reducir los retrasos en los controles fronterizos y mejorar la calidad de dichos controles gracias al cálculo automático de la estancia autorizada de cada viajero;
- ❖ asegurar una identificación sistemática y fiable de las personas que rebasan la duración de estancia autorizada;
- ❖ reforzar la seguridad interior y la lucha contra el terrorismo y otras formas graves de delincuencia permitiendo el acceso de las autoridades policiales a los registros de historiales de viaje.

El nuevo sistema será creado por eu-LISA en cooperación con los Estados miembros. La entrega de la nueva arquitectura informática prevé que el sistema de entradas y salidas entrar en funcionamiento en el primer semestre de 2025.

2.4.5 El Sistema Europeo de Información y Autorización de Viajes (ETIAS).

El Consejo adoptó el Reglamento por el que se establece el Sistema Europeo de Información y Autorización de Viajes (SEIAV) en septiembre de 2018. Este sistema informático se utilizará para llevar a cabo inspecciones previas de los viajeros carentes de la obligación de visado y para denegarles la autorización de viaje si fuera necesario.

Será similar a los sistemas ya operativos en EE. UU., Canadá y Australia, entre otros países, y ofrecerá varias ventajas, por ejemplo:

- ❖ una mejora de la seguridad interior,
- ❖ una mejor prevención de la inmigración ilegal,
- ❖ menores riesgos para la salud pública y menos retrasos en las fronteras.

El ETIAS está siendo desarrollado por la Agencia y estará listo para entrar en funcionamiento en la primavera de 2025. la agencia de la UE encargada de la gestión de los sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

2.4.6 El Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)

El Sistema Europeo de Información de Antecedentes Penales (ECRIS-TCN), proporcionará un intercambio electrónico de información de antecedentes penales de forma centralizada entre los Estados miembros. Permitirá a las autoridades que gestionan los antecedentes penales de los Estados miembros obtener información completa sobre condenas anteriores de nacionales de la UE del Estado miembro de nacionalidad de esa persona. ECRIS-TCN, una vez creado, será un sistema centralizado que permitirá a las autoridades de los Estados miembros identificar qué otros Estados miembros tienen antecedentes penales de los nacionales de terceros países o apátridas objeto de control, para que luego puedan utilizar el sistema ECRIS-TCN existente para abordar solicitudes de información sobre condenas únicamente a los Estados miembros identificados.

La mejora de ECRIS-TCN forma parte de la Agenda Europea de Seguridad. Esta iniciativa se integra en el nuevo enfoque impulsado por la Comisión Europea para gestionar los datos relacionados con fronteras y seguridad. Según este enfoque, todos los sistemas de información centralizados de la UE destinados a la seguridad, control fronterizo y gestión migratoria deben ser interoperables, garantizando al mismo tiempo el respeto pleno de los derechos fundamentales.

ECRIS-TCN está siendo desarrollado y gestionado por la Agencia. Un Estado miembro que desee identificar el propio que posee información de antecedentes penales sobre un TCN en particular puede hacerlo realizando una búsqueda de "acierto/no acierto" en el sistema central de TCN.

Estos seis sistemas son complementarios y, con la excepción del Sistema de Información de Schengen (SIS), se centran exclusivamente en los nacionales de terceros países. Apoyan a las autoridades nacionales en la gestión de las fronteras, la migración, la tramitación de visados y el asilo, así como en la lucha contra la delincuencia y el terrorismo. Esto último es aplicable en particular al SIS, que es la herramienta de intercambio de información policial más utilizada en la actualidad.

Además de los sistemas mencionados anteriormente, para mejorar la seguridad de la UE, es necesario implementar componentes de interoperabilidad adicionales, los cuales se detallarán en el capítulo posterior: Portal Europeo de Búsqueda (PEB), Repositorio de Identidades Comunes (CIR), Detector de Identidades Múltiples (MID), Servicio de Coincidencia Biométrica Compartida (sBMS) y el Repositorio Central de Informes y Estadísticas (CRRS). Los componentes serán utilizados por los mismos usuarios finales que utilizan SIS, VIS y EURODAC, etc., y no por ciudadanos corrientes. Sin embargo, ETIAS también es accesible para uso público (registro para viajar a la zona Schengen) a través de Internet.

2.4.7 Otros sistemas relacionados

Además de los sistemas de información gestionados centralmente en la UE, el alcance de la interoperabilidad también abarca las bases de datos de Interpol, como la de documentos de viaje robados y perdidos (SLTD), que, según el Código de Fronteras Schengen, se consulta sistemáticamente en las fronteras exteriores de la UE, y la base de documentos de viaje vinculados a alertas (TDAWN). Asimismo, incluye datos de Europol que sean relevantes para el funcionamiento del sistema ETIAS propuesto y que puedan apoyar a los Estados miembros en la consulta de datos sobre delincuencia grave y terrorismo.

Los sistemas de información nacionales y aquellos descentralizados gestionados por la Unión Europea no se incluyen dentro del alcance de este análisis. No obstante, si en el futuro se justifica su integración, algunos sistemas descentralizados, como los relacionados con el marco de Prüm, la Directiva sobre el Registro de Nombres de Pasajeros (PNR) y la Directiva de Información Anticipada de Pasajeros (API), podrían conectarse a uno o más de los componentes definidos dentro del marco de interoperabilidad de los sistemas de la UE. Esta posibilidad refleja el potencial de ampliar el alcance de la interoperabilidad para incluir sistemas que actualmente operan de manera independiente. La incorporación de estos sistemas tendría como objetivo mejorar la conectividad y la eficacia en el

intercambio de información entre diferentes jurisdicciones y niveles administrativos, contribuyendo a una mayor coherencia en la gestión de datos de seguridad y migración. Sin embargo, cualquier decisión en este sentido deberá estar respaldada por un análisis riguroso que demuestre su necesidad y utilidad en el contexto de los objetivos generales de la interoperabilidad.

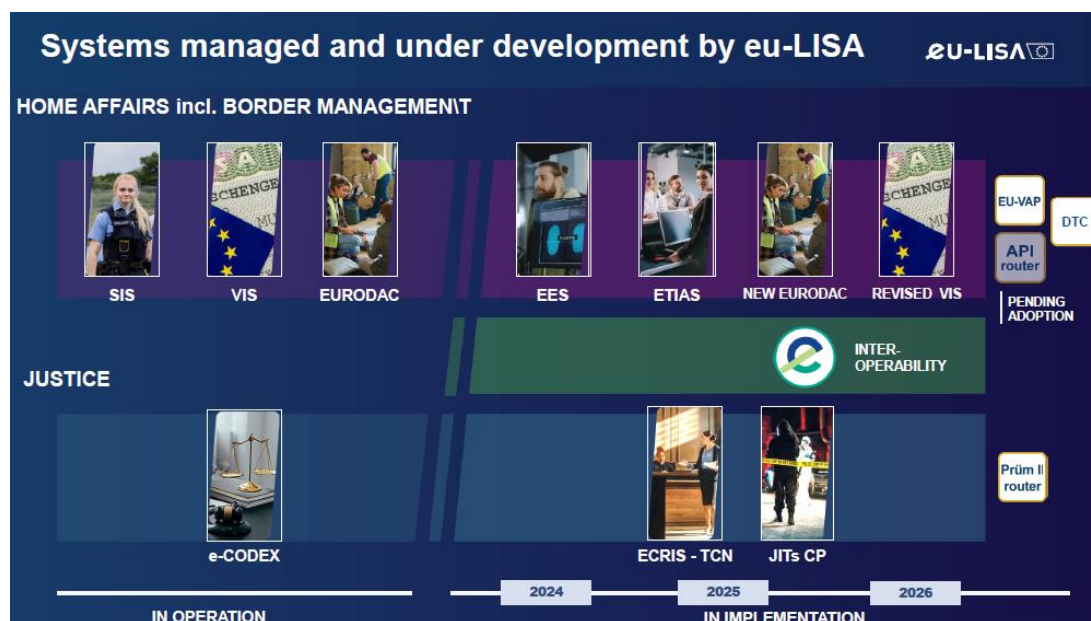


Figura 2-3 Sistemas gestionados por la Agencia (fuente: euLISA [13] [25])

2.5 Costes económicos y financiación de la IO.

La IO en la Unión Europea implica costos significativos tanto para los Estados miembros como para la agencia, que es responsable de la gestión operativa de los grandes sistemas de información en los ámbitos de la seguridad, la migración y las fronteras. Esta inversión tiene como objetivo mejorar la eficacia de los sistemas de información para la seguridad interna y la gestión fronteriza de la UE.

La implementación de la IO exige una inversión considerable por parte de los Estados miembros. Los costos incluyen la actualización de la infraestructura tecnológica necesaria para la interoperabilidad de los sistemas nacionales con los sistemas europeos como el Sistema de Información de Schengen (SIS II), el Sistema de Información de Visados (VIS), EURODAC, el Sistema de Entrada/Salida (EES) y el Sistema Europeo de Información y Autorización de Viajes (ETIAS). Los Estados deben integrar sus sistemas nacionales con estos sistemas paneuropeos, lo que requiere recursos para formación de personal, actualización de software y hardware, y el fortalecimiento de la seguridad de los datos.

Costes para eu-LISA y la UE: eu-LISA ha recibido una cantidad considerable del presupuesto de la UE para llevar a cabo la interoperabilidad. En su presupuesto plurianual, la agencia asigna una porción significativa para desarrollar, operar y mantener estos sistemas de información. En el marco del Marco Financiero Plurianual (MFP) 2021-2027, la UE ha asignado fondos específicos a programas relacionados con la seguridad y la gestión de fronteras, incluidos los sistemas interoperables gestionados por eu-LISA. En 2019, se informó que los costos de la interoperabilidad se estimaban en varios miles de millones de euros para toda la duración del proyecto, lo que refleja la magnitud de esta tarea.

Además, la UE también canaliza fondos a través de mecanismos como el Fondo de Seguridad Interior (FSI) y el Fondo de Asilo, Migración e Integración (FAMI). Estos fondos están diseñados para apoyar a los Estados miembros en la implementación de medidas de interoperabilidad y gestión de fronteras.

Teniendo en cuenta el impacto económico, el desarrollo de sistemas interoperables trae consigo un ahorro a largo plazo mediante la reducción de duplicidades en la gestión de datos y la mejora de la eficiencia operativa. Sin embargo, los costos iniciales de implementación son elevados, debido a la necesidad de modernizar infraestructuras tecnológicas, reforzar la ciberseguridad y garantizar que los

sistemas puedan manejar un mayor volumen de datos y usuarios. Según algunos informes, el coste de desarrollar y desplegar estos sistemas podría alcanzar varios miles de millones de euros, lo que incluye no solo la infraestructura técnica, sino también la formación del personal y las mejoras en seguridad cibernética para evitar amenazas externas.

El presupuesto total de la Agencia ha aumentado significativamente en los últimos años debido a la creciente demanda de sistemas interoperables. En el período 2021-2027, se ha destinado una parte considerable de los recursos para apoyar la creación y el mantenimiento de sistemas de gran escala que respalden la interoperabilidad en toda la UE. Estos sistemas también garantizan la protección de datos y el cumplimiento de las normativas del Reglamento General de Protección de Datos (GDPR).

El costo de la interoperabilidad para los Estados miembros y la Agencia es significativo, con una inversión que supera los €4.5 mil millones en total entre el presupuesto de la UE, el apoyo a los Estados miembros y los sistemas gestionados por la Agencia. Estos costos, aunque elevados, están destinados a mejorar la eficiencia en la seguridad y gestión de fronteras, contribuyendo a un espacio Schengen más seguro y mejor conectado. Sobre este aspecto financiero y presupuestario se hablará más adelante en un capítulo dedicado a la financiación de la IO.

3 NORMATIVA, PRINCIPIOS Y POLÍTICAS DE LA AGENCIA

3.1 Principios y políticas de la Agencia

Un principio es una regla para garantizar el logro de las estrategias/aspiraciones organizativas y de TI. Los Principios orientan las soluciones relevantes, y hacen que las reclamaciones y decisiones sean más claras y rastreables. Los principios pueden contradecirse entre sí y es necesario establecer prioridades para ellos. El “Documento de definición de arquitectura de interoperabilidad” describe los principales aspectos de la arquitectura de la Agencia y enumera su priorización [26]. En el caso de eu-LISA, los datos se consideran un activo que debe gestionarse adecuadamente, manteniendo la calidad de los datos. El principal motivo es el hecho de que los Estados miembros confían sus valiosos datos en manos de eu-LISA mediante el uso de CBS (Core Business System) y esperan que sus datos se gestionen en consecuencia. Los datos son la base del conocimiento que guiará al progreso, las estrategias y la toma de decisiones de la organización.

La continuidad del negocio es otro principio que debe considerarse. Los sistemas se vuelven más dependientes unos de otros a medida que se vuelven más ubicuos e interoperables. Por lo tanto, es necesario garantizar la fiabilidad de estos sistemas durante su diseño y uso continuo. Los posibles fallos de hardware, los desastres naturales y la corrupción de datos no deberían permitir la interrupción de las actividades del sistema, ya que ese es el principal objetivo de la Agencia. Ésta, debe contar con procesos adecuados de continuidad del negocio y recuperación ante desastres para evitar cualquier tipo de pérdida de información o corrupción de datos. La dependencia de aplicaciones de sistemas compartidos implica monitorear y predecir de antemano los riesgos de interrupción del negocio o pérdida de datos comerciales. Esto se puede lograr mediante revisiones y pruebas constantes de sistemas de importancia crítica para garantizar que nunca se produzcan fugas o pérdidas de datos. Una solución podría ser almacenar datos vitales en diferentes ubicaciones.

Para determinar las medidas de seguridad apropiadas que se implementarán en las fases posteriores del proyecto para mitigar los riesgos y posibles efectos adversos, los sistemas recientemente desarrollados o la evolución de los sistemas existentes deben someterse a un análisis exhaustivo de riesgos de seguridad desde el comienzo de la creación del proyecto.

La confidencialidad, la integridad y la disponibilidad (CIA, por sus siglas en inglés) son principios de seguridad de TI bien conocidos y se pueden considerar atributos adicionales como autenticidad, responsabilidad y no repudio, como subconjuntos de estos principios [27] [16]. eu-LISA debe seguir estos principios para respetar la base jurídica, garantizar la cobertura de las necesidades de seguridad, cumplir con todas las consideraciones reglamentarias y hacer que la implementación de la interoperabilidad sea más segura. Además, un aumento repentino de la carga comercial podría producirse y la Agencia debe poder responder a dicha solicitud de manera oportuna y eficiente.

Desde el principio, los procesos comerciales de CBS deben estructurarse para cumplir con los estándares de seguridad de los datos y procesar únicamente los datos personales necesarios para cada propósito de procesamiento particular. Eso incluye la cantidad de datos personales obtenidos, el grado de su procesamiento, la duración del almacenamiento y la accesibilidad (derivada de la base legal del RGPD-Reglamento General de Protección de Datos). Específicamente, las regulaciones de la UE, el GDPR y la base legal CBS requieren que la privacidad de los Terceros Nacionales sea respetada y protegida dentro de los límites de la ley.

Además, los datos que se utilizarán en múltiples sistemas en la creación de aplicaciones deben tener un vocabulario común en los CBS para facilitar el intercambio de datos eficaz y fluido. Un vocabulario común simplificará las interacciones y permitirá un diálogo exitoso. La Agencia debe desarrollar el vocabulario común inicial para la CBS, de acuerdo con sus partes interesadas. Ahí es donde los factores políticos juegan un papel importante, ya que cada agencia tuvo que llegar a una decisión unánime, ya que las definiciones seleccionadas deberían usarse continuamente durante todo el ciclo de vida en todos los sistemas.

Cada elemento de datos tiene una única fuente autorizada, cuyo objetivo es garantizar la integridad de los datos dentro de los Estados miembros y la Agencia. En general, la fuente autorizada se define en función del proceso comercial que inicialmente recopila los datos o dentro del activo de datos o el ciclo de vida de entrega comercial de la Agencia. Es importante asignar el propietario oficial responsable de los datos comerciales y operativos, así como su fuente.

Cualquier conjunto de medidas de seguridad desarrolladas para la CBS y sus procesos asociados debe ser capaz de adaptarse en contextos legales/organizacionales y evolucionar para hacer frente a peligros, desafíos técnicos y riesgos emergentes. A medida que surgen constantemente nuevas tecnologías y sistemas con requisitos de interoperabilidad adicionales, el marco legal está cambiando. Por lo tanto, la Agencia tiene que ser capaz de adaptar nuevos sistemas, al tiempo que define todos los riesgos asociados a todo ese proceso.

En el caso de la Agencia, las políticas se pueden dividir en tres grupos: Legislación sobre la interoperabilidad, legislación sobre los principales negocios y legislación sobre seguridad/privacidad.

3.2 Normativa sobre Interoperabilidad, sistemas y seguridad

La legislación sobre la interoperabilidad se compone de dos regulaciones interconectadas que describen la futura arquitectura interoperable mediante la introducción de cinco nuevos componentes de interoperabilidad.

Los reglamentos que se complementan entre sí son el Reglamento (CE) 2017/0351(COD) y Reglamento (CE) 2017/0352(COD). Estas regulaciones sientan las bases para el futuro relaciones internas, funcionalidades y leyes de la arquitectura. Hay impactos importantes que estas regulaciones de interoperabilidad tienen en la arquitectura de la Agencia. Los documentos indicaron que cinco nuevos componentes deben introducirse, desarrollarse y mantenerse (PEB, sBMS, CIR, DIM y CRRS). Además, se decidió que los datos (biométricos, de viaje y de identidad) ya no se almacenarán en un solo lugar (CBS) y en su lugar deberían almacenarse en CIR. Esa decisión tiene enormes implicaciones para la seguridad, la privacidad de los datos, el rendimiento y la protección de los datos. Además, Las regulaciones establecieron que los CBS no tendrán su propio servicio de comparación biométrica y en su lugar cambiará a sBMS que permite que todos los sistemas de información manejen los datos biométricos. La nueva edición presentada fue el uso de MID para detectar múltiples identidades en todos los sistemas y no en sistemas individuales. Y finalmente, estas regulaciones definen estrictamente los datos propietarios y la retención, así como su almacenamiento, calidad y protección dentro componentes de interoperabilidad.

Debido a que el reglamento de interoperabilidad se basa en una infraestructura establecida y en evolución, en la arquitectura de interoperabilidad también deben tenerse en cuenta las regulaciones de las estructuras comerciales principales actuales y previstas.

Es por eso por lo que se deben integrar los siguientes seis sistemas comerciales (nuevos y existentes):

- ❖ VIS (Reglamento (CE) 2023/2627)
- ❖ SIS (Reglamento (CE) 2018/1860, 2018/1861 y 2018/1862)
- ❖ EURODAC (Reglamento (UE) 2024/1358)
- ❖ SES (Reglamento (CE) 2017/2226)
- ❖ ETIAS (Reglamento (UE) 2018/1240 y 2018/1241)
- ❖ ECRIS-TCN (Reglamento (CE) 2017/0144(COD))

La normativa propia de la seguridad y la privacidad se ocupa de proteger la seguridad de los datos y la privacidad de los ciudadanos. Incluye medidas para prevenir el acceso no autorizado, salvaguardar la información sensible y garantizar la confidencialidad.

La Agencia está altamente comprometida con el procesamiento de datos personales desde el punto de vista legal.

Cuando la Agencia procesa datos personales, garantiza el respeto de los derechos a la privacidad y la protección de datos previstos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. En este sentido, la Agencia procesa cualquier dato personal recopilado de acuerdo con lo dispuesto en el Reglamento (UE) 2018/1725 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos, oficinas y agencias de la Unión y en la libre circulación de dichos datos. Como complemento a este texto, la Decisión de la Dirección sobre las normas de ejecución relativas al Reglamento (CE) n.º 2018/1275 también regula el tratamiento de datos personales por parte de la Agencia.

Ésta, no solo procesa datos personales para el desempeño de tareas realizadas en interés público de conformidad con el derecho de la Unión Europea o en el ejercicio legítimo del poder oficial conferido a la Agencia. Además, el tratamiento de datos personales es lícito como parte de una obligación legal o contractual o cuando el interesado haya dado su consentimiento inequívoco. En cualquier caso, la Agencia no tratará datos personales con fines publicitarios o comerciales.

En el sitio web de la Agencia hay disponible un formulario de "contacto" que está diseñado para permitir a los usuarios hacer consultas y solicitar información directamente de la Agencia. Cuando un usuario envía su información personal a través de este formulario, como su nombre, apellidos y dirección de correo electrónico, la Agencia solo utiliza estos datos estrictamente para responder a la consulta específica del interesado, asegurando que los datos se manejen de acuerdo con los principios de privacidad y protección de datos establecidos en la normativa de la UE.

Para garantizar el cumplimiento del Reglamento General de Protección de Datos (GDPR), la Agencia proporciona un "Aviso de privacidad" en su sitio web, que detalla cómo recopila, procesa y protege los datos personales en estas interacciones. Este aviso de privacidad aclara los derechos de los interesados, como el derecho a acceder a sus datos, a rectificarlos si son inexactos, a limitarlos o, incluso, a eliminarlos en ciertas circunstancias. Los interesados pueden conocer más sobre sus derechos visitando la sección correspondiente en el sitio web de la Agencia, donde también se especifican los pasos para ejercer estos derechos.

La Agencia emplea políticas internas y procedimientos de seguridad específicos para asegurar que los datos personales no se utilicen con otros fines ni se compartan con terceros sin autorización. En este sentido, el tratamiento de datos personales realizado se ajusta a la normativa europea sobre protección de datos y es supervisado por el Supervisor Europeo de Protección de Datos (EDPS), quien vela por el respeto de los derechos de los interesados en el contexto de las instituciones de la UE.

El sitio web de la Agencia proporciona enlaces a otros sitios web institucionales de la Unión Europea, dentro del dominio 'europa.eu'. Dado que la Agencia no los administra, es recomendable que se revise sus políticas de privacidad.

Para garantizar que los datos personales se procesen legalmente, la Agencia nombró un delegado de Protección de Datos que controla la correcta aplicación de los principios de protección de datos en la Agencia.

La Autoridad de Control, en materia de tratamiento de datos personales, es el Supervisor Europeo de Protección de Datos (EDPS). El EDPS es responsable del seguimiento de las instituciones y organismos de la Unión Europea y de su cumplimiento de las normas de protección de datos, garantizando que se respeten los derechos a la privacidad y a la protección de datos, como derechos humanos fundamentales.

3.3 Marco europeo de la interoperabilidad

El Marco Europeo de Interoperabilidad (EIF, por sus siglas en inglés) es una estrategia de la Unión Europea diseñada para facilitar la interoperabilidad entre los sistemas de administración pública de los Estados miembros. Su objetivo principal es mejorar la eficiencia, cooperación y la prestación de servicios públicos en toda la UE, permitiendo un intercambio de información sin problemas entre organismos nacionales y de la UE. El EIF se centra en crear un marco que permita a los sistemas nacionales de cada país miembro trabajar conjuntamente sin importar sus diferencias técnicas, organizativas o jurídicas y muestra la voluntad de las organizaciones en colaborar hacia objetivos mutuamente beneficiosos que implican el intercambio de información y experiencia entre diferentes organizaciones a través de los respectivos procesos de negocio asistidos por el intercambio de datos entre sus sistemas TIC [28]. En la cumbre de Sevilla (2002), los representantes de los Estados miembros de la UE adoptaron el Plan de Acción Europeo de 2005 [29], que exigía a los Estados miembros preparar marcos de interoperabilidad que permitieran la prestación de servicios paneuropeos de gobierno electrónico para ciudadanos y empresas. El Marco Europeo de Interoperabilidad está dirigido a gestores de proyectos de gobierno electrónico en los estados miembros de la UE y las instituciones de la Unión Europea.

En 2004, la CE publicó la primera versión del Marco Europeo de Interoperabilidad, que obligaba a los Estados Miembros a crear y apoyar un Marco Nacional de Interoperabilidad, para garantizar la interoperabilidad en toda la Unión Europea [30].

La Unión Europea se enfrenta a una serie de desafíos complejos y cada vez más interconectados en áreas cruciales como la gestión de fronteras, la migración y la seguridad interna. En primer lugar, los flujos migratorios irregulares, las crisis humanitarias y el aumento de las amenazas terroristas y transnacionales han puesto a prueba la capacidad de los Estados miembros para gestionar de manera eficiente tanto la seguridad externa como la interna. Estos problemas no solo afectan la seguridad de las fronteras físicas, sino también la protección de la integridad y estabilidad política y social de los países miembros. Además, las amenazas emergentes, como el crimen organizado y la ciberdelincuencia, agravan la situación, mostrando que los sistemas tradicionales de control y seguridad ya no son suficientes.

Ante estos retos, la necesidad de mejorar la gestión de fronteras y migración en la UE se ha vuelto aún más urgente. Esto implica no solo el refuerzo de los controles fronterizos, sino también una gestión más efectiva y segura de la información relacionada con la movilidad de las personas y la seguridad interna. En este contexto, los sistemas de información de defensa, fronteras y migración de la UE deben adaptarse y evolucionar para ser más interoperables, eficientes y eficaces en el intercambio de datos.

Una de las soluciones clave para enfrentar estos desafíos es el compromiso de la Unión Europea de mejorar el intercambio de información entre los diferentes sistemas de datos relacionados con la gestión de fronteras y migración. La interoperabilidad entre estos sistemas es fundamental para que las autoridades nacionales, como las fuerzas de seguridad y las agencias de inmigración, puedan acceder a la información relevante de manera rápida y segura. Para ello, la UE ha implementado una serie de iniciativas y proyectos, como el Sistema de Información Schengen (SIS), el Sistema Europeo de Información y Autorización de Viaje (ETIAS) y el Sistema de Entrada/Salida (EES), entre otros, que están diseñados para facilitar el acceso y la compartición de datos entre los Estados miembros.

El intercambio eficiente de información no solo facilita el control y la gestión de la migración, sino que también fortalece las capacidades de respuesta ante las amenazas a la seguridad interna, como el terrorismo, el crimen organizado y la trata de seres humanos. La interoperabilidad permite a los sistemas detectar patrones sospechosos de comportamiento, identificar individuos de interés en tiempo real y facilitar la toma de decisiones informadas. Además, este enfoque contribuye a la optimización de recursos, al permitir que las autoridades competentes trabajen de manera coordinada y evitar duplicaciones de esfuerzos en la recopilación y el análisis de datos.

El Nuevo EIF [31] se centra en la creación del mercado digital y tiene como objetivo mejorar la calidad de los servicios públicos europeos. El concepto de dicha interoperabilidad se muestra en la Fig. 2 a continuación.

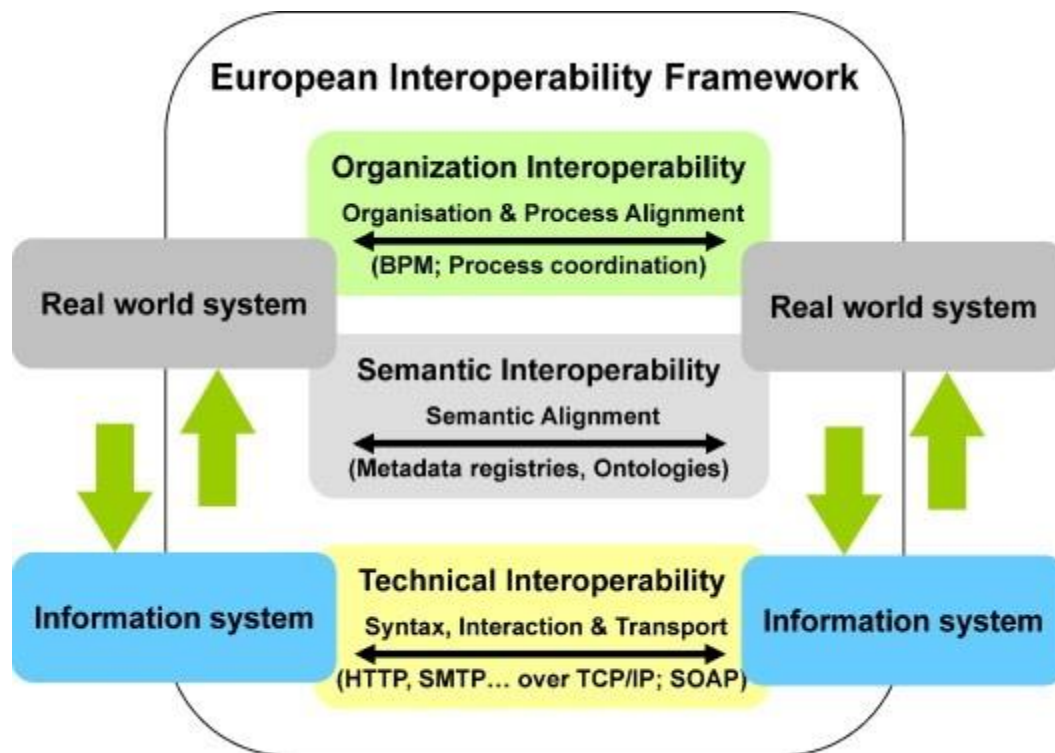


Figura 3-1 Marco Europeo de Interoperabilidad (fuente: Vernadat 2009 [32])

El modelo de IO debe contener al menos tres niveles: organizativo, semántico y técnico. El intercambio de datos entre sistemas de software aplicados y plataformas de software que implementan tecnología de modelado de información (componentes de sistemas de información) se considera no solo desde el punto de vista de la implementación técnica (el nivel técnico), sino también a nivel semántico y organizacional.

La técnica de la IO incluye el intercambio de información, elementos de la infraestructura teleinformática de las TIC, como líneas de comunicación, plataformas informáticas con sistemas operativos, software en forma de sistemas de gestión de bases de datos, una aplicación de software para desarrollar los sistemas necesarios, etc. Desde el punto de vista de la interoperabilidad. Desde nuestro punto de vista, los estándares de comunicación a nivel de transmisión de bits en redes locales y globales, o la transmisión de los mensajes entre componentes de software son vitales [33]. Este nivel se puede dividir en otros subniveles [34], pero este trabajo se centra en un solo nivel.

El nivel semántico de IO debe garantizar el funcionamiento coordinado de varios sistemas de información y sus componentes sobre la base de una interpretación única e inequívoca del valor de la información obtenida como resultado del intercambio. También refleja la necesidad de asegurar la compatibilidad de la información durante el intercambio de datos y garantiza la posibilidad de acceso

completo y procesamiento independiente de esta información por parte de terceros sin contactar al propietario de la información [35]

A nivel organizacional de IO, se deben determinar formas de alinear los procesos de negocios tanto a nivel interno como externo. Así, se acuerdan objetivos empresariales y se alcanzan acuerdos de cooperación y de intercambio de información [32].

Uno de los cambios importantes que se produjo en la Agencia tiene que ver con la contratación, cambiándola completamente. Anteriormente, la Agencia tenía un enfoque de "Silo" (un solo contratista por sistema) y ahora está siendo reemplazado por una "Adquisición Transversal" que permite que múltiples contratistas trabajen juntos para mitigar los desafíos que surgen con la implementación de la interoperabilidad.

4 METODOLOGÍA DE INVESTIGACIÓN

4.1 Investigación cualitativa

La investigación cualitativa se ha seleccionado como la metodología principal de este estudio debido a su capacidad para comprender en profundidad la esencia del fenómeno de la IO en los sistemas de información de la Unión Europea (UE). Este enfoque permite explorar la complejidad de los sistemas, que no puede ser explicada adecuadamente a través de métodos cuantitativos o limitados. La investigación cualitativa es ideal para examinar sistemas dinámicos y multifacéticos, ya que facilita el análisis detallado de los diversos factores en juego, como los retos organizativos, tecnológicos y legales que afectan a la implementación de la IO [36].

La elección de este enfoque permite capturar una visión más rica de las experiencias y percepciones de los actores clave involucrados en el proceso, como los responsables de la Agencia y los representantes de los Estados miembros. Este tipo de análisis cualitativo también es útil para identificar y comprender las barreras y oportunidades que surgen en la implementación de la interoperabilidad, proporcionando un análisis más profundo que permite evaluar no solo los aspectos técnicos, sino también los políticos y sociales. En resumen, la investigación cualitativa ofrece un marco adecuado para explorar los sistemas complejos de IO en la UE, al ofrecer una comprensión integral de los factores involucrados [36].

El control sobre la estructura de la investigación se orienta hacia el desarrollo de un conjunto preliminar de preguntas diseñadas para la recolección de datos, con un énfasis en el estudio de patrones entre múltiples variables [37]. Esto es crucial para identificar las interrelaciones y los contextos que influyen en la implementación de la IO.

La elección del enfoque cualitativo se justifica por su capacidad para centrar la atención en datos descriptivos textuales, a diferencia del enfoque cuantitativo, que se enfoca en datos numéricos. Este aspecto es particularmente relevante para analizar la implementación de sistemas de información, ya que permite explorar y comprender las percepciones y experiencias de los actores involucrados.

Para llevar a cabo esta investigación, se utilizarán diversas técnicas, como entrevistas, grupos focales y análisis documental. Estas metodologías permitirán identificar patrones, desafíos y oportunidades asociados con la IO. El enfoque cualitativo proporciona una visión holística y detallada de los procesos y dinámicas que caracterizan este contexto específico, facilitando así un entendimiento más profundo de los problemas y las posibilidades en el ámbito de la interoperabilidad de la UE.

Esta metodología es especialmente valiosa en estudios de sistemas complejos, ya que permite captar la diversidad de opiniones y experiencias que pueden influir en la eficacia y eficiencia de los sistemas de información en la UE.

Estos son los aspectos característicos de este modelo de investigación:

- ❖ Generación de nuevas teorías: La investigación cualitativa permite la exploración profunda de fenómenos no comprendidos previamente, lo que puede conducir al desarrollo de nuevas teorías o marcos conceptuales.
- ❖ Desarrollo o cuestionamiento de teorías existentes: Además de generar nuevas teorías, la investigación cualitativa puede mejorar las teorías existentes al proporcionar nuevas perspectivas y revelar complejidades que pueden haber sido pasadas por alto.
- ❖ Proposición de implicaciones prácticas: Los hallazgos de la investigación cualitativa pueden tener aplicaciones prácticas significativas, informando políticas, prácticas y estrategias de intervención en diversos campos.
- ❖ Mejora de la comprensión y la empatía: Al profundizar en las experiencias humanas, la investigación cualitativa promueve una mayor comprensión y empatía, lo que contribuye a sociedades más compasivas e inclusivas.
- ❖ Informar la investigación de métodos mixtos: Los resultados de la investigación cualitativa pueden complementar y mejorar la investigación cuantitativa, permitiendo un enfoque más completo y robusto para abordar cuestiones de investigación complejas.

La investigación cualitativa abarca cinco métodos fundamentales: narrativa, etnografía, teoría fundamentada, fenomenología y estudio de caso.

- ❖ Narrativa: Este método se centra en la descripción de acontecimientos pasados con el fin de comprender las situaciones presentes. La narrativa permite a los investigadores explorar las historias de vida de las personas y los significados que estas atribuyen a sus experiencias [38].
- ❖ Etnografía: Este enfoque busca describir las características culturales de un grupo, incluidos sus patrones y creencias compartidas. Harris (1968) destaca que la etnografía se basa en la observación y la participación en la vida cotidiana de las personas para obtener una comprensión más profunda de sus comportamientos y contextos sociales [39] [40].
- ❖ Teoría Fundamentada: Este método se centra en el descubrimiento y desarrollo de teorías a partir de datos recopilados. Strauss y Corbin (1998) indican que este enfoque permite a los investigadores generar teorías a partir de la práctica, en lugar de probar hipótesis preexistentes [41].
- ❖ Fenomenología: La fenomenología tiene como objetivo describir las experiencias vividas por varios individuos y encontrar lo que tienen en común. Manen (1990) argumenta que este enfoque permite captar la esencia de las experiencias humanas, lo que resulta en un entendimiento más profundo de los significados que las personas asignan a sus vivencias [42].
- ❖ Estudio de Caso: Este método describe la experiencia en profundidad de personas, comunidades u organizaciones. Yin (1984) [43] define el estudio de caso como un enfoque empírico que busca comprender un fenómeno en un contexto real, especialmente cuando los límites entre el fenómeno y el contexto son difusos. Los estudios de caso pueden incluir uno o varios casos y pueden abarcar una o más unidades de análisis [44].

En base a las definiciones anteriores, se optó por realizar una investigación de *estudio de caso*, ya que este método es el que se considera más adecuado para las preguntas de investigación planteadas. Permite un análisis detallado y contextualizado de la IO en los sistemas de información de la UE, facilitando la comprensión de los retos y oportunidades que surgen en su implementación. Este enfoque proporciona un marco que permite examinar en profundidad las dinámicas y experiencias de los actores involucrados, lo que resulta fundamental para abordar las cuestiones de gobernanza y recursos en este ámbito.



Figura 4-1 Métodos de Investigación (fuente: web Question Pro [45])

Los estudios de caso pueden clasificarse en tres tipos: exploratorios, explicativos y descriptivos. Cada tipo tiene un enfoque diferente [46]:

- ❖ *Estudios de Caso Exploratorios*: Se utilizan para obtener una comprensión inicial de un fenómeno. Responden a preguntas como “qué” y “cómo”, permitiendo explorar conceptos y relaciones en profundidad sin requerir la prueba de hipótesis [46]. Esta flexibilidad es esencial para el descubrimiento de nuevas ideas y áreas de investigación.
- ❖ *Estudios de Caso Explicativos*: Se centran en desentrañar relaciones de causa y efecto, abordando cuestiones que no han sido estudiadas en profundidad. Este tipo de investigación es útil para explicar por qué ocurre un fenómeno particular [46].
- ❖ *Estudios de Caso Descriptivos*: Ayudan a definir los aspectos de un fenómeno y proporcionan una imagen detallada de personas y eventos, pero no suelen ofrecer nuevos conocimientos. La investigación descriptiva se basa en la recopilación de datos para dar cuenta de una situación o contexto específico [47].

Dado que este trabajo se enfoca en la exploración cualitativa, se clasifica como un *estudio de caso exploratorio*. Esto permite profundizar en el fenómeno de la IO y examinar sus implicaciones sin las restricciones de una hipótesis rígida.

Sobre esta clasificación, el papel del investigador crece en la *etapa de la interpretación*, que empieza al comienzo de la recopilación de datos, el análisis y el uso de la comprensión subjetiva de la situación. El significado de los datos puede ser subjetivo y puede ser la base de varias interpretaciones [48]. Para minimizar interpretaciones erróneas, la metodología utilizada en este trabajo consiste en la *combinación de datos Primarios y Secundarios* [49]. Los datos primarios se refieren a la realización de un estudio de campo con el fin de obtener información por parte del propio investigador sobre un fenómeno particular que se está estudiando con base en la metodología elegida, mientras que los datos secundarios se refieren al uso de información disponible basada en estudios previos que afectan directa o indirectamente el tema de investigación [50]. Las ventajas y desventajas de ambos métodos de análisis de datos se enumeran a continuación [51] [52]:

<u>Datos Primarios</u> (entrevistas, encuestas, experimentos, etc)		<u>Datos Secundarios</u> (informes, documentación electrónica/papel, etc)	
Ventajas	Desventajas	Ventajas	Desventajas
Centrarse en un tema de investigación clave	La necesidad de recursos humanos adicionales	Disponibilidad inmediata de los datos	Es más difícil obtener datos relevantes para las necesidades de los investigadores
Mejor interpretación de la fuente de datos	Alto coste financiero y de tiempo	Disponibilidad de información sobre la metodología de investigación	Información incompleta
Originalidad, relevancia, uso efectivo de la información y singularidad de los datos.	Insuficiente disponibilidad de caso de investigación	Costes reducidos o inexistentes en la obtención de la información	Datos limitados en el proceso de colecta

Tabla 4-1 Análisis comparativo de la metodología utilizada (fuente: elaboración propia del autor)

Mediante la combinación de estos dos métodos, se pueden obtener datos más fiables. En este caso, los datos primarios se refieren a la charla informal con el director ejecutivo de la Agencia y otros miembros de su Consejo de Administración y los datos secundarios implican el análisis de documentos, actas de reuniones, etc. El análisis de documentos se considera una interpretación de varios documentos por parte del investigador y el propósito de este método es extraer y registrar información que luego se utilizará para encontrar respuesta a la pregunta principal de la investigación [53]. Los documentos más habituales para la investigación son documentos escritos [54].

Se ha utilizado principalmente la técnica de la *entrevista*, que implica realizar una serie de preguntas dirigidas a obtener respuestas específicas [54]. Este enfoque es fundamental para profundizar en los temas de interés de mi investigación, ya que permite explorar las experiencias y perspectivas de los participantes de manera detallada.

Además, es crucial llevar a cabo un análisis exhaustivo de los documentos disponibles que se relacionen con las principales cuestiones de investigación [53]. Esta revisión documental ayuda a contextualizar las entrevistas y a respaldar los hallazgos con información adicional. En mi caso particular, al ser delegado en el Consejo de Administración de la Agencia, he tenido acceso a una variedad de documentos relevantes que han facilitado este proceso.

El análisis de documentos es, en términos generales, un proceso de evaluación que busca generar conocimiento empírico y desarrollar una comprensión más profunda del tema en estudio. Este tipo de análisis exige un alto nivel de objetividad por parte del investigador [55], asegurando que los resultados no estén sesgados y reflejen fielmente la realidad.

Finalmente, la metodología utilizada en este trabajo se resume en una figura que ilustra claramente los enfoques y técnicas aplicados en la investigación, destacando la combinación de entrevistas y análisis documental como pilares fundamentales para alcanzar los objetivos del estudio.



Figura 4-2 Diagrama de la metodología empleada (Fuente: Elaboración propia del autor)

Se han seleccionado los métodos de análisis de datos primarios, como las entrevistas, y secundarios, como la revisión de documentación, como base del razonamiento. Desde el principio, estos fueron los métodos óptimos tras evaluar todas las opciones disponibles. Las entrevistas permitieron comparar los datos obtenidos de informes escritos y documentos encontrados en línea, evaluando su integridad. Además, en su calidad de miembro del Consejo de Administración, tuvo acceso a información confidencial que no estaba disponible en línea. Las entrevistas también facilitaron la estructuración de preguntas de manera que se obtuviera información adicional, no accesible ni en línea ni en los documentos de acceso limitado proporcionados por la Agencia. De esta forma, las entrevistas fueron diseñadas para responder directamente a la pregunta principal de la investigación.

El análisis de la documentación fue la parte principal de la investigación, ya que proporcionó acceso instantáneo a la información sobre la IO, la colaboración de la Agencia junto con otras instituciones relevantes de la UE y la metodología de investigación, también me supuso un gran apoyo, todo ello sin contraprestaciones adicionales por mi parte. Sin embargo, fue más difícil obtener datos relevantes para las necesidades específicas y preguntas de investigación, ya que a veces faltaba la información completa, además en los últimos tiempos la Agencia ha tenido que realizar diversos ajustes en su organización y estructura que han supuesto algún contratiempo. Esta desventaja se vio contrarrestada por las facilidades en la realización de las entrevistas, ya que me permitieron hacer preguntas específicas, incluso sobre cuestiones ‘delicadas’.

A partir del análisis de documentos y de una entrevista con el director ejecutivo de la Agencia y demás miembros del consejo de administración, se ha realizado una lista de impulsores y barreras que van a influir en la implementación de la IO.

A continuación, expongo el listado de preguntas que se trasladaron a los miembros de la Agencia y sobre cuyas respuestas he han generado las distintas interpretaciones:

❖ Preguntas Generales

1. ¿Cuáles son los objetivos específicos de la interoperabilidad en los sistemas de información de la UE?

- A) Facilitar el acceso a datos para todos los ciudadanos.
 - B) Mejorar la cooperación y la seguridad entre los Estados miembros.
 - C) Aumentar el uso de tecnología obsoleta.
2. ¿Qué desafíos y limitaciones se han identificado en la implementación de la interoperabilidad?
- A) La falta de voluntad política y coordinación entre agencias.
 - B) La abundancia de recursos tecnológicos disponibles.
 - C) La alta satisfacción de los usuarios con los sistemas actuales.
3. ¿Qué oportunidades se presentan para los ciudadanos y las instituciones de la UE a través de la interoperabilidad?
- A) Mejora en la gestión de fronteras y seguridad.
 - B) Reducción de la comunicación entre países.
 - C) Creación de más burocracia en los procesos.

❖ **Desafíos en la Implementación**

4. ¿Qué obstáculos han enfrentado los Estados miembros en el proceso de integración de sistemas de información?
- A) Diferencias en los lenguajes de programación.
 - B) Diversas legislaciones y marcos legales.
 - C) Un aumento en el número de ciudadanos.
5. ¿Cómo afectan las diferencias en la gobernanza y los marcos legales entre los Estados miembros a la interoperabilidad?
- A) Facilitan la integración de sistemas.
 - B) Dificultan la colaboración y el intercambio de información.
 - C) No tienen ningún impacto.
6. ¿Qué problemas han surgido en términos de adquisición de tecnología y gestión de recursos?
- A) Recursos ilimitados para la tecnología.
 - B) Presupuestos limitados y falta de capacitación.
 - C) Exceso de tecnología disponible en el mercado.

❖ **Aspectos Técnicos**

7. ¿Cómo se gestionan y protegen los datos sensibles en el contexto de la interoperabilidad?
- A) Mediante el cifrado y el acceso restringido.
 - B) No se gestionan ni se protegen.
 - C) A través de copias físicas de los datos.
8. ¿Qué rol juegan las tecnologías emergentes (como inteligencia artificial y análisis de datos) en la mejora de la interoperabilidad?
- A) Facilitan la recopilación y el análisis de datos.
 - B) No tienen un rol significativo.
 - C) Solo crean más complicaciones.

9. ¿Qué componentes técnicos son esenciales para una implementación efectiva de la interoperabilidad?
- A) Software desactualizado.
 - B) Infraestructura de datos y estándares tecnológicos.
 - C) Sistemas no conectados entre sí.

❖ **Implicaciones para los Stakeholders**

10. ¿Cómo perciben los diferentes grupos de interés (ciudadanos, funcionarios de fronteras, instituciones) la interoperabilidad y su implementación?
- A) Como un obstáculo en la gestión de datos.
 - B) Como una herramienta para mejorar la seguridad y la eficiencia.
 - C) Como un gasto innecesario.
11. ¿Qué medidas se han considerado para garantizar la formación y preparación del personal que gestionará estos sistemas?
- A) Capacitación continua y talleres.
 - B) No se están tomando medidas.
 - C) Capacitación limitada solo a unos pocos empleados.
12. ¿Qué tipo de feedback han proporcionado los usuarios sobre la efectividad de los sistemas de información actuales?
- A) Generalmente positivo, pero con áreas de mejora.
 - B) Totalmente negativo sin oportunidades de mejora.
 - C) Los usuarios no han proporcionado feedback.

❖ **Evaluación y Futuro**

13. ¿Cómo se medirán los resultados de la implementación de la interoperabilidad?
- A) A través de auditorías y análisis de desempeño.
 - B) No se medirán.
 - C) Solo se medirán de forma subjetiva.
14. ¿Qué lecciones se han aprendido de proyectos anteriores de interoperabilidad en la UE?
- A) La importancia de la planificación y la colaboración.
 - B) Que no se debe intentar la interoperabilidad.
 - C) Que todos los sistemas deben ser aislados.
15. ¿Cuál es el futuro de la interoperabilidad en la UE, y qué cambios se anticipan en los próximos años?
- A) Un aumento en la fragmentación de sistemas.
 - B) Mayor integración y cooperación entre sistemas de información.
 - C) Estancamiento en los avances tecnológicos.

La interpretación de las respuestas reveló un fuerte apoyo hacia la IO en los sistemas de información de la UE, con una clara identificación de los desafíos y oportunidades. Los participantes eran conscientes de la importancia de la colaboración, la capacitación del personal y la necesidad de una estructura legal coherente para superar las barreras existentes. La percepción positiva general y el reconocimiento de los

beneficios potenciales sugieren que, con las estrategias adecuadas, la interoperabilidad puede mejorar significativamente la seguridad y la gestión de fronteras en la UE.

4.2 Marco teórico y el modelo de Novakouski

En el proceso de búsqueda de posibles marcos teóricos para el estudio de caso, se encontró el que más se ajustaba al propósito del trabajo, el *Marco de Interoperabilidad Empresarial (EIF)*, también conocido como *Enterprise Interoperability Framework*; es un enfoque valioso para recopilar y estructurar conocimientos y soluciones relacionadas con la interoperabilidad empresarial. Este modelo se caracteriza por un enfoque basado en *barreras* que las clasifica en tres niveles: *conceptuales, tecnológicas y organizativas* [56]. El modelo aborda las barreras, de igual manera que la investigación; sin embargo, las barreras que presenta este modelo son de diferente tipo. Las barreras conceptuales se referían a las diferencias sintácticas y semánticas dentro de la información intercambiada [56]. Las barreras tecnológicas tienen que ver con la incompatibilidad de infraestructuras o plataformas. Y finalmente las barreras organizativas se refieren a la delegación de responsabilidades.

Todos los sistemas dependientes de la Agencia son los llamados sistemas centralizados y trabajan en colaboración con los sistemas nacionales (es decir, VIS, SIS y EURODAC), por lo que los sistemas de la Agencia podrían considerarse como sistemas que trabajan para una organización en cooperación con sistemas nacionales que intercambian datos del sistema nacional al central y viceversa. Es difícil afirmar que existen dificultades organizativas ya que cada sistema es diferente dependiendo de los sistemas nacionales. La Agencia no tiene autoridad para acceder a los datos y, a nivel nacional, los diferentes usuarios finales pueden acceder a diferentes partes de los datos según sus derechos de acceso, pero no está unificada en todos los Estados miembros. En principio, todos los sistemas podrían carecer de barreras conceptuales ya que las diferencias sintácticas y semánticas son menos notables debido a que utilizan el mismo sistema operativo (Oracle Application Server). A pesar de que los sistemas podrían crearse en diferentes momentos y tener diferentes tecnologías, siguen siendo parte del sistema central. Sería difícil analizar y comparar las barreras conceptuales, tecnológicas y organizativas de los sistemas nacionales, especialmente porque el foco principal de esta investigación son los sistemas centrales de la Agencia.

Por esa razón, para responder a la pregunta principal de la investigación, se va a utilizar un modelo para comprender la IO, el conceptualizado por Marc Novakouski para lograr objetivos de interoperabilidad exitosa. Estos objetivos son el acuerdo de procesos, el intercambio de funciones y el intercambio de datos.

Este modelo incluye niveles que permiten que los objetivos de interoperabilidad se complementen entre sí para lograr objetivos más complejos. Estos niveles de interoperabilidad son: *Organizativo, Semántico y Técnico*. Además, el modelo propuesto por Novakouski profundiza para descubrir otros factores que también influyen como: *legales, políticos y sociales/culturales*. Estos factores de influencia tienen diferentes impactos dependiendo de la organización o de cualquier sistema de gobierno electrónico. Por eso este trabajo se centrará en aplicar este modelo para evaluar la implementación de la IO en el ámbito de la Agencia y descubrir qué desafíos y oportunidades surgen durante el proceso.

Marc Novakouski ha coescrito estudios y propuestas centrados en la interoperabilidad dentro del sector público, con un enfoque particular en la administración electrónica. Sus investigaciones abordan modelos que incorporan factores legales, políticos y socioculturales, con el afán de mejorar la cooperación entre múltiples sistemas de información. Novakouski promueve la interoperabilidad como una solución para superar las barreras tecnológicas y organizativas que enfrentan los gobiernos. Su trabajo se destaca por proponer enfoques que facilitan la colaboración interinstitucional y optimizan la gobernanza mediante sistemas más conectados y eficientes.

En su propuesta sobre interoperabilidad, Novakouski identifica varios factores que influyen en su implementación, incluyendo aspectos *legales, políticos y socioculturales*. Estos factores son aplicables a cualquier organización, independientemente de su nivel de interoperabilidad, y pueden tener impactos variados [57].

Todas las organizaciones que gestionan información pública deben considerar aspectos legales, como qué contenido puede ser accesible al público; aspectos políticos, como el cumplimiento de políticas y prioridades existentes; y factores socioculturales, como la necesidad de comunicarse con audiencias que no hablan inglés. Abordar estos temas es crucial para lograr la interoperabilidad. Por lo tanto, Novakouski propuso un modelo de interoperabilidad que incluye estos factores de influencia, como se ilustra en la Figura 2-3. Este modelo se ha utilizado como plantilla para analizar las influencias sobre la Agencia, Europol, Interpol, EASO, FRONTEX, IO PMB y la Comisión/Parlamento Europeo/Consejo Europeo.

Todas estas entidades involucradas en la gestión de información pública deben enfrentar varios desafíos al considerar qué información puede ser divulgada. En primer lugar, deben tener en cuenta *cuestiones legales* relacionadas con la transparencia y la protección de datos, asegurándose de que el contenido que se comparte cumple con las normativas de privacidad y derechos de autor. Esto implica evaluar qué datos pueden ser considerados de acceso público y cuáles deben ser resguardados para proteger la información sensible.

Además de los desafíos técnicos y legales que enfrentan las organizaciones, también deben abordar *cuestiones políticas* clave para garantizar el cumplimiento con las políticas y prioridades establecidas a nivel institucional. Estas políticas no solo orientan las operaciones internas, sino que también influyen en la forma en que se comunica la información al público y a otras partes interesadas. Las organizaciones deben alinearse estratégicamente con los objetivos y directrices políticas actuales, asegurando que toda la comunicación respalde las metas institucionales y no contradiga iniciativas prioritarias. Este alineamiento no solo fortalece la coherencia organizacional, sino que también evita malentendidos o conflictos con las autoridades reguladoras. Además, es crucial evaluar cómo la información difundida puede impactar la percepción pública y las decisiones políticas, ya que un manejo inadecuado podría comprometer la credibilidad de la organización o desviar los debates políticos.

Por otra parte, los *aspectos socioculturales* son igualmente significativos y deben ser abordados con sensibilidad y precisión. Las audiencias a las que se dirige la información son diversas, abarcando personas con diferentes idiomas, culturas y niveles de acceso tecnológico. Esto requiere que las organizaciones implementen estrategias inclusivas que garanticen la accesibilidad y la comprensión de la información por todos los grupos interesados. Proveer traducciones precisas en múltiples idiomas, así como adaptar los mensajes al contexto cultural de las audiencias, es esencial para evitar malentendidos y promover una comunicación efectiva.

Abordar estas cuestiones políticas y socioculturales no solo garantiza la alineación con los objetivos estratégicos, sino que también fomenta un entorno más inclusivo y equitativo. Esto es especialmente relevante en el contexto de la interoperabilidad, donde la cooperación y la confianza entre múltiples partes interesadas son fundamentales para el éxito de los sistemas y procesos compartidos.

Para abordar todas estas complejidades y lograr una interoperabilidad efectiva, Novakouski propuso un modelo de interoperabilidad que incluye estos *factores de influencia* [58]. Este modelo sirve como plantilla para analizar cómo la Agencia, Europol, Interpol, EASO, FRONTEX, el Programa de Gestión de Fronteras (PMB) y las instituciones de la Comisión Europea, el Parlamento Europeo y el Consejo de la UE pueden interactuar y colaborar en la gestión de la información. En la figura 2-3, se representarán estos factores de influencia, destacando cómo cada uno impacta en la capacidad de las organizaciones para operar de manera interoperable y eficaz en un entorno complejo.

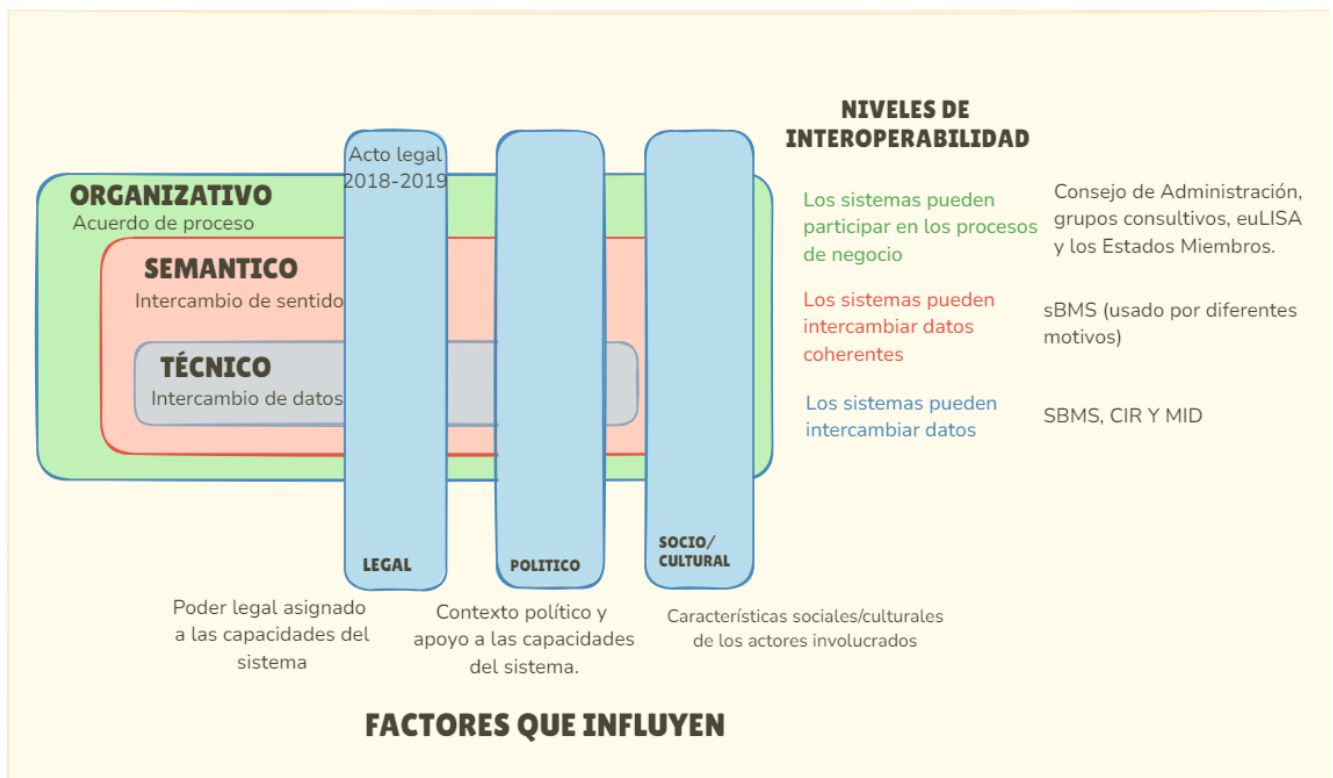


Figura 4-3 Modelo de interoperabilidad propuesto por Novakouski (Fuente: elaboración propia del autor)

4.2.1 Niveles de interoperabilidad en el modelo de Novakouski

El nivel organizativo de la Agencia está compuesto por varias entidades y estructuras clave que garantizan la colaboración y la coordinación en la implementación de la IO de los sistemas de información. Estas incluyen:

- ❖ Consejo de Administración: Es el órgano decisorial principal que supervisa la gestión y el funcionamiento de la Agencia, asegurando que se alineen los objetivos estratégicos de interoperabilidad con las políticas de la UE.
- ❖ Consejo de Gestión del Programa: Este consejo se encarga de la planificación y la ejecución de los programas de interoperabilidad, facilitando la implementación efectiva de las iniciativas en toda la UE.
- ❖ Grupo Asesor de Interoperabilidad: Este grupo proporciona recomendaciones y asesoramiento sobre cuestiones de interoperabilidad, garantizando que se consideren las mejores prácticas y enfoques en la colaboración interinstitucional.
- ❖ Estados Miembros y Agencias de la UE: La colaboración con los Estados miembros es fundamental, así como la participación de agencias como EUROPOL, EASO (Oficina Europea de Apoyo al Asilo), FRONTEX y Eurojust. Cada una de estas entidades tiene un papel específico en la gestión de la seguridad y la migración, lo que resalta la importancia de la interoperabilidad en la compartición de información entre diferentes organismos.

El nivel semántico se centra en la comprensión y la coherencia de los datos compartidos entre sistemas. Dentro del marco de interoperabilidad de eu-LISA, este nivel incluye:

- ❖ sBMS (Shared Biometric Matching System): Un sistema que permite el emparejamiento de datos biométricos de diferentes bases de datos de la UE, asegurando que la información sobre los viajeros se interprete de manera uniforme y coherente.
- ❖ ESP (European Search Portal): Este portal se utiliza para realizar búsquedas en múltiples sistemas de información, facilitando el acceso a datos relevantes de manera rápida y eficiente. El

uso de estos sistemas en diferentes contextos es vital para la interoperabilidad, ya que permite que diversos organismos trabajen con la misma base de datos de manera efectiva.

El nivel técnico incluye todos los componentes y herramientas necesarias para implementar la interoperabilidad. Algunos de los elementos clave en este nivel son:

- ❖ *CIR (Common Identity Repository)*: Este sistema se utiliza para almacenar y gestionar identidades biométricas y no biométricas, proporcionando un repositorio centralizado para acceder a la información de los viajeros.
- ❖ *MID (Multi-Identity Database)*: Un sistema que permite el manejo de múltiples identidades asociadas a una persona, facilitando la verificación y el control de identidad a través de diferentes plataformas.
- ❖ *CRRS (Common Reporting and Registration System)*: Este sistema es fundamental para el registro y la gestión de información sobre las entradas y salidas de los viajeros, asegurando que los datos sean accesibles y utilizables por diferentes organismos.

4.2.2 Factores que influyen en la Interoperabilidad

La implementación eficaz de estos tres niveles de IO es crucial para mejorar la seguridad en las fronteras de la UE, optimizar la gestión de la migración y garantizar que los derechos de los ciudadanos sean respetados. Al facilitar el intercambio de información entre diversas agencias y sistemas, la IO contribuye a una respuesta más coordinada y eficiente ante los desafíos relacionados con la seguridad y la gestión de la migración en Europa.

Marc Novakouski destaca varios factores que influyen en la interoperabilidad de los sistemas de información en el sector público, especialmente en el ámbito de la administración electrónica. A continuación, se presentan estos factores con mayor profundidad:

Es vital identificar las cuestiones legales de las organizaciones públicas como la Agencia para asignar responsabilidades. Las organizaciones deben cumplir con las normas, leyes y reglamentos pertinentes, protección de datos, etc [59]. La Agencia no es una excepción y es responsable de tales preocupaciones, especialmente porque es responsable del desarrollo, mantenimiento y operación de una serie de sistemas. Siempre es importante que los diseñadores de sistemas piensen en los posibles fallos de cualquier sistema y desarrollen una respuesta adecuada a dichas fallos. En su trabajo Novakouski mencionó que abordar cuestiones legales no necesariamente resulta en la creación de una nueva meta de interoperabilidad, sino que más bien influye en metas ya existentes [57].

Los principales objetivos de las medidas legislativas 2017/0351 (COD) y 2017/0352 (COD) surgen de la necesidad de mejorar la gestión de las fronteras exteriores Schengen. Los siguientes artículos del Tratado de Funcionamiento de la Unión Europea constituirían la base jurídica básica: artículo 16, apartado 2, artículo 74, artículo 77, apartado 2, letras a), b), letras d) y e) (Reglamento (CE) 2017/0351-2). El artículo 16, apartado 2, establece que la Unión tendrá competencia para tomar medidas en materia de seguridad de las personas y del tratamiento de datos personales por parte de las organizaciones, agencias y Estados miembros de la Unión. El Consejo debería tomar medidas para garantizar la cooperación administrativa en el ámbito de la libertad y la justicia entre los departamentos de los Estados miembros, como se menciona en el artículo 74. El último artículo 77, apartado 2, habla de que el Consejo y el Parlamento Europeo podrán tomar cualquier medida necesaria para el paso. establecimiento gradual de sistemas de interoperabilidad. Es vital que las fronteras exteriores sean seguras y funcionen con eficacia. Los Estados miembros han acordado abordar estos desafíos compartiendo información a través de sistemas centralizados de justicia y asuntos de interior de la UE.

Antes de utilizar componentes de IO, algunas condiciones necesarias se enumeran en el artículo 76. En primer lugar, se debe proporcionar la formación necesaria sobre cómo se utilizarán los componentes de IO (Reglamento (UE) 2018/1726). El programa de formación debe incluir normas relativas a la protección de datos, la seguridad de los datos y las obligaciones enumeradas en los artículos 32(4), 33(4) y 47.

Es de vital importancia que los componentes producidos se ajusten a la base jurídica bajo la cual se introducen y a los actos de ejecución que los definen. Los responsables del aseguramiento de la calidad deben evaluar constantemente si, durante la implementación del proyecto, el diseño y la creación de los sistemas es compatible con la base legal [60].

Uno de los impactos legales que afectó a la Agencia es el reglamento (CE) 2017/0351-2 que define un conjunto de criterios organizativos para la integración de los componentes de interoperabilidad. En dicho reglamento, el artículo 54 dispone la creación de una Junta Directiva del Programa.

Es importante definir cuáles son las preocupaciones legales relacionadas con los sistemas de información a nivel de la UE y qué influencia podrían tener en la implementación de la interoperabilidad. En el contexto de las reuniones del Comité de Interoperabilidad y del Grupo de Expertos, la Agencia ayudó a la CE y a los Estados miembros en la preparación de las acciones legales pertinentes. Junto con la Agencia, la CE definió los actos delegados y de ejecución necesarios para que las bases jurídicas lleven a cabo las acciones de contratación adecuadas y garanticen que la Agencia cumplirá plenamente el calendario de ejecución previsto. Debieron producirse seis actos antes de finalizar 2019, cinco adicionales en el primer semestre de 2020 y dos para la primera parte de 2021 [61].

Con la introducción de nuevas iniciativas, ha surgido un gran volumen de legislación secundaria que es esencial para el avance de la Agencia. Esta legislación puede traer consigo tanto beneficios como inconvenientes.

- ❖ ***Beneficios:*** La legislación secundaria ayuda a proporcionar un marco claro y específico para la implementación de políticas y procedimientos relacionados con la interoperabilidad y la gestión de datos. Facilita la colaboración entre Estados miembros, ya que establece normas y requisitos comunes que todos deben seguir. Esto es particularmente importante en el contexto del intercambio de datos, donde es crucial que todos los Estados miembros estén totalmente alineados para asegurar la efectividad y seguridad en el manejo de información.
- ❖ ***Inconvenientes:*** Sin embargo, la creación de una gran cantidad de legislación secundaria puede resultar en un proceso complejo y, a veces, burocrático, lo que puede dificultar la agilidad en la implementación de las políticas. Además, puede haber diferencias en cómo cada Estado miembro interpreta y aplica estas regulaciones, lo que podría generar inconsistencias en la práctica.

La única forma de asegurar que todos los Estados miembros estén alineados en el intercambio de datos es a través de la regulación. Existen dos tipos principales de instrumentos legislativos que se utilizan en la UE:

- ❖ ***Directivas:*** Estas establecen objetivos generales que los Estados miembros deben alcanzar, pero dejan un margen considerable para que cada país decida cómo implementarlas. Esto significa que los Estados miembros pueden adoptar diferentes enfoques para cumplir con los mismos objetivos, lo que puede llevar a disparidades en la práctica.
- ❖ ***Reglamentos:*** Por otro lado, los reglamentos contienen prescripciones detalladas que son obligatorias y que todos los Estados miembros deben aplicar de manera uniforme. Esto significa que una vez que un reglamento es adoptado, tiene efecto directo en todos los países de la UE y no requiere que cada Estado miembro lo transcriba a su legislación nacional. Esto promueve una mayor coherencia en la implementación y asegura que todos operen bajo las mismas normas.

Para que la Agencia progrese y los Estados miembros puedan intercambiar datos de manera eficaz, es fundamental contar con una legislación que ofrezca claridad y uniformidad, ya sea a través de reglamentos que exigen una implementación estricta o de directivas que establecen objetivos a cumplir.

La ventaja de este enfoque es que en los actos jurídicos primarios no hay más detalles técnicos, solo objetivos políticos y lo que se debe lograr, lo que no era necesariamente el caso antes [62]. Ahora hay más flexibilidad a medida que la Agencia trabaja junto con la Comisión y los Estados miembros para desarrollar los actos de ejecución y delegados, abordando cuestiones relevantes adecuadas para el propósito. La desventaja es que el número de actos delegados y de ejecución requiere tiempo para

debatirlos, acordarlos y adoptarlos. Para EES todo está en marcha, pero para ETIAS y la IO es un trabajo en progreso. La Agencia, junto con los Estados miembros y la Comisión, acordaron un calendario que prioriza los actos de ejecución que tienen un efecto directo sobre la capacidad de la Agencia para finalizar las especificaciones y realizar las licitaciones.

Hubo riesgos potenciales en el contexto legal asociados con el entorno jurídico y los requisitos, que incluyeron las consecuencias de la posible demora en la implementación de las modificaciones correspondientes al ETIAS. Para mitigar este riesgo, y basándose en las recomendaciones de la Comisión Europea (CE), la Agencia comenzó la preparación de la documentación de licitación de los componentes de interoperabilidad y gestionó los cambios en los actos legales relacionados con las licitaciones durante la implementación [63].

Además, se monitorearon de cerca los impactos en el cronograma y el presupuesto para la implementación, y se involucró la gestión del cambio, cuando se consideró apropiado, para garantizar la alineación de los componentes de interoperabilidad con el marco legal en el momento de la implementación.

El éxito de cualquier implementación de interoperabilidad es de vital importancia y depende en gran medida de factores políticos. Hay cuatro áreas generales de preocupación que contienen barreras relacionadas con la interoperabilidad enumeradas en el informe Gartner [64]. Esas áreas se centran en los departamentos de TI, las administraciones, los responsables políticos y la accesibilidad. Lo interesante es que la lista presenta sólo dos notas sobre cuestiones técnicas. Pero el principal tema común que queda gira en torno a la cooperación entre agencias y varios departamentos. En su estudio, [65] compiló una lista que contiene seis barreras principales de interoperabilidad, cinco de las cuales se centran en cuestiones presupuestarias y de coordinación. Y el borrador del EIF 2.0 percibe factores políticos entre los niveles más altos de interoperabilidad, lo que hace que el apoyo político sea vital para el éxito del proyecto de interoperabilidad [59]. Para evaluar el nivel de cooperación entre diferentes agencias y Estados miembros es necesario tener en cuenta los desafíos técnicos, semánticos y organizativos que afectan la implementación de la interoperabilidad. Y la voluntad política actúa como motor para abordar los problemas que pueda enfrentar el proyecto.

Con respecto a la base de datos de documentos de viaje robados y perdidos (base de datos SLTD) mencionada en el Reglamento de IO (Reglamento (UE) 2019/818) que gestiona INTERPOL, para tener acceso a esta base de datos a nivel europeo debería existir un acuerdo firmado entre la UE e INTERPOL. Según el director ejecutivo (ED) de la Agencia, esto está sucediendo actualmente, pero aún no está implementado y es posible que no esté disponible al comienzo de la nueva arquitectura de interoperabilidad. Además, mencionó que con el tiempo y después de que demuestren su eficiencia, se deberá integrar más los demás sistemas como Registro de Nombres de Pasajeros (PNR), Interfaz de Programación de Aplicaciones (API) y sistemas Nacionales que actualmente no forman parte de la arquitectura de interoperabilidad.

Lo que hace ahora la Agencia no es el punto final, sino más bien un hito en un gran viaje hacia la integración de fuentes de información a nivel europeo. Depende de la voluntad de los Estados miembros de intercambiar datos y de la información y el coraje político de todos los legisladores para afrontar la realidad de que la información es el activo más importante para la seguridad interior y la gestión de fronteras. Esa información no debe ocultarse a puertas cerradas, sino más bien compartirse con las partes interesadas pertinentes.

Aunque los tres niveles de interoperabilidad pueden verse influenciados por factores sociales y culturales, hay otro aspecto crucial que tiene especial importancia: la adopción por parte de los usuarios. Si la información implementada por los sistemas no cumple con el objetivo del gobierno, los Estados miembros y especialmente de los ciudadanos, es posible que los servicios prestados no se adopten plenamente.

La red TNS Political & Social llevó a cabo una encuesta en los 28 Estados miembros para evaluar la opinión del público sobre su conciencia y experiencias en materia de seguridad (Eurobarómetro

especial, 2007). Mientras que una gran mayoría de europeos en su ciudad inmediata y sus vecinos se sienten seguros, están menos convencidos de que la UE sea un lugar estable para vivir.

En general, los factores sociales y culturales desempeñan, aunque significativos, un papel mínimo en la implementación de la interoperabilidad comparó factores legales y políticos.

La Agencia, en cierto modo, es una entidad única en comparación con otras agencias de la UE. Tuvo que comenzar sus operaciones desde el primer día de su existencia, ya que necesitó que hacerse cargo de las operaciones ya existentes y asegurarse de que no hubiera interrupciones en las operaciones, ya que son vitales para los Estados miembros [62]. Desde el primer día de existencia de la organización, demostraron que lo que implementaron era lo suficientemente eficiente y ágil para manejar todo en el momento oportuno. Demostró que tenían confianza y capacidad para hacer su trabajo correctamente y, a medida que crecían sus operaciones, también crecía la confianza de las partes interesadas y los Estados miembros. Además, evolucionaron sustancialmente los sistemas existentes, aumentando su valor para las partes interesadas. Además, la Agencia se convirtió en un asesor de confianza para las partes interesadas políticas a nivel de la UE (Comisión, Parlamento y Consejo) y participó en nuevos desarrollos donde asesoró como experto en capacidades tecnológicas para apoyar iniciativas políticas. Y eso ayudó a la Agencia a generar un alto nivel de confianza en su capacidad para hacer las cosas correctamente e ir más allá de lo que originalmente se consideraba el límite de operaciones y responsabilidades.

Muchas partes interesadas estuvieron involucradas en la arquitectura objetivo de la Agencia. Estas partes interesadas incluían a los ciudadanos de Europa, las instituciones y agencias de la UE, así como a los Estados miembros. Durante el proceso de diseño del proyecto, fue necesario abordar las necesidades de todas las partes interesadas para considerar el proyecto un éxito. Aunque se debieron tener en cuenta todas las opiniones, existió una alta probabilidad de que algunas de ellas fueran opuestas. Por ello, fue vital identificar a las partes interesadas principales para todo el proyecto.

Una de las maneras de conocer las necesidades u opiniones de las partes interesadas fue a través de cuestionarios o encuestas. Estas herramientas se utilizaron para evaluar la satisfacción con el proyecto y obtener retroalimentación sobre el mismo, lo que permitió medir la satisfacción general de las partes interesadas [60].

El estudio realizado por Deloitte recopiló comentarios de las respuestas de la encuesta realizada por las partes interesadas y mostró la necesidad de requisitos adicionales y reveló inquietudes con respecto al proyecto [26]. Las preocupaciones de la Agencia giraban en torno a garantizar que la calidad de los datos cumpliera con los estándares y fuera segura durante su procesamiento, transferencia y almacenamiento. Otra preocupación giraba en torno a que la arquitectura cumpliera con la base legal y fuera capaz de adaptarse a los requisitos cambiantes de las regulaciones y garantizar un rendimiento adecuado del sistema sin salirse del presupuesto.

EUROPOL e INTERPOL desean que sus datos expuestos fueran utilizados adecuadamente. Como propietarios de sistemas nacionales, los Estados miembros quisieron asegurarse de que la arquitectura del proyecto cumpliera con los estándares y permita la funcionalidad necesaria y una alta disponibilidad para que los Estados miembros operen continuamente. Además, es necesario reducir los tiempos de espera y las colas en los controles fronterizos para mejorar el proceso de cruce de fronteras. Los legisladores como el Parlamento Europeo y el Consejo están preocupados principalmente por la seguridad de la UE, la calidad de los datos y las legislaciones sobre privacidad. El Supervisor Europeo de Protección de Datos, que supervisa las actividades de tratamiento de datos personales de la Agencia, estaba preocupado por la proporcionalidad de las medidas y la capacidad de controlar fácilmente todas las actividades en la arquitectura. Las principales preocupaciones de los ciudadanos europeos incluyeron la seguridad general de la Unión Europea y el procesamiento justo/legal de sus datos personales con respecto a sus derechos (principios de privacidad). Los nacionales de terceros países compartieron sus preocupaciones con respecto a la velocidad del procesamiento de los cruces fronterizos y las identificaciones, así como su deseo de que el cruce de fronteras tenga un precio razonable y no sea demasiado inconveniente [62].

5 COMPONENTES TÉCNICOS Y ARQUITECTURA DE LA INTEROPERABILIDAD

Los componentes técnicos de la interoperabilidad de la UE permiten una mayor eficacia en el control fronterizo y la seguridad interna al facilitar el acceso y la gestión de datos a través de múltiples sistemas de información. Estos componentes, que incluyen portales de búsqueda, sistemas biométricos y repositorios de datos, son esenciales para cumplir con los objetivos de seguridad de la UE mientras se optimiza la cooperación entre los Estados miembros.

La interoperabilidad de los sistemas de información de la UE se basa en varios **componentes técnicos clave** que permiten el intercambio eficiente y seguro de datos entre diferentes sistemas. Estos componentes son fundamentales para garantizar una integración coherente de las bases de datos a gran escala y mejorar la seguridad y el control en las fronteras.

5.1 Componentes clave

5.1.1 Portal Europeo de Búsqueda (ESP)

El Portal Europeo de Búsqueda (ESP) tiene como objetivo facilitar el acceso rápido y eficiente a todos los sistemas gestionados por la Agencia, además de permitir la consulta en bases de datos de EUROPOL e Interpol. Este portal actúa como un punto único de búsqueda compartido, conectando los distintos sistemas de información a través de un canal de comunicación seguro. El ESP optimiza la interoperabilidad entre los sistemas, proporcionando a las autoridades pertinentes una herramienta que les permite acceder y consultar información crítica en tiempo real, mejorando así la eficiencia operativa en áreas clave como la gestión de fronteras y la seguridad interna [7].

5.1.2 Repositorio común de identidades (CIR)

El CIR se está creando con el propósito de detectar y prevenir delitos terroristas, respaldar a MID (ver más abajo) y ayudar a identificar correctamente a las personas registradas en VIS, EURODAC, EES, ETIAS y ECRIS-TCN [7]. Puede recopilar y almacenar información biométrica y biográfica básica. Si es necesario, podrá corregir la identificación de nacionales de terceros países independientemente del sistema central. Además, la Agencia, junto con los Estados miembros, implementarán un documento de control de interfaz externo (ICD) para el CIR basado en el formato de mensaje universal (UMF). El CIR no podrá alterar o modificar los derechos de acceso de los usuarios finales ni tratar nuevos datos. En general, el CIR se representa como un componente presente en todos los sistemas que pueden almacenar y recuperar datos de identidad de personas (como la fecha de nacimiento).

5.1.3 Detector de identidades múltiples (MID)

El MID se crea únicamente para apoyar al CIR y dar acceso a los datos almacenados a las autoridades centrales y a la Solicitud de Información Complementaria en la Oficina Nacional de Entradas (SIRENE) del Estado miembro. SIRENE es responsable de cualquier intercambio complementario de información y de la coordinación de actividades que impliquen las alertas del SIS. Como su nombre indica, el MID es responsable de detectar si diferentes nombres se vinculan a la misma identidad y alertar a los guardias fronterizos u otros agentes encargados de hacer cumplir la ley en caso de fraude de identidad [7].

5.1.4 Servicio de comparación biométrica compartida (sBMS)

El Servicio de Comparación Biométrica Compartida (SCB) es un componente clave del sistema de interoperabilidad de la UE, diseñado para mejorar la verificación y comparación de datos biométricos entre diferentes sistemas de información. Este servicio es compatible con el Repositorio Común de Identidad (CIR) y el Sistema de Detección de Identidades Múltiples (MID), facilitando la comparación eficiente de huellas dactilares e imágenes faciales.

El SCB, a través del Sistema de Coincidencia Biométrica (sBMS), permite la recuperación de plantillas biométricas almacenadas en el CIR y el Sistema de Información Schengen (SIS) para comparar y verificar identidades. El Reglamento (UE) 2019/818, en su artículo 12, establece la base legal para el uso de este servicio dentro de los sistemas de información de la UE, asegurando que las autoridades competentes puedan acceder a datos biométricos compartidos para mejorar la seguridad y la identificación en fronteras y otras áreas críticas.

5.1.5 Repositorio Central de Informes y Estadísticas (CRRS)

El Repositorio Central de Informes y Estadísticas (CRRS) es responsable de la generación de informes analíticos y datos estadísticos anónimos sobre los diferentes sistemas de información interoperables de la UE. Este componente se destaca por su capacidad para procesar datos de forma anónima, garantizando que los datos proporcionados no incluyan información personal identificable. Su propósito principal es ayudar en la toma de decisiones estratégicas y proporcionar informes con fines políticos y de presentación de informes estadísticos.

Dado que el CRRS opera de forma automatizada, se limita estrictamente a usos estadísticos y de reporte, asegurando que no se acceda a datos personales con fines operativos. De acuerdo con el Reglamento (UE) 2019/818, específicamente en el artículo 39, el acceso al CRRS está cuidadosamente regulado para evitar cualquier vulneración de la privacidad de los datos personales.

5.2 Arquitectura global de la IO

La siguiente figura ilustra la interconexión de los diversos componentes de interoperabilidad, incluidos el CIR (Common Identity Repository), el MID (Multiple Identity Detector), el sBMS (shared Biometric Matching System) y el CRRS (Common Return and Reintegration System), los cuales se integran para formar un sistema cohesivo. Esta integración no solo facilita la conexión y el intercambio de información entre los distintos sistemas nacionales de los Estados miembros y las bases de datos paneuropeas, sino que también optimiza el uso de los datos dentro de los marcos legales establecidos, como el Reglamento General de Protección de Datos (GDPR), garantizando así la protección de la privacidad y los derechos fundamentales de los ciudadanos.

Al permitir una interacción eficiente entre los sistemas, estos componentes contribuyen de manera significativa a la mejora de la gestión de los controles fronterizos y de la seguridad interna de la UE. El CIR, por ejemplo, ayuda a centralizar las identidades de los ciudadanos y residentes de la UE, lo que facilita la detección de fraude o múltiples identidades falsas. El MID complementa este proceso mediante la identificación y resolución de identidades duplicadas o no verificadas. El sBMS, por su parte, optimiza la verificación biométrica, lo que incrementa la seguridad en los controles de fronteras, mientras que el CRRS facilita la gestión de los procesos de retorno de migrantes, mejorando así las políticas de migración y reintegración.

Además de su impacto en la seguridad y el control de fronteras, la interoperabilidad entre estos sistemas permite generar informes estadísticos detallados que ofrecen datos valiosos sobre flujos migratorios, actividades transfronterizas y situaciones de seguridad interna. Estos informes no solo proporcionan una visión más clara de la situación actual en la UE, sino que también son cruciales para el desarrollo de políticas europeas más efectivas y ajustadas a las necesidades cambiantes, promoviendo una UE más segura, cohesionada y ágil en la toma de decisiones.

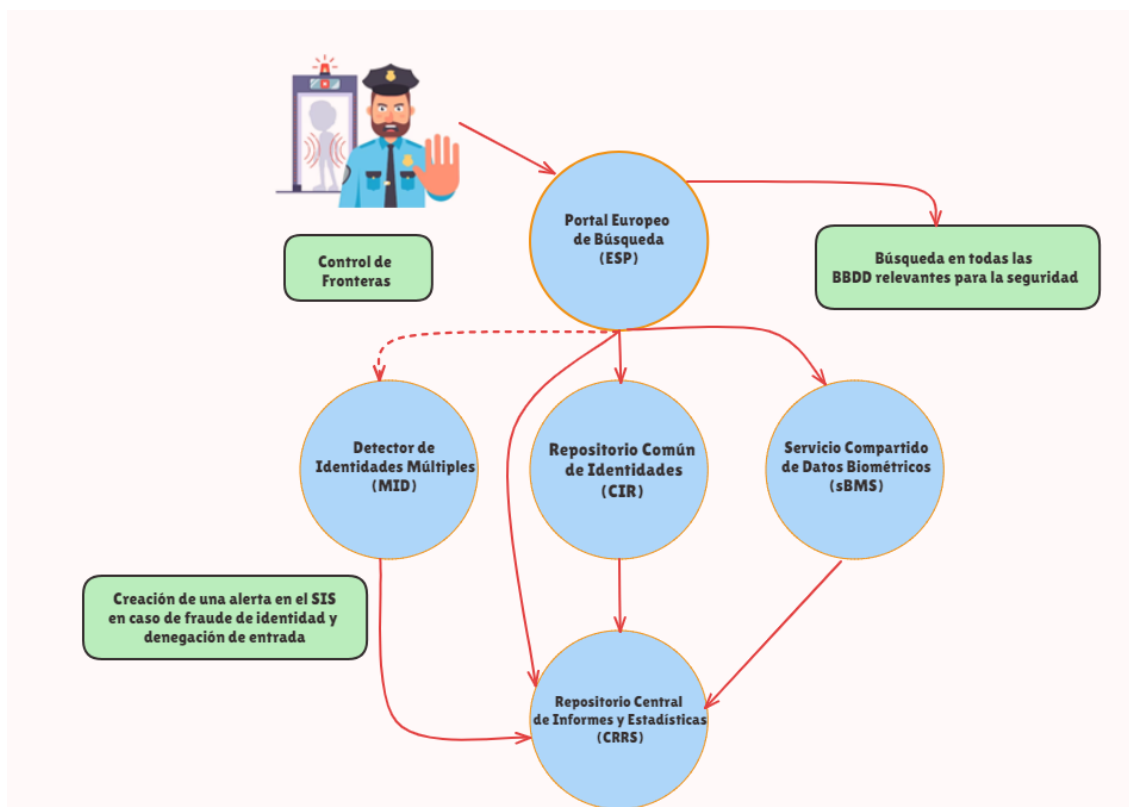


Figura 5-1 Esquema de componentes IO (fuente: elaboración propia del autor)

Los componentes técnicos de interoperabilidad en los sistemas de información de la Unión Europea (UE), tales como el Portal Europeo de Búsqueda (ESP), el Registro Común de Datos de Identidad (CIR), el Modelo de Identidad Múltiple (MID), el Comparador Biométrico Compartido (sBMS) y el Sistema de Referencia Central (CRRS), están diseñados para interactuar de manera sinérgica, facilitando el acceso, la gestión y el intercambio seguro de información crítica. Esta interacción no solo mejora la eficiencia operativa, sino que también refuerza la seguridad y la efectividad de las operaciones de las autoridades responsables de la gestión de fronteras y la seguridad interior.

El Portal Europeo de Búsqueda (ESP) funciona como un punto central que agrupa el acceso a múltiples bases de datos y sistemas de información. Su diseño permite a los usuarios realizar búsquedas de información en diferentes sistemas de la Agencia, así como en bases de datos de EUROPOL e Interpol. Al centralizar el acceso, el ESP reduce la complejidad y la redundancia, mejorando la eficiencia operativa al permitir a los usuarios realizar consultas a través de una única interfaz [63]. Los usuarios finales, como los agentes de fronteras y las fuerzas policiales, pueden acceder a datos relevantes de manera rápida, lo que les permite tomar decisiones informadas en tiempo real.

El Registro Común de Datos de Identidad (CIR) almacena datos biométricos e información crítica de identidad, lo que es esencial para la identificación de individuos que cruzan las fronteras. Este componente permite que las autoridades competentes consulten los datos de identidad cuando sea necesario, contribuyendo significativamente a la seguridad interna. El acceso al CIR está controlado, garantizando que solo los usuarios autorizados, como las fuerzas policiales y Europol, puedan obtener

la información requerida [7]. Esto asegura que la información se maneje de manera segura y se utilice únicamente para fines legítimos, como la prevención del crimen y el terrorismo.

El Modelo de Identidad Múltiple (MID) facilita la identificación y detección de múltiples identidades asociadas a un mismo individuo en diferentes sistemas. Este componente juega un papel crucial en la reducción del fraude y mejora la precisión en la identificación, al consolidar información sobre identidades de diferentes bases de datos desconectadas. A través del MID, las agencias pueden detectar coincidencias entre identidades y asegurar que cada persona tenga un registro único en el sistema, lo que es fundamental para la integridad de la información en la gestión de fronteras.

El Comparador Biométrico Compartido (sBMS) se encarga de comparar datos biométricos, como huellas dactilares y fotos faciales, para identificar a las personas de manera eficiente. Este componente permite que diferentes sistemas de información utilicen una base de datos biométrica única para realizar las comparaciones necesarias, lo que incrementa la interoperabilidad y reduce la duplicación de esfuerzos en la gestión de datos biométricos [63]. Para los usuarios finales, como los oficiales de frontera, el sBMS simplifica el proceso de verificación de identidad, permitiendo un acceso rápido y preciso a la información.

El Sistema de Referencia Central (CRRS) actúa como un sistema vinculante que gestiona las referencias a los datos almacenados en los distintos sistemas de información. Su función principal es facilitar la coordinación entre los diversos componentes de interoperabilidad, asegurando que la información se mantenga actualizada y que las referencias sean precisas. Esto es fundamental para que las autoridades competentes accedan a datos confiables y en tiempo real. Además, el CRRS permite a los usuarios finales, como los analistas de seguridad y los funcionarios de inmigración, obtener una visión consolidada de los datos, lo que mejora la capacidad de respuesta ante situaciones críticas.

La interacción de estos componentes permite que los sistemas de información trabajen de manera integrada, eliminando zonas de sombra donde la información podría perderse o no estar disponible. Los usuarios finales, que incluyen no solo a las fuerzas del orden y a las autoridades fronterizas, sino también a los responsables de la gestión de políticas de seguridad, se benefician de esta interoperabilidad al tener acceso a información precisa y actualizada que les permite tomar decisiones informadas.

Por ejemplo, al realizar una verificación de identidad en un control fronterizo, un agente puede emplear el Portal Europeo de Búsqueda (ESP) para realizar una consulta centralizada en múltiples bases de datos, incluyendo el Registro Común de Datos de Identidad (CIR). A través del ESP, el agente obtiene acceso inmediato a datos biométricos, como huellas dactilares o imágenes faciales, almacenados en el CIR. Estos datos pueden ser analizados mediante el Comparador Biométrico Compartido (sBMS) para verificar si coinciden con otros registros existentes en sistemas interoperables, como el Sistema de Información de Schengen (SIS) o EURODAC.

Si el sBMS detecta coincidencias relacionadas con múltiples identidades, el Modelo de Identidad Múltiple (MID) entra en acción para consolidar los datos y ofrecer una visión integrada de los posibles perfiles asociados a un individuo. Esto permite identificar situaciones de fraude de identidad o casos en los que un individuo ha utilizado diferentes documentos o nombres en distintos Estados miembros. En caso de que se detecten inconsistencias o sospechas de actividad ilícita, el agente puede emitir una alerta a las autoridades competentes, como Europol o las fuerzas policiales nacionales, a través del Sistema de Referencia Central (CRRS), que facilita la comunicación y coordinación entre las entidades relevantes.

Este proceso, que combina la eficiencia de la tecnología con la integración de datos en tiempo real, no solo agiliza el control fronterizo, sino que también fortalece la seguridad interior de la Unión Europea. Al garantizar que los agentes fronterizos tengan acceso a información actualizada, relevante y verificada, se reduce el riesgo de errores y se mejora la capacidad de respuesta ante posibles amenazas. Además, este enfoque refuerza la confianza en los sistemas de gestión de fronteras, al tiempo que respeta las normativas de protección de datos al asegurar que solo los usuarios autorizados accedan a la información necesaria para cada caso. Este modelo también facilita la colaboración entre Estados miembros y agencias de la UE, promoviendo un entorno más seguro y cohesionado [63].

Además de todos los componentes enumerados anteriormente, a la Agencia se le encomendó la tarea de crear un Grupo Asesor de Interoperabilidad (AG) que proporcione experiencia técnica e informes al Consejo de Gestión del Programa (PMB) [7] y estos a su vez a Consejo de Administración (MB).

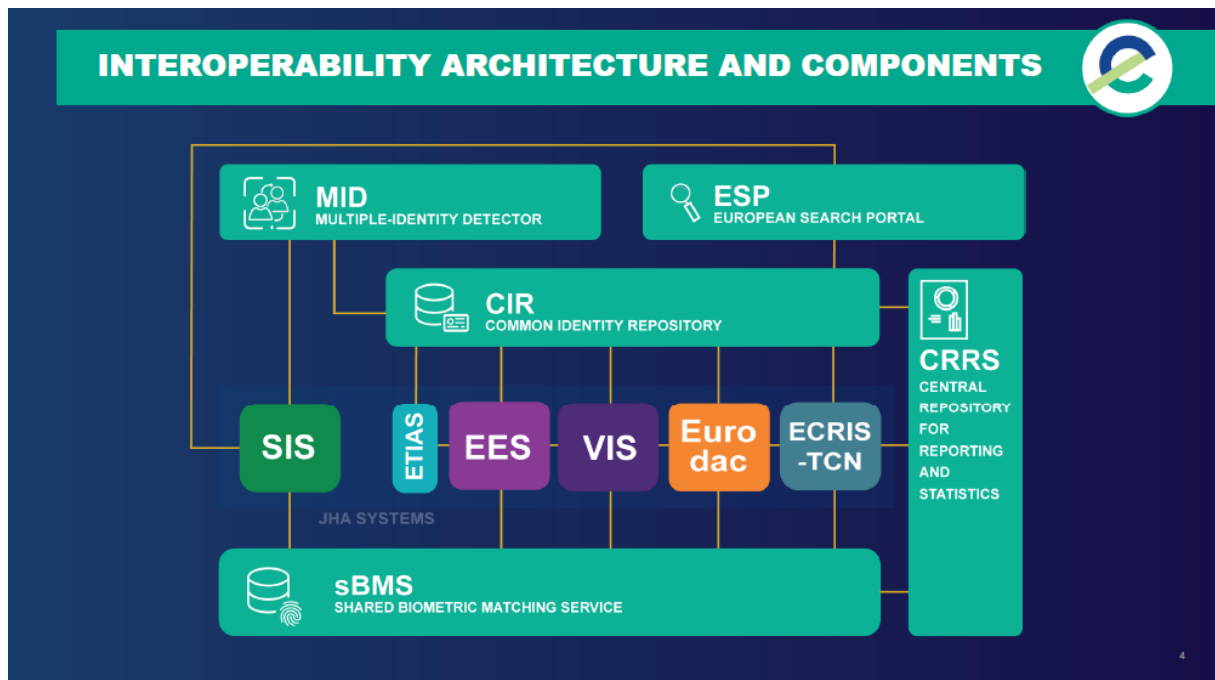


Figura 5-2 Conexión de sistemas relacionados con la IO (fuente: euLISA [13])

6 OBJETIVOS Y OPORTUNIDADES DE LA INTEROPERABILIDAD

La visión estratégica de la arquitectura de interoperabilidad de los sistemas de información de la UE en el ámbito de la gestión de datos y el control fronterizo se basa en tres objetivos de negocio clave que buscan optimizar el acceso a la información, aumentar la seguridad, y mejorar la eficiencia operativa de las fuerzas del orden. Estos objetivos son esenciales para garantizar un uso eficaz de los sistemas de información y para ofrecer un control más robusto de las fronteras exteriores y la seguridad interna de la Unión [66]. A continuación, se describe cómo estos objetivos contribuyen a dicha visión.

6.1 Objetivos técnicos y de negocio

6.1.1 Interconexión y complementariedad de los sistemas

La interconexión y complementariedad de los sistemas representan una estrategia técnica y de negocio esencial para la interoperabilidad de los sistemas de información de la UE. Desde una perspectiva técnica, la interconexión garantiza que los sistemas puedan comunicarse entre sí, compartiendo datos de manera fluida y precisa, mientras que la complementariedad asegura que cada sistema aporte funciones específicas que mejoren la utilidad general del ecosistema. En términos de negocio, estos conceptos son fundamentales para alcanzar objetivos operativos, económicos y estratégicos en la gestión de fronteras y la seguridad interior.

Desde el punto de vista técnico, la interconexión permite a sistemas como SIS II, VIS, EURODAC, EES y ETIAS operar como una red cohesionada, en lugar de funcionar como entidades aisladas. Esto implica el desarrollo de interfaces estandarizadas, la adopción de tecnologías de interoperabilidad como APIs avanzadas y la utilización de estándares comunes para datos y protocolos. Estas capacidades técnicas reducen redundancias, optimizan el uso de recursos tecnológicos y fortalecen la resiliencia frente a amenazas cibernéticas, al tiempo que se asegura la compatibilidad entre sistemas desarrollados en diferentes épocas y con tecnologías diversas.

En el ámbito del negocio, la complementariedad entre sistemas fomenta sinergias que mejoran la eficiencia y efectividad operativa. Por ejemplo, la integración de datos biométricos y biográficos entre EURODAC y EES permite una validación más precisa de identidades, mejorando la toma de decisiones en tiempo real. Además, la colaboración entre estos sistemas reduce los tiempos de procesamiento, mejora la experiencia de los usuarios y facilita la detección de actividades ilegales como el fraude de identidad. Estos beneficios refuerzan la confianza entre los Estados miembros, optimizan la gestión de recursos y aumentan el valor estratégico del ecosistema interoperable para la UE.

A nivel organizacional, la interconexión y la complementariedad también impulsan la adaptabilidad a cambios regulatorios y la capacidad de responder rápidamente a nuevas necesidades o amenazas. Por ejemplo, la integración técnica entre sistemas permite implementar actualizaciones legislativas sin interrumpir la funcionalidad operativa, lo que es crucial en un entorno político y normativo en constante evolución. Esto se traduce en una ventaja competitiva para las instituciones de la UE, permitiéndoles actuar de manera ágil y eficiente en un contexto global complejo.

En resumen, la interconexión y complementariedad de los sistemas de información son objetivos fundamentales que combinan avances técnicos con estrategias de negocio para maximizar la utilidad y el impacto del marco de interoperabilidad de la UE. Su implementación efectiva contribuye no solo a la seguridad y gestión de fronteras, sino también al fortalecimiento de la cooperación y la eficiencia en toda la Unión Europea.

6.1.2 Enfoque modular y adaptabilidad tecnológica

La interoperabilidad de los sistemas de información de la Unión Europea (UE) enfatiza la importancia de un enfoque modular y la adaptabilidad tecnológica para lograr una arquitectura sostenible y eficiente en la gestión de datos y control fronterizo. Este enfoque modular no solo facilita la innovación tecnológica, sino que también permite una mejor integración de principios esenciales como la privacidad desde el diseño y la seguridad por diseño, garantizando que los sistemas puedan evolucionar y mantenerse al día con las amenazas y requerimientos cambiantes sin comprometer la seguridad o la eficacia operativa.

El enfoque modular implica que la arquitectura de los sistemas de información se construya en módulos independientes, pero interconectados, lo que proporciona una gran flexibilidad. Esta modularidad significa que cada componente del sistema puede desarrollarse, actualizarse o modificarse sin que afecte negativamente al funcionamiento del sistema en su conjunto. Esto es fundamental en un entorno como la gestión de fronteras y la seguridad interior, donde las tecnologías y amenazas evolucionan constantemente, y los sistemas deben poder adaptarse rápidamente.

Por ejemplo, en lugar de rediseñar completamente un sistema cuando se requiere una actualización de seguridad o la incorporación de nuevas funcionalidades, la modularidad permite que solo los módulos específicos sean modificados o reemplazados. Esto acelera el proceso de implementación de mejoras y reduce los costos y el tiempo de inactividad del sistema. En el contexto de los sistemas de información de la UE, esto se traduce en una capacidad de respuesta más rápida ante nuevas demandas operativas, como el aumento en los flujos migratorios o la introducción de nuevas regulaciones.

Este enfoque es particularmente relevante en sistemas de gran escala como el Sistema de Información Schengen (SIS), el Sistema de Entrada y Salida (EES) o el Sistema Europeo de Información y Autorización de Viajes (ETIAS), donde los datos se integran a gran escala y es crucial que las actualizaciones puedan realizarse sin causar interrupciones a nivel operativo.

Los medios técnicos para alcanzar los objetivos comerciales relacionados con la interoperabilidad de los sistemas de información son fundamentales para mejorar la eficiencia operativa y la seguridad. La arquitectura diseñada debe ofrecer a las fuerzas del orden un acceso rápido, sistemático y controlado a la información necesaria, eliminando la complejidad de tener que verificar cada sistema individualmente para obtener datos relevantes. Este enfoque no solo agiliza el proceso, sino que también reduce el riesgo de errores que podrían surgir al acceder a múltiples bases de datos [26].

Además, es esencial que la detección de múltiples identidades en diferentes sistemas sea más eficiente para combatir el fraude de identidad. La capacidad de identificar rápidamente si un individuo tiene múltiples identidades en diferentes registros es clave para la integridad del sistema y para garantizar que las fuerzas del orden puedan actuar de manera efectiva. En este contexto, el Portal Europeo de Búsqueda (ESP) jugará un papel crucial al facilitar la correcta identificación de los nacionales de terceros países dentro del territorio europeo. Actualmente, los guardias de frontera deben verificar diferentes sistemas para acceder a los registros de un individuo, lo que puede resultar en un proceso engorroso y

propenso a descuidos. Por lo tanto, simplificar este proceso a través del ESP permitirá un flujo de información más eficiente y seguro.

Asimismo, es vital que las fuerzas del orden tengan acceso a sistemas no policiales para prevenir el crimen y el terrorismo. Este acceso se logrará mediante una nueva consulta de datos de dos pasos, que permitirá a los oficiales verificar posibles "aciertos/no aciertos" en la coincidencia de datos ingresados. Al recibir una alerta cuando se detecta una coincidencia, los oficiales podrán actuar de inmediato, garantizando así una respuesta más rápida y efectiva ante posibles amenazas.

Por último, es fundamental fortalecer tanto la seguridad interna como externa, así como la protección de datos, mediante la implementación de directivas, regulaciones y principios de seguridad relevantes. Esto incluye la aplicación de controles de seguridad a sistemas específicos, asegurando que se respeten los principios de necesidad de saber y privacidad por diseño. Estas medidas son esenciales para proteger la información sensible y garantizar que la IO se lleve a cabo de manera que respete los derechos y la privacidad de los ciudadanos. La combinación de estos medios técnicos no solo facilitará el acceso a la información, sino que también contribuirá a una gestión más segura y eficiente de los datos dentro de la Unión Europea.

Los objetivos de negocio relacionados con la interoperabilidad de los sistemas de información de la UE no solo mejoran el acceso a los datos y la eficiencia operativa, sino que también refuerzan la seguridad y protegen los derechos de los ciudadanos. Estos objetivos son fundamentales para construir una infraestructura de datos segura, interconectada y eficiente, que permita a la UE enfrentar de manera más eficaz los desafíos de seguridad actuales y futuros.

6.2 Oportunidades para los actores clave

6.2.1 Para la Agencia

En la entrevista con el director ejecutivo de la Agencia [62], mencionó que cuando la gente habla de IO, muy a menudo no se dan cuenta de que la interoperabilidad no es una cuestión técnica. Es posible que hayan tenido esa impresión al observar todos los nuevos grandes sistemas de información que están en implementación, pero ese no es el caso. En realidad, la interoperabilidad puede considerarse una iniciativa política que debe desarrollarse, como respuesta de la UE, para satisfacer la demanda y las preocupaciones de los ciudadanos de la UE por una gestión fronteriza más eficiente y una mayor seguridad. Lo que significa que no es sólo un tecnicismo. Otro punto que se planteó durante la entrevista fue que la interoperabilidad traerá una gama de nuevas capacidades que actualmente no están presentes o son limitadas. Esas capacidades cambiarán sustancialmente la forma en que los guardias fronterizos, las fuerzas del orden y los funcionarios de migración hacen su trabajo. La interoperabilidad, en cierto modo, es un gran facilitador e impulsor de una transformación importante en la forma en que se realizan la gestión de fronteras y la seguridad interna en Europa.

La mayor oportunidad en el proyecto general de interoperabilidad es la creación de una nueva arquitectura de información para la seguridad interior y la gestión de fronteras. Paralelamente, también se está construyendo el nuevo ecosistema tecnológico para ayudar a la seguridad interior. La iniciativa más ambiciosa consiste en tener un nivel de estandarización de los equipos y soluciones para recolectar todos los datos y un nivel de estandarización de los equipos y soluciones necesarios para acceder a la información que se gestionará en la nueva arquitectura de información. Lo que hace que ésta sea una de las iniciativas más ambiciosas de los últimos 60 o 70 años es el hecho de que muchos otros países intentaron hacer lo mismo, pero no a la misma escala ni al mismo ritmo. La Agencia tiene previsto llevar a cabo todas las acciones de manera simultánea, así como implementar un enfoque de extremo a extremo en 2024. Esto no solo representa una de las mayores oportunidades, sino que también implica desafíos significativos que deberán ser gestionados cuidadosamente. La integración de múltiples sistemas y procesos en un único marco operativo podría mejorar la eficiencia y la efectividad en la gestión de datos y la seguridad, pero también requiere una planificación meticulosa y la coordinación entre diferentes partes interesadas para garantizar que todos los componentes funcionen de manera cohesiva y sin

interrupciones. La complejidad del proyecto requerirá un sólido enfoque en la gestión del cambio y la capacitación del personal para adaptarse a nuevas tecnologías y métodos de trabajo [62].

6.2.2 Para los sistemas de interoperabilidad

Los dos beneficios más importantes mencionados por Krum Garkov y que forman parte de la agenda política son hacer que el acceso a la información sea más fácil y eficiente. La tecnología desplegada en “silos” realmente no sirve para nada hoy en día, ya que la información es el activo más importante de los datos de la Agencia que debe compartirse al abordar la gestión de la migración. Otro beneficio importante de la es unir los puntos entre diferentes “silos”, donde se guarda la información (diferentes sistemas de información) para brindar acceso a esta información de una manera más eficiente, transparente y rápida.

El próximo gran beneficio proviene de la implementación de un enfoque completamente nuevo e integral para la gestión de identidades. Krum Garkov puso como ejemplo el ataque con camión de Berlín de 2016 al mercado navideño que se cobró la vida de 12 personas. Después de la investigación de los servicios alemanes, resultó que el atacante tenía 14 identidades diferentes en diferentes sistemas europeos y nacionales. Por ese motivo, un enfoque nuevo e integral para la gestión de identidad es un beneficio importante que aporta la arquitectura de interoperabilidad. Con componentes de interoperabilidad como sBMS, CIR, MID, ESP y CRRS, ese tipo de robo de identidad ya no será posible ya que los datos biométricos permanecen de manera unívoca para cada individuo. Esto tiene un enorme efecto positivo en la gestión de fronteras y la seguridad interior.

Una vez que se finalicen los importantes desarrollos y se implemente una nueva arquitectura de la información, esto será de vital importancia para Europa. Esta arquitectura se convertirá en un eje central para el intercambio de información relacionada con la gestión de fronteras y la seguridad interna, lo que implicará que los Estados miembros y las agencias competentes, como FRONTEX y EUROPOL, dependerán en gran medida de ella. Sin embargo, esto también conlleva el riesgo de convertirse en un único punto de fallo, lo que podría tener repercusiones negativas significativas para la UE en caso de que se vea comprometida. Por lo tanto, uno de los objetivos primordiales al desarrollar esta arquitectura de la información es garantizar su máxima resiliencia para reducir la probabilidad de fallos y mitigar los posibles impactos adversos en Europa. Esto se logra implementando el modelo operativo conocido como Activo-Activo para los nuevos sistemas, tal como se mencionó anteriormente.

La situación con los sistemas existentes es ligeramente diferente, ya que VIS y SIS han sido diseñados para funcionar mejor en un servicio "silo" y el servicio activo-activo no está integrado en ellos, lo que significa que es necesario que se produzca un cambio arquitectónico importante en esos sistemas junto con la implementación de la refundición de sus instrumentos legales que agregan una serie de nuevas capacidades a esos sistemas. La Agencia realizó una evaluación de impacto exhaustiva al respecto, que exploró diferentes soluciones técnicas que podrían ser adecuadas para ese propósito, seleccionando la mejor opción para sus necesidades, que se implementarán gradualmente durante los próximos dos a cuatro años [62]. La situación de EURODAC es un poco diferente, ya que fue el primer sistema a gran escala implementado en el ámbito de la justicia y los asuntos de interior. Puede considerarse antiguo y anticuado en todos los aspectos (técnica y arquitectónicamente), por lo que para el EURODAC hay que crear un nuevo sistema. EURODAC 2.0 brindará la oportunidad de incorporar el nuevo concepto de operaciones activo-activo desde cero. En general, incorporar un modelo de operaciones activo-activo en los sistemas eu-LISA será el mayor cambio desde el punto de vista arquitectónico.

Por último, el director ejecutivo de la Agencia menciona el plan para el futuro de integrar muchos sistemas en la nueva arquitectura de interoperabilidad y tener capacidades de acceso a teléfonos móviles. La razón de esto se debe simplemente al hecho de que la nueva arquitectura de interoperabilidad debería beneficiar a los profesionales que están sobre el terreno, como los agentes del orden o la guardia de fronteras. No tienen una infraestructura fácilmente disponible mientras viajan, por lo que necesitan acceder a la información a través de dispositivos y redes móviles. Esto será esencial para la nueva arquitectura de la información y también requeriría algunos cambios arquitectónicos en los sistemas que

ya existen. La nueva arquitectura de la información manejará grandes cantidades de datos e información sin procesar, pero su valor real proviene de su capacidad de entregar la información necesaria a los profesionales sobre el terreno en las fronteras o en los campos de refugiados. Por ese motivo se necesitan soluciones y acceso a la telefonía móvil. Pero eso conlleva riesgos adicionales relacionados con niveles de seguridad mucho más estrictos que deben implementarse.

Por primera vez, los nuevos sistemas como el Sistema de Entrada/Salida (EES) y el Sistema Europeo de Información y Autorización de Viajes (ETIAS) estarán accesibles a través de Internet, lo que representa un cambio significativo en la forma en que se gestionan y procesan los datos relacionados con los viajeros y sus compañías aéreas. Este acceso directo implica que estos sistemas interactuarán no solo con las autoridades de frontera y las agencias de seguridad, sino también con los propios viajeros y las aerolíneas, lo que aumenta la necesidad de implementar medidas de seguridad mucho más robustas.

La apertura de estos sistemas a Internet plantea varios desafíos en términos de ciberseguridad. Dado que los datos personales, incluidos los biométricos, se procesarán y almacenarán en estas plataformas, se requiere un enfoque integral para proteger esta información sensible de ataques externos. Esto incluye la adopción de tecnologías avanzadas de encriptación, sistemas de autenticación multifactor y firewalls de última generación para evitar accesos no autorizados [67]. También es fundamental realizar auditorías de seguridad regulares y pruebas de penetración para identificar y mitigar vulnerabilidades antes de que puedan ser explotadas por actores maliciosos [4].

Además, la implementación de políticas de privacidad y protección de datos es esencial. Esto implica cumplir con normativas como el Reglamento General de Protección de Datos (RGPD) de la UE, que exige transparencia en el uso de los datos y el consentimiento explícito de los viajeros para procesar su información. Las agencias y compañías involucradas deben establecer protocolos claros sobre cómo se manejarán y compartirán estos datos, así como garantizar que solo el personal autorizado tenga acceso a ellos [68].

Desde una perspectiva arquitectónica, se deberá integrar un diseño de seguridad desde el inicio del desarrollo de estos sistemas, lo que significa incorporar medidas de seguridad en cada etapa del ciclo de vida del software. Esto incluye la identificación y clasificación de datos sensibles, la implementación de controles de acceso estrictos y la capacitación continua del personal sobre las mejores prácticas de seguridad [69].

6.2.3 Para los Estados Miembros

Para los Estados miembros la principal oportunidad es mejorar la eficiencia y la eficacia de los servicios en el ámbito de la gestión de fronteras, aumentando su seguridad, especialmente debido a los últimos ataques terroristas.

La demanda de estos servicios aumentó en términos de su eficiencia y el nivel de protección que los Estados miembros brindan a los ciudadanos, pero con la condición de que logren abordar los desafíos que se mencionan más adelante en el texto. Por otro lado, la oportunidad para los ciudadanos es obtener mayor seguridad y estar mejor protegidos en términos de una mayor eficiencia de los servicios gubernamentales. Los efectos más amplios para los ciudadanos son seguir siendo parte de un mercado económico próspero. Europa tiene que mantenerse en la cima del resto del mundo, ya que es parte de la economía global. El director ejecutivo de la Agencia mencionó que en 2017 las personas que llegaron de otros países a la Unión Europea por diversos motivos contribuyeron con casi 300 mil millones de euros al Producto Interno Bruto (PIB) europeo. El beneficio directo para los ciudadanos europeos, además de una mayor seguridad, será que la IO y la forma en que facilitará una gestión fronteriza más eficiente y una mayor seguridad también respaldarán el crecimiento económico.

6.2.4 Para Frontex y Europol

Actualmente, tanto FRONTEX como EUROPOL han mejorado su acceso a información crítica relacionada con la gestión de fronteras y la seguridad interior, lo cual es vital para que ambas agencias realicen su trabajo de manera eficiente. FRONTEX ha estado en proceso de expansión, aumentando su

personal permanente de guardias fronterizos, que se desplegarán en las fronteras exteriores de la Unión Europea para apoyar a los Estados miembros en la protección de estas fronteras.

Sin embargo, como mencionó Krum Grakov, la eficacia de estos despliegues depende de que los guardias tengan acceso a la información adecuada. La integración en una nueva arquitectura de información, que incluye sistemas de IO, beneficiará enormemente a FRONTEX y EUROPOL, permitiéndoles acceder a datos que mejorarán sus flujos de trabajo y operaciones.

Tradicionalmente, la seguridad fronteriza se basaba en aspectos físicos, como vallas y personal. Hoy en día, el enfoque ha cambiado hacia una frontera digital, donde la protección se basa en la información recopilada y utilizada para realizar evaluaciones de riesgo. Esta evolución es crucial para hacer frente a los desafíos actuales, como el aumento de la migración irregular y la evolución de las redes de tráfico humano. Según el análisis de FRONTEX [70], la situación geopolítica sigue generando presiones migratorias significativas, lo que hace aún más necesario un enfoque basado en inteligencia y cooperación internacional para la gestión de fronteras.

7 IMPULSORES, BARRERAS Y DESAFÍOS DE LA INTEROPERABILIDAD

7.1 Impulsores principales

Un estudio realizado por Deloitte identificó seis impulsores y oportunidades principales para la Agencia con la ayuda de las partes interesadas que se pueden aprovechar [26]. Todos los impulsores apuntan y dan forma a la arquitectura del proyecto de una manera única y se enumeran a continuación:

- ❖ Grado de reutilización y uso compartido
- ❖ Migración y planificación ante desastres
- ❖ Adopción del formato universal de mensajería (UMF) y Arquitectura (SOA)

7.1.1 *Grado de reutilización y uso compartido*

La Agencia se apoya en soluciones tecnológicas para gestionar sus operaciones diarias y, en un principio, desarrolló lo que se conoce como "silos" como su estrategia tecnológica. Esta estructura permite una mayor autonomía, pero también contribuye a una arquitectura fragmentada. Para mejorar la interoperabilidad (IO) de sus sistemas y optimizar el funcionamiento de la infraestructura, se propone compartir y reutilizar las soluciones existentes. En este contexto, "compartir" implica el uso de los mismos componentes de hardware y software en distintos sistemas, mientras que "reutilizar" se refiere a la utilización de software previamente desarrollado. Sin embargo, esto requeriría la creación y el mantenimiento de un repositorio que albergue servicios o hardware reutilizables para facilitar el intercambio [71]. El enfoque para optimizar la IO de los sistemas de información se fundamenta en varias premisas esenciales que buscan incentivar la colaboración y la reutilización de recursos [72].

La primera premisa es el intercambio, que se refiere a la práctica de poner a disposición componentes de hardware y software en diferentes sistemas [56]. Este enfoque fomenta la colaboración entre las partes interesadas y permite una mejor optimización de los recursos disponibles. Al facilitar el uso compartido de componentes, la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud puede disminuir la redundancia en los sistemas, lo que a su vez optimiza los esfuerzos de mantenimiento y ayuda a construir un ecosistema de tecnología de la información (TIC) más integrado y cohesivo.

La segunda premisa es la reutilización, que se centra en el uso eficiente del software existente. Esto implica utilizar componentes de software, como módulos, bibliotecas o aplicaciones, en diferentes contextos sin tener que desarrollarlos de nuevo. La reutilización de software no solo ahorra tiempo en el proceso de desarrollo, sino que también asegura que haya coherencia en las aplicaciones utilizadas y minimiza la necesidad de "reinventar la rueda" al aplicar soluciones ya probadas [58] [39].

Para facilitar tanto el intercambio como la reutilización, es fundamental establecer un repositorio de servicios y hardware reutilizables. Este repositorio central podría contener servicios de software que son reutilizables, como módulos, interfaces de programación de aplicaciones (API) o microservicios que pueden ser integrados en diversos sistemas [35]. Además, debería albergar componentes de hardware estandarizados, como servidores, almacenamiento y redes, que se puedan compartir entre las diferentes instituciones y sistemas. El repositorio requeriría mantenimiento constante, actualizaciones regulares y una documentación adecuada para asegurar su efectividad.

Los beneficios de implementar estas prácticas son múltiples. En primer lugar, la reducción de costos es un factor importante, ya que compartir y reutilizar componentes ayuda a evitar la duplicación de esfuerzos, lo que se traduce en ahorros significativos [32]. En segundo lugar, la eficiencia se ve incrementada, ya que la reutilización de soluciones ya verificadas acelera los ciclos de desarrollo, permitiendo a las organizaciones adaptarse rápidamente a nuevas necesidades. También se logra una mayor IO, ya que el uso de componentes comunes mejora la compatibilidad entre los diferentes sistemas. Finalmente, la innovación es impulsada por este enfoque, ya que la colaboración y el intercambio de conocimientos entre los distintos actores fomentan la creatividad y el desarrollo de nuevas soluciones [64].

Para estructurar estos esfuerzos de intercambio y reutilización, se puede emplear un marco para compartir y reutilizar soluciones tecnológicas de la información (TI). Este marco, que se ha desarrollado dentro del programa ISA de la Unión Europea, ofrece directrices claras para las administraciones públicas. Incluye diez recomendaciones clave que buscan promover el intercambio y la reutilización, tales como crear un ambiente innovador y alentar la participación del personal. Adicionalmente, el marco presenta diecinueve medidas de apoyo diseñadas específicamente para organizaciones centrales [59].

Al adoptar estrategias de intercambio y reutilización, la Agencia no solo puede crear un panorama de TI más cohesivo y eficiente, sino también avanzar hacia una interoperabilidad efectiva que beneficie a toda la comunidad de la Unión Europea.

7.1.2 Migración y planificación de la recuperación ante desastres

Los nuevos componentes de cualquier sistema están intrínsecamente ligados a datos existentes, y la integración de estos nuevos elementos no garantiza de inmediato una operatividad total. En este contexto, la migración se refiere exclusivamente a la transferencia de datos, un proceso crucial que permite la adecuación de la información necesaria a los nuevos componentes del sistema. Esta migración de datos puede abrir diversas oportunidades, entre las cuales se destaca la implementación de un enfoque conocido como "Big Bang". Este enfoque implica que todos los datos se transfieren de manera simultánea durante un período de inactividad programado del sistema, lo que puede minimizar el impacto en las operaciones diarias [73].

El método de migración "Big Bang" ha sido recomendado tras un análisis exhaustivo de los documentos y resultados presentados por Deloitte, lo que indica su eficacia en situaciones donde se requiere una integración rápida y completa de los sistemas. Esta estrategia busca garantizar que, al finalizar el proceso de migración, todos los datos relevantes estén disponibles en los nuevos componentes, permitiendo así una transición fluida y efectiva hacia una operatividad óptima del sistema [73]. Sin embargo, aunque este enfoque tiene ventajas, es fundamental considerar los riesgos asociados, como la posibilidad de pérdidas de datos o interrupciones prolongadas en el servicio si no se gestiona [11]. Por lo tanto, es crucial planificar meticulosamente cada fase del proceso de migración para asegurar que se cumplan los objetivos establecidos y que se mantenga la integridad de los datos durante la transición.

En la actualidad se empieza a apostar con más vehemencia por la implementación flexible ya que, permite dividir el proceso de migración en fases más manejables, lo que facilita la identificación y corrección de problemas en etapas tempranas antes de que se conviertan en crisis [74].

Además, el enfoque flexible se adapta mejor a las necesidades cambiantes de los usuarios finales y del entorno operativo. A medida que se implementan nuevos componentes, es posible recibir feedback

continuo y realizar ajustes en tiempo real, asegurando que los sistemas se alineen con las expectativas y requerimientos de los usuarios [75]. Esto es especialmente importante en contextos como el de la interoperabilidad de los sistemas de información de la UE, donde las necesidades de las autoridades pueden evolucionar rápidamente debido a factores externos, como cambios en la legislación o nuevas amenazas de seguridad.

Otro beneficio de la implementación flexible es la capacidad de realizar pruebas y validaciones de los sistemas en paralelo a la migración. Esto permite a los equipos de implementación identificar rápidamente las fallas y realizar ajustes antes de que se complete la migración completa, reduciendo así el tiempo de inactividad y mejorando la satisfacción del usuario final (Williams, 2021).

Finalmente, al optar por una estrategia de migración flexible, las organizaciones pueden minimizar los costos y el tiempo asociados a la migración. En lugar de asumir un gran gasto de recursos para una única migración, las organizaciones pueden distribuir el gasto a lo largo del tiempo, permitiendo una gestión más efectiva de los recursos y reduciendo el impacto financiero general [76].

Es fundamental que la arquitectura del proyecto garantice una alta disponibilidad en todo momento para asegurar que los servicios y sistemas funcionen sin interrupciones. No obstante, en situaciones de desastres u otros eventos inesperados, a menudo resulta difícil estar completamente preparado para enfrentarlos. Por esta razón, es esencial implementar una planificación robusta para la recuperación ante desastres, que incluya diversas estrategias para minimizar los efectos de tales eventualidades. Una solución eficaz para mitigar las repercusiones de un posible desastre es mantener en funcionamiento tanto la Unidad Central (CU) como las Unidades Centrales de Respaldo (BCU). Esto permite que todos los sitios web funcionen simultáneamente, asegurando la coherencia de la información a través de la replicación de mensajes entre los sistemas [75] [77].

Además, se puede considerar la opción de tener dos sitios web físicos activos en todo momento. Esta configuración asegura que, en caso de que uno de los sitios falle, el otro pueda asumir el control de manera inmediata, manteniendo así la continuidad del servicio y reduciendo al mínimo el tiempo de inactividad. Sin embargo, en el escenario más desfavorable donde ambos sitios experimentan fallas, la reactivación de los sistemas requerirá una intervención manual, lo que puede llevar un tiempo considerable para que ambos sitios vuelvan a estar operativos. Este enfoque resalta la importancia de una planificación proactiva y de la implementación de redundancias en la infraestructura para asegurar la resiliencia del sistema ante imprevistos [73].

7.1.3 Adopción del formato de mensaje universal (UMF) y arquitectura SOA

Todos los sistemas de información utilizan formatos específicos para el intercambio de datos, lo que hace imprescindible comprender e interpretar los mensajes durante la comunicación entre diferentes plataformas. Dado que cada sistema opera en su propio formato, es necesaria una adaptación que permita que los sistemas se entiendan mutuamente. Este enfoque, sin embargo, no es el más ideal, ya que complica la comunicación y puede llevar a malentendidos. Por esta razón, es fundamental que cada sistema acuerde un formato común para el intercambio de mensajes, lo que simplifica el diseño, el desarrollo y la gestión de los sistemas. Esta solución se ha consolidado en el formato de Mensaje Universal (UMF, por sus siglas en inglés).

El UMF es un estándar de intercambio de datos diseñado para facilitar las comunicaciones entre sistemas policiales dispersos, y debe ser implementado en una arquitectura interoperable siempre que sea posible. La adopción de este formato común permite un mayor intercambio de información entre la Agencia y las autoridades encargadas de hacer cumplir la ley, en particular los guardias fronterizos. Para asegurar una implementación exitosa del UMF, es recomendable desarrollar un traductor que sea capaz de interoperar con todos los sistemas existentes, además de integrarse de manera nativa con aquellos que adopten el estándar UMF tras realizar los cambios internos necesarios. Este enfoque no solo mejorará la eficiencia en el intercambio de datos, sino que también fortalecerá la colaboración entre las diferentes entidades involucradas en la seguridad y la gestión de fronteras [73].

La Arquitectura Orientada a Servicios (SOA) se caracteriza por la inclusión de diversos servicios que están débilmente acoplados, lo que permite que cada componente opere de forma independiente. La granularidad de estos servicios se establece de acuerdo con el nivel de SOA seleccionado, lo que implica que una mayor finura en la granularidad resulta en servicios individuales más simples y específicos. Este modelo habilita a la Agencia para proporcionar servicios a otros componentes a través de un protocolo de comunicación en red, facilitando así la interacción y el intercambio de información [78] [79].

Al adoptar la SOA, la Agencia logra un avance significativo en la reutilización de servicios, permitiendo que diferentes funcionalidades se implementen de manera eficiente y efectiva. Este modelo no solo optimiza el uso de recursos, sino que también mejora la flexibilidad y la escalabilidad del sistema, ya que los servicios pueden ser modificados, actualizados o reemplazados sin afectar a toda la arquitectura. En resumen, la implementación de la Arquitectura Orientada a Servicios es un paso estratégico para eu-LISA, que potencia la interoperabilidad y la colaboración entre diversos sistemas y componentes, favoreciendo un ecosistema más dinámico y adaptable [73].

Actualmente, se identifica una clara deficiencia en la IO entre los sistemas existentes en lo que respecta a la seguridad y la gestión de fronteras. Es fundamental que estos sistemas se integren en una arquitectura cohesiva que facilite una transferencia fluida de datos, en lugar de operar de manera aislada en "silos". Una de las oportunidades más relevantes para lograr esta integración es a través del uso del Bus de Servicios Empresariales (Enterprise Service Bus, ESB). Este sistema proporciona una plataforma que permite distribuir las tareas entre los distintos componentes conectados de una aplicación, optimizando así el flujo de información y mejorando la eficiencia operativa [74].

Los principios esenciales del ESB incluyen la orquestación, la transformación, el transporte, la mediación y la coherencia no funcional. Estos elementos son críticos para integrar los sistemas existentes y garantizar una comunicación interna efectiva [80]. Además, la conectividad basada en API facilita la exposición de servicios externos, como el Sistema Europeo de Información y Autorización de Viajes (ETIAS). Esta mejora en la accesibilidad a los servicios refuerza también la capacidad de colaboración entre las diferentes entidades implicadas en la gestión de fronteras y la seguridad interior [25].

En resumen, la implementación de un enfoque basado en el ESB se configura como una estrategia clave para abordar la falta de IO y promover un entorno más cohesionado y eficiente en el ámbito de la seguridad y la gestión de fronteras [81].

7.2 Barreras y desafíos

Una de las principales barreras tiene que ver con las políticas de seguridad y privacidad, ya que todo el proyecto debe estar alineado con las decisiones actualizadas de la CE sobre seguridad de las TIC. El ejemplo pueden ser las normas de ejecución (2017/8841 y 2018/559) [82] y la decisión de la Comisión (2017/46) [83]. Además, las propuestas de reglamentos de interoperabilidad dictan un cronograma específico en el que los nuevos sistemas deben estar operativos, al tiempo que respaldan los requisitos de interoperabilidad (2017/0351 y 2017/0352) [84]. Estas propuestas de revisión aún están pasando por los procedimientos legislativos del Consejo, la CE y el Parlamento Europeo.

Entre las preocupaciones más relevantes se encuentra la dependencia de la Agencia de contratistas externos para el desarrollo y la adquisición de soluciones de software. Este aspecto es crítico, ya que la calidad y funcionalidad del software deben alinearse con todos los requisitos establecidos, y, además, el costo debe mantenerse dentro de los límites del presupuesto asignado. La gestión de este proceso es compleja, pues implica no solo la selección de contratistas capaces y competentes, sino también la supervisión constante de su trabajo para asegurar que el software entregue el rendimiento esperado y se ajuste a las necesidades operativas de la Agencia [76].

Durante la implementación de nuevos sistemas, es fundamental que los sistemas existentes continúen funcionando sin interrupciones. La interrupción de servicios podría no solo comprometer la seguridad y eficiencia operativa, sino también socavar la confianza en la capacidad de la Agencia para gestionar la información de manera efectiva. En caso de que surjan problemas que amenacen la

operatividad, debería existir un plan de mitigación detallado, acompañado de un presupuesto razonable, considerando que los recursos financieros de la Agencia son limitados [85].

Además, el Reglamento de Interoperabilidad se fundamenta en las bases jurídicas de otros sistemas de información. Por lo tanto, cualquier cambio en estas bases jurídicas podría tener repercusiones significativas en el diseño y la implementación de la interoperabilidad. Esto implica que la Agencia debe estar atenta a los cambios legislativos y adaptarse rápidamente para asegurar que todos los sistemas permanezcan en conformidad y funcionales [82].

Finalmente, otra preocupación crítica es el riesgo de que el sistema principal experimente un colapso debido a problemas de disponibilidad en la red que afecten al componente central. Un fallo de este tipo podría tener consecuencias devastadoras para la capacidad de la Agencia de gestionar la información de manera efectiva y responder a las necesidades de seguridad en tiempo real. La planificación para garantizar la disponibilidad continua y el rendimiento del sistema es esencial para mitigar estos riesgos, lo que a su vez requiere una inversión considerable en infraestructura tecnológica y capacidades de red.

Desde la perspectiva de la Agencia, la interoperabilidad y la nueva arquitectura de la información son procesos transversales, ya que conectan los puntos entre los "silos" previamente existentes. Para gestionar adecuadamente esta nueva arquitectura, la estructura interna y las capacidades de la Agencia deben alinearse con las demandas de las partes interesadas [62]. Por esta razón, se implementó el modelo conocido como eu-LISA 2.0. Originalmente, la Agencia operaba como una organización de TI clásica, estructurada en torno a varios "silos" grandes, cada uno con su propia pila de servicios y suministros. Este modelo resultaba ineficiente y no respondía a las exigencias del nuevo mandato, que requería un enfoque más transversal [32]. En 2018, se inició una transformación organizativa significativa que incluyó cambios en la estructura, un nuevo modelo operativo y un cambio cultural para adaptarse a las nuevas responsabilidades [73]. Es fundamental que los empleados comprendan y se adapten a este nuevo entorno organizativo, ya que muchos de ellos han pasado la mayor parte de su carrera en una estructura basada en silos. El cambio cultural es crucial para el éxito de esta transformación [35].

Uno de los principales desafíos en la interoperabilidad, además del desarrollo técnico, es rediseñar los procesos comerciales. No basta con tener la tecnología más avanzada si los procesos de negocio siguen siendo obsoletos, ya que esto limitaría el valor añadido [64]. Cambiar la forma en que trabajan los guardias fronterizos y los agentes del orden es esencial para maximizar los beneficios de la interoperabilidad. Otro desafío importante es el desarrollo de capacidades. No basta con implementar nuevas tecnologías; es necesario que las personas comprendan y aprovechen al máximo las nuevas capacidades proporcionadas por estos sistemas. La formación en los Estados miembros es un reto significativo, ya que hay más de 800.000 usuarios del Sistema de Información de Schengen II (SIS II), incluidos agentes del orden, guardias de fronteras y funcionarios de inmigración, todos los cuales necesitan formación para utilizar los nuevos sistemas [62].

El tercer desafío es la capacidad de la industria para satisfacer la gran demanda de equipos y tecnologías necesarios para la interoperabilidad. El calendario de implementación es ajustado, con una fecha límite para principios de 2024, lo que aumenta la presión sobre la industria para ofrecer soluciones rápidas e integradas, especialmente en el contexto de la crisis económica mundial. Además, la medida del éxito de esta iniciativa no depende solo de la tecnología, sino también de la confianza que los ciudadanos depositen en los sistemas. Es vital proporcionar salvaguardias de privacidad y garantizar que los datos se utilicen con fines legítimos y no para vigilancia masiva [7]. Los derechos fundamentales y la privacidad son factores clave [62].

En cuanto a los Estados miembros, también deben adaptarse para aprovechar la nueva arquitectura de interoperabilidad. Esto implica trabajar de manera más transparente y cooperar horizontalmente entre estructuras gubernamentales, rediseñar procesos comerciales e invertir en el desarrollo de capacidades (Comunidades Europeas, 2008). Aunque existen muchas tecnologías detrás de la interoperabilidad, no es solo una iniciativa técnica, sino un programa integral de transformación en la seguridad y gestión de fronteras en Europa. El mayor desafío para los Estados miembros es seguir el estricto calendario de

implementación, lo que requiere una gran coordinación a nivel nacional, ya que el trabajo es extremadamente complejo [62].

Otro reto para la Agencia es que todos los avances en interoperabilidad se están desarrollando en paralelo y son interdependientes. Eu-LISA ha avanzado considerablemente en la implementación del Sistema de Entrada/Salida (SES), pero el Sistema Europeo de Información y Autorización de Viajes (ETIAS) depende del progreso del SES, mientras que la arquitectura de interoperabilidad depende de ambos. Además, la Agencia debe seguir manteniendo operativos sistemas existentes como VIS, SIS II y EURODAC mientras avanza en la nueva arquitectura. Las enmiendas regulatorias de ETIAS y VIS están actualmente en espera debido a la crisis del COVID-19, lo que introduce un riesgo adicional para la agencia [73].

Por otro lado, Europol y Frontex han logrado avances significativos en la adaptación a la nueva arquitectura de interoperabilidad. Ahora cuentan con derechos de acceso comparables a los de los Estados miembros, lo que mejora su capacidad para realizar sus funciones [7]. Sin embargo, deben enfrentarse a desafíos relacionados con la coordinación y la implementación del calendario establecido. Estas agencias también dependen de la colaboración con ministerios y agencias nacionales para garantizar la alineación de políticas y operaciones [65]. El entorno político en los Estados miembros puede influir en su capacidad para cumplir con los plazos.

En términos de contratación, la Agencia enfrenta un desafío considerable debido al tamaño de su cartera de proyectos, que supera los mil millones de euros. Este reto ha requerido una transformación en la arquitectura contractual, pasando de contratos "silo" a contratos translúcidos, lo que obliga a las empresas a crear nuevas alianzas [64]. Las alianzas estratégicas con grandes empresas tecnológicas son fundamentales para la mejora de la infraestructura técnica de interoperabilidad [86].

8 DERECHOS FUNDAMENTALES Y PROTECCIÓN DE DATOS

La interoperabilidad entre los sistemas de información de la Unión Europea (UE) en los ámbitos de las fronteras y la seguridad tiene como objetivo facilitar y agilizar el acceso a datos sobre personas que cruzan las fronteras hacia la UE. Esto incluye la información de nacionales de terceros países, solicitantes de asilo y visitantes temporales. Si bien esta interoperabilidad presenta muchas oportunidades, también implica riesgos en relación con los derechos fundamentales, especialmente la privacidad y la protección de datos personales [87]. Para garantizar que los derechos individuales sean respetados durante el proceso de interoperabilidad, es esencial que se implementen salvaguardias adecuadas, como las establecidas en la Carta de Derechos Fundamentales de la UE [88].

El Supervisor Europeo de Protección de Datos (EDPS) ha enfatizado la importancia de que los sistemas interoperables respeten estrictamente los derechos fundamentales, en particular la privacidad y la protección de los datos personales [87]. Para el EDPS, la interoperabilidad no es solo un avance técnico, sino también un asunto legal y político, dado su impacto en los ciudadanos europeos. Para cumplir con el Reglamento General de Protección de Datos (GDPR), es crucial que estos sistemas sigan principios como la minimización de datos, la transparencia y la seguridad en su tratamiento [89]. Además, se recomienda la implementación de evaluaciones de impacto de protección de datos (DPIA) como un mecanismo esencial para identificar y mitigar riesgos potenciales durante el proceso de interoperabilidad [90].

El marco legal que rige la interoperabilidad está sustentado en el GDPR y complementado por el Reglamento (UE) 2019/818, que introduce normas específicas para sistemas como el Sistema de Información de Schengen (SIS), el Sistema de Información de Visados (VIS) y el Sistema de Entrada/Salida (EES) (Reglamento (UE) 2019/818). Estas disposiciones garantizan que los datos personales se procesen legalmente y para fines específicos, asegurando el respeto a los derechos fundamentales de los ciudadanos.

En cuanto al derecho de acceso de los usuarios finales en el contexto de la interoperabilidad, este está regulado por los artículos 20 y 22 del Reglamento (UE) 2019/818. Dichos artículos especifican los criterios bajo los cuales las autoridades policiales y Europol pueden acceder al Registro Común de Datos de Identidad (CIR) (Reglamento (UE) 2019/818, art. 20, 22). Según el Artículo 20, las autoridades pueden consultar el CIR para identificar a una persona cuando falta documentación válida o hay dudas sobre la autenticidad de los documentos. El Artículo 22 permite el acceso a datos en investigaciones criminales, siempre que existan sospechas fundadas de que una persona está involucrada en delitos graves. Ambos artículos aseguran que el acceso a los datos esté justificado y limitado a lo necesario [7].

La supervisión y control de estos derechos y del manejo de los datos en los sistemas interoperables recaen en el EDPS, quien asegura el cumplimiento normativo y colabora con las autoridades nacionales de protección de datos. El EDPS realiza auditorías regulares y evaluaciones de impacto, trabajando en

coordinación con las autoridades nacionales para garantizar que las normativas de protección de datos se implementen correctamente en los Estados miembros [90]. Estas autoridades también investigan posibles infracciones y tienen la capacidad de imponer sanciones cuando se violan los derechos de los ciudadanos.

Para garantizar una protección adecuada de los datos personales, las agencias de la UE y los Estados miembros deben implementar procedimientos estrictos, que incluyan políticas de seguridad de la información, controles de acceso y auditorías internas regulares. Estos mecanismos ayudan a asegurar el cumplimiento y la efectividad de las medidas de protección de datos [91].

En resumen, la interoperabilidad de los sistemas de información en la UE ofrece importantes beneficios en términos de seguridad y eficiencia, pero plantea desafíos importantes en la protección de los derechos fundamentales. El EDPS y otras autoridades desempeñan un papel crucial en la implementación de mecanismos de control y supervisión para garantizar que la interoperabilidad no comprometa la privacidad y los derechos de los ciudadanos europeos [87].

9 ANÁLISIS

Al describir los factores que influyen en las operaciones de eu-LISA, los sistemas de información de la UE, las instituciones de la UE y los Estados miembros, el modelo de interoperabilidad de Novakouski ha permitido profundizar en la comprensión de los problemas que plantea la implementación de la interoperabilidad. Los factores legales, políticos y sociales revelaron una serie de desafíos y oportunidades a los que se enfrenta no solo eu-LISA, sino también las instituciones mencionadas anteriormente. Mi investigación descubrió seis desafíos y oportunidades principales que conlleva la implementación de la interoperabilidad.

Principales impulsores/oportunidades	Principales barreras/desafíos
1. Acceso a los sistemas interoperables desde dispositivos móviles.	1. Todos los desarrollos se suceden en paralelo al mismo tiempo y son codependientes (big bang).
2. Creación de una nueva arquitectura para la seguridad interior y control de fronteras.	2. Los procesos de negocio de eu-LISA deben ser rediseñados.
3. Mejorar la eficacia y eficiencia de los servicios en el área de la gestión de fronteras.	3. Desarrollo de capacidades y formación.
4. Hacer que el acceso a la información sea más eficiente y amigable.	4. Recursos limitados y dependencia política en los desarrollos.
5. Nuevos sistemas abiertos a internet (EES/ETIAS)	5. Los MS no tendrán que rediseñar sus procesos de negocio adaptado a una forma traslucida de trabajar.
6. Proporcionar a acceso a la interoperabilidad a otras Agencias FRONTEX/EUROPOL.	6. Tiempo muy ajustado para la implementación de la IO.

Tabla 9-1 Oportunidades y Desafíos

- ❖ El enfoque inicial debería centrarse en identificar las principales barreras y desafíos, considerando que los desarrollos se llevan a cabo de manera paralela y son interdependientes. Los avances relacionados con los nuevos sistemas, como el EES, ETIAS y ECRIS-TCN, están ocurriendo simultáneamente. Mientras tanto, los sistemas VIS, SIS II y EURODAC ya están operativos; sin embargo, se prevé una actualización del VIS, y existe la posibilidad de que la

reforma del EURODAC experimente retrasos. Si uno de estos sistemas tiene un retraso debido, por ejemplo, a algunas dificultades con los contratistas, la interoperabilidad total no tendrá una funcionalidad completa. Por tanto, se retrasará la plena funcionalidad de los sistemas de interoperabilidad. La interoperabilidad general se logrará eventualmente, por lo que el problema es sólo con una funcionalidad óptima y completa. Está el desarrollo de la interoperabilidad en sí y, si se retrasa, toda la funcionalidad no estará disponible. Es de suma importancia no tener retrasos en las partes de interoperabilidad y si hay retrasos en otros elementos como EES, ETIAS y ECRIS-TCN, significa que la utilización óptima del sistema se verá afectada.

- ❖ Es necesario rediseñar los procesos de negocio. La implementación del nuevo modelo operativo podría retrasarse y podría haber retrasos en el procesamiento de las solicitudes de cambio, así como retrasos en la implementación total del presupuesto y causar retrasos en la gestión general del proyecto relacionada con la interoperabilidad. El rediseño posiblemente tendrá algunas ineficiencias, por lo que el objetivo principal del personal y la dirección de eu-LISA debería ser finalizar el rediseño de los procesos de negocio lo antes posible, ya que tendrá efecto en todos los elementos.
- ❖ Desarrollo de capacidades y capacitación. El desarrollo de capacidades no es urgente en este momento para la capacitación, ya que la capacitación se realizará más adelante, cuando los sistemas ya estén implementados. Cualquier retraso en los preparativos de la formación no tendrá un efecto significativo ya que todos los elementos estarán listos en un par de años. Es importante para la implementación a largo plazo, pero un pequeño retraso en la creación y optimización de capacidades no es un problema importante, especialmente porque todavía hay tiempo para preparar la subcontratación de la capacitación si fuera necesario.
- ❖ Recursos limitados y dependencia de los acontecimientos políticos. Si la renovación de la enmienda sobre interoperabilidad no crea contradicciones con las características existentes, se podrán añadir más adelante. Es posible que no influyan en el retraso, sino que proporcionen beneficios adicionales en el futuro. Sin embargo, si la enmienda resultará en cambios sustanciales en la arquitectura de información actual, eso podría resultar en el retraso de la implementación actual. En el peor de los casos, podría generar más necesidades presupuestarias y un retraso en la implementación general; en el mejor de los casos, la implementación actual se realizará según lo planeado y se agregarán beneficios adicionales más adelante. Si la modificación requiere cambios sustanciales en la legislación actual y cambios en el diseño técnico de la interoperabilidad, todo el proceso deberá suspenderse.
- ❖ Los Estados miembros tendrán que rediseñar sus procesos empresariales y adaptar una forma transparente de trabajar. Es tan importante para los Estados miembros rediseñar sus procesos comerciales como lo es para eu-LISA. Sin embargo, los Estados miembros son usuarios finales, por lo que tienen más tiempo hasta que los sistemas estén operativos o al menos en la fase de prueba, lo que hace que sea más vital para eu-LISA rediseñar sus procesos comerciales.
- ❖ Calendario ajustado para la implementación de la interoperabilidad. En el escenario en el que todos los Estados miembros están preparados, pero el sistema central no, una de las formas en que eu-LISA puede acelerar el proceso es destinando dinero a recursos adicionales, como empleados adicionales. Si los Estados miembros también se enfrentan a un retraso, el único inconveniente es llegar tarde, sin implicaciones financieras adicionales. Cualquier retraso, ya sea en la contratación o en la contratación de personal, podría afectar a la reputación de eu-LISA. No tener los sistemas listos a tiempo será un pequeño inconveniente, ya que los sistemas ya existentes seguirán funcionando. Sin embargo, la reputación de eu-LISA podría verse dañada.
- ❖ En cuanto a las oportunidades, destaca el acceso a los sistemas interoperables desde dispositivos móviles, considerado uno de los elementos clave. No obstante, existe el riesgo de que sea necesario adaptar la base jurídica en determinados Estados miembros para autorizar dicho acceso. Esta medida representa una importante ventaja para los agentes de fronteras en trenes, barcos y pasos fronterizos para automóviles, donde deben interactuar físicamente con las

personas en lugar de esperar su llegada. Es fundamental que se alcance un consenso político y se aprueben las modificaciones legales con suficiente antelación. Una vez logrado este paso, se espera que la usabilidad de los sistemas mejore significativamente.

- ❖ La creación de una nueva arquitectura de información para la seguridad interna y la gestión de fronteras proporcionará una escalabilidad total de los sistemas y la economía final a largo plazo. Desde el punto de vista económico, el desarrollo a largo plazo de la arquitectura de la información es la parte más importante.
- ❖ La mejora de la eficiencia y la eficacia de los servicios en el ámbito de la gestión de fronteras en los Estados miembros permitirá a las personas esperar menos tiempo en los puntos de control. También se agradece la oportunidad de agregar teléfonos móviles, lo que hace que el acceso a la información sea más fácil y eficiente para una mejor gestión del tiempo en el cruce de fronteras.
- ❖ La apertura de nuevos sistemas a Internet (EES y ETIAS) es una oportunidad, pero también un gran riesgo. Ciertos elementos de ETIAS deben estar abiertos a través de Internet, por lo que el sistema debe ser a prueba de balas para evitar cualquier tipo de piratería. Será más fácil para los usuarios finales introducir y obtener los documentos requeridos, pero al mismo tiempo es un riesgo alto que eu-LISA debe abordar e idealmente mitigar.
- ❖ Proporcionar a otras agencias como FRONTEX y EUROPOL acceso a la información de los sistemas de interoperabilidad tendrá oportunidades adicionales. La Agencia facilita el trabajo de otras agencias, no sólo de los ciudadanos. FRONTEX proporcionará guardias fronterizos a los Estados miembros si así lo solicitan y EUROPOL proporcionará información a los sistemas eu-LISA sobre actividades delictivas, al tiempo que tendrá acceso a sus sistemas.

10 CONCLUSIONES Y LÍNEAS FUTURAS

A lo largo de los últimos años se ha producido un cambio significativo en los ámbitos del control de fronteras, la seguridad interior y la gestión migratoria, pasando del entorno físico al virtual. La heterogeneidad de los sistemas de información de la UE actualmente vigentes complica innecesariamente el acceso a los datos. Puede generar puntos ciegos para los organismos encargados de hacer cumplir la ley, ya que los vínculos entre fragmentos de datos pueden ser muy difíciles de identificar. Esta fragmentación se aborda mediante la interoperabilidad de los diferentes sistemas de información a nivel de la UE. Esto garantiza que los sistemas puedan complementarse entre sí, de modo que cuando lo necesiten, las personas adecuadas tengan acceso a la información que necesitan.

La Comisión está completando este trabajo introduciendo nuevos instrumentos para desarrollar los sistemas de información de la UE y garantizar la cohesión entre ellos. La interoperabilidad entre sistemas ayudará a abordar la migración irregular, identificar correctamente a las personas, combatir el fraude de identidad, validar los documentos de viaje y, en última instancia, contribuirá a un mayor nivel de seguridad dentro del espacio de libertad, seguridad y justicia de la Unión.

El análisis del estado del arte revela que, a pesar de los esfuerzos realizados, aún persisten desafíos considerables. La implementación de la arquitectura de interoperabilidad se ha visto obstaculizada por la falta de preparación técnica y la necesidad de una reforma legislativa significativa. Según un informe de la Comisión Europea (2023), las discusiones sobre la interoperabilidad a menudo se centran en los aspectos técnicos, pero los factores políticos y sociales juegan un papel igualmente crucial. La resistencia al cambio por parte de los Estados miembros y las diferencias en las capacidades técnicas son barreras que deben ser superadas para avanzar hacia una interoperabilidad efectiva.

El objetivo principal de la Comisión de la UE es mitigar la amenaza a la seguridad de los ciudadanos. Reducir el número de turistas no es favorable ya que está vinculado con el crecimiento económico. El hecho de que sistemas como VIS, SIS y EURODAC se crearon en épocas diferentes con diferentes tecnologías, creó la necesidad de interoperabilidad para unificar todos estos sistemas y reorganizarlos para su uso óptimo. Este trabajo se hará en beneficio no solo de la Agencia, sino también de los ciudadanos, las instituciones de la UE, otras agencias y los Estados miembros.

Los objetivos de esta investigación, establecidos en la introducción, incluyen identificar los desafíos en materia de adquisiciones, gobernanza, gestión de recursos e implementación operativa relacionados con la interoperabilidad, así como explorar las oportunidades que esta brindará a ciudadanos, Estados miembros e instituciones de la UE. La tesis busca proporcionar una visión integral que permita entender las implicaciones de la interoperabilidad desde una perspectiva holística y centrada en el impacto real.

El proyecto se presenta como una iniciativa de enorme relevancia política, con un alto nivel de riesgo y costes financieros significativos, además de estar lleno de desafíos, siendo considerado el más

ambicioso de los últimos 60 o 70 años, según lo señalado por el director ejecutivo de la Agencia. No obstante, existe una firme convicción de que la implementación de la interoperabilidad será exitosa y proporcionará los beneficios esperados tanto para la Agencia como para las instituciones de la UE y los Estados miembros.

Este trabajo ha explorado a fondo los desafíos y oportunidades que enfrenta la Agencia y las instituciones asociadas al implementar un marco interoperable en el contexto de la seguridad y la movilidad. A través de una investigación cualitativa, se han identificado factores legales, políticos y sociales que influyen en el éxito de estas iniciativas.

Asimismo, se ha basado en un enfoque cualitativo utilizando entrevistas semiestructuradas con expertos de la Agencia y representantes de Estados miembros, así como un análisis del modelo de interoperabilidad de Novakouski. Esta metodología permitió obtener una comprensión rica y matizada de las dinámicas en juego. Se identificaron seis desafíos y oportunidades principales, que incluyen la necesidad de colaboración entre agencias, la adaptación a nuevas tecnologías y el desarrollo de un marco legal coherente.

Este estudio ha destacado la importancia de la interoperabilidad en la seguridad y la gestión de fronteras de la UE. A pesar de los desafíos identificados, como la resistencia política, la preparación técnica y la falta de un marco legal coherente, las oportunidades para mejorar la eficiencia y la colaboración entre agencias son significativas. La implementación efectiva de la interoperabilidad no solo es crucial para el éxito de la Agencia y la UE, sino que también tiene el potencial de beneficiar a los ciudadanos al proporcionar un acceso más eficiente a la información y una gestión más efectiva de las fronteras.

Para el futuro, se identifican tres líneas de acción prioritarias:

1. **Desarrollo de capacidades técnicas:** Invertir en la actualización de infraestructuras tecnológicas y en la formación del personal para garantizar que los sistemas puedan operar de manera eficiente bajo el marco de interoperabilidad.
2. **Colaboración y armonización legislativa:** Fomentar la colaboración entre los Estados miembros para establecer un marco normativo unificado que facilite la implementación de la interoperabilidad, respetando al mismo tiempo los principios de protección de datos y los derechos fundamentales.
3. **Evaluación continua y mejora:** Diseñar mecanismos para monitorear y evaluar el impacto de la interoperabilidad, asegurando la identificación rápida de problemas y el ajuste oportuno de las estrategias implementadas.

En un mundo cada vez más interconectado y dinámico, la interoperabilidad no es simplemente una opción tecnológica, sino una necesidad estratégica para la seguridad y la eficiencia de la Unión Europea. Este proyecto representa el compromiso de Europa por superar barreras históricas y aprovechar al máximo el potencial de sus sistemas de información. No es solo una cuestión de mejorar procesos; es una apuesta por garantizar que las fronteras sean más seguras, las decisiones más rápidas y los derechos de los ciudadanos más protegidos. La interoperabilidad es el camino hacia una Europa más unida, resiliente y preparada para los desafíos del futuro.

11 BIBLIOGRAFÍA

- [1] EUROPOL, «Informe sobre la situación de la delincuencia organizada y la delincuencia grave en la UE,» 2021.
- [2] Comisión Europea, Migración y Asuntos de Interior., «"Strengthening Border and Migration Management,"» 2023.
- [3] Comisión Europea, «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad,» Bruselas, 6.4.2016 COM(2016) 205 final, Bruselas, 2016.
- [4] NIST - National Institute of Standards and Technology, «NIST SP,» 2018. [En línea]. Available: <https://doi.org/10.6028/NIST.SP.800-160v1>.
- [5] Comisión Europea, *Frequently asked questions - Interoperability of EU information systems for security, border and migration management*, Strasbourg: Fact Sheet, 2017.
- [6] Comisión Europea, «Comunicación de la Comisión al Parlamento Europeo y al Consejo,» 2020.
- [7] Parlamento Europeo y Consejo de la Unión Europea, *Reglamento (UE) 2019/818, de 20 de mayo de 2019, por el que se establece un marco para la interoperabilidad entre los sistemas de información de la Unión en el ámbito de las fronteras y los visados*, 2019.
- [8] Comisión Europea, «Live, work, travel in the EU,» 2018. [En línea]. Available: https://home-affairs.ec.europa.eu/what-we-do/policies/borders-and-visas_en.
- [9] T. G. & W. Cummings, «Organization Development and Change (10th ed.). Cengage Learning,» 2015.
- [10] eu-LISA, «eulisa.europa.eu,» 2024. [En línea]. Available: <https://www.eulisa.europa.eu/>.
- [11] I. S. A. G. I. & O. Olaronke, « Interoperability in Healthcare: Benefits, Challenges and Resolutions,» *International Journal of Innovation and Applied Studies*, vol. 3, nº 1, pp. 262-270, 2013.
- [12] Parlamento Europeo y Consejo, *Reglamento (UE) n.º 1025/2012*, 2012.
- [13] euLISA, «https://www.linkedin.com/posts/eu-lisa_it-strasbourg-france-activity,» 2022. [En línea].

- [14] Comisión Europea, «Hoja de Ruta para la Interoperabilidad de los Sistemas de Información en la UE,» 2023.
- [15] eu-LISA, «eu_LISA,» noviembre 2023. [En línea]. Available: <https://www.eulisa.europa.eu/Newsroom/News/Pages/Updated-roadmap-to-Interoperability-endorsed-by-EU-Council.aspx>.
- [16] Organización Internacional de Normalización (ISO), *ISO/IEC 2382: Information Technology - Vocabulary*, 2000.
- [17] Comisión Europea, *Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, por el que se establece un marco para la interoperabilidad entre los sistemas de información de la Unión en el ámbito de las fronteras y los visados*, 2019.
- [18] Comisión Europea, *Hoja de Ruta para la Interoperabilidad de los Sistemas de Información de la UE*, 2016.
- [19] Comisión Europea, «Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece un marco de interoperabilidad entre los sistemas de información de la Unión Europea,» 2016.
- [20] Consejo de la Unión Europea, *Decisión 2007/533/JHA del Consejo, de 12 de junio de 2007, sobre el establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II)*, 2007.
- [21] Comisión Europea, «Documento de trabajo de los servicios de la Comisión: Informe sobre la mejora de la gestión de los sistemas de información de la Unión Europea,» 2018.
- [22] Comisión Europea, «Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la modificación del Reglamento (UE) 603/2013 relativo al sistema Eurodac para la comparación de huellas dactilares de solicitantes de asilo y de personas detenidas,» 2016.
- [23] eu-LISA, «eu-LISA,» 2024. [En línea]. Available: <https://www.eulisa.europa.eu/>.
- [24] Comisión Europea. "Sistema de información de visados - VIS", 2021.
- [25] J. Roberts, «"Enhancing Accessibility and Collaboration in Border and Security Management",» *European Security Review*, vol. 22, nº 4, pp. 112-230, 2019.
- [26] eu-LISA, «(dwp 1.01) Documentos de trabajo sobre la interoperabilidad en la UE,» 2020.
- [27] Organización Internacional de Normalización (ISO), *ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements*, 2013.
- [28] Comisión Europea, *Marco Europeo de Interoperabilidad (EIF) para los servicios públicos europeos.*, Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2017.
- [29] Comisión Europea, *Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre la creación de un sistema de información sobre visados y sobre la gestión de las fronteras*, 2002.
- [30] Comisión Europea, «Interoperability Solutions for European Public Administrations,» 2004.
- [31] Comisión Europea, *Comunicación de la Comisión al Parlamento Europeo y al Consejo: "Una nueva agenda para la migración"*, 2017.

- [32] F. Vernadat, «Enterprise Interoperability: A Key Challenge for SMEs,» 2009.
- [33] Comisión Europea, «European Interoperability Framework for European Public Services: Version 2.0 (IDABC Draft),» 2010.
- [34] J. Lewis, « Framework for Information System Interoperability: Technical and Organizational Aspects,» *Journal of Interoperability and Information Sharing.*, 2008.
- [35] J. Gibbons, «Information Interoperability: Principles and Practices,» de *En Proceedings of the International Conference on Information Systems.*, 2007.
- [36] Galliers, «Choosing appropriate information systems research approaches: A revised taxonomy.,» de *Information Systems Research: Issues, Methods and Practical Guidelines* , R. D. Galliers, 1992, pp. 144-162.
- [37] R. E. Stake, «Qualitative Case Studies,» de *The Sage Handbook of Qualitative Research*, Sage Publications, 2005, pp. 443-466.
- [38] D. E. Polkinghorne, «Narrative Configuration in Qualitative Analysis,» de *Life History and Narrative*, The Falmer Press, 1995, pp. 5-23.
- [39] D. & Z. R. Carney, *A Framework for Enterprise Interoperability*, 2011.
- [40] M. Harris, *The Rise of Anthropological Theory: A History of Theories of Culture*, New York: Thomas Y. Crowell Company, 1968.
- [41] A. S. y. J. Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Thousand Oaks, California: Sage Publications, 1998 (2ª edición).
- [42] M. V. Manen, *Researching Lived Experience: Human Science for an Action Sensitive Pedagogy*, Albany, New York: State University of New York Press (SUNY Press), 1990.
- [43] R. K. Yin, *Case Study Research: Design and Methods*, Beverly Hills, California: Sage Publications, 1984.
- [44] J. Gerring, *Case Study Research: Principles and Practices*, Cambridge, Reino Unido: Cambridge University Press, 2007.
- [45] QuestionPro, «<https://www.questionpro.com/blog/es/metodos-de-investigacion-cualitativa-y-cuantitativa>,» [En línea].
- [46] R. K. Yin, *Case Study Research: Design and Methods* (2nd ed., 1994; 5th ed., 2014), Sage Publications, 2009.
- [47] C. Robson, *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*, Blackwell Publishing, 1993.
- [48] A. & P. D. Klotz, *Qualitative Methods in International Relations: A Pluralist Guide*, Palgrave Macmillan, 2008.
- [49] E. P. Douglas, *Qualitative Research in Engineering Education: A Guide for Engineering Educators*, Springer, 2015, pp. 141-164.
- [50] O. Mesly, «More on Data Percolation,» de *Creating Models in Psychological Research*, Springer, 2015, pp. 1-10.

- [51] R. Johansson, *Case Study Methodology*, Emerald Group Publishing Limited, 2003, pp. 1-11.
- [52] R. & D. M. Vanwysberghe, «Research Design in the Study of Practice: A Case Study of the Case Study Method,» de *Research Methods in Education*, Sage Publications., 2007, pp. 150-162.
- [53] G. A. Bowen, «Document Analysis as a Qualitative Research Method,» *Qualitative Research Journal*, vol. 9(2), nº Qualitative Research Journal, pp. 27-40, 2009.
- [54] Z. O'Leary, *The Essential Guide to Doing Your Research Project* (3rd ed.), Sage Publications, 2014.
- [55] Triad 3, *An Introduction to Document Analysis*. (Recuperado de TRUBOX), N/A, 2016.
- [56] D. Chen, «Enterprise Interoperability: A New Approach to Knowledge and Information Systems,» de *Enterprise Interoperability II: A Comprehensive Overview*, Springer, 2006, pp. 155-162.
- [57] Carnegie Mellon University Software Engineering Institute, *Enterprise Architecture: A Framework for the Implementation of Interoperability*, Carnegie Mellon University Software Engineering Institute, 2011.
- [58] M. Novakouski, *A Framework for Interoperability in the Public Sector: Building an Interoperable Architecture*, Software Engineering Institute, Carnegie Mellon University, 2014.
- [59] Comunidades Europeas, «Interoperability of European Information Systems: Guidelines and Recommendations,» 2008.
- [60] eu-LISA, «(DWP 3.02) Documentos de trabajo sobre la interoperabilidad y la calidad de los sistemas,» 2020.
- [61] eu-LISA, «Informe IO PMB 2020-15,» 2020.
- [62] K. Garkov, Interviewee, [Entrevista]. Noviembre 2021.
- [63] euLISA, «Informe del gestor del programa de IO,» Tallin (Estonia), 2019.
- [64] S. Malotaux, *Interoperability: The Need for a New Approach*, Gartner Research, 2007.
- [65] S. Varney, «Interoperability in the Public Sector: An Analysis of Barriers and Solutions,» 2006.
- [66] Comisión Europea, https://ec.europa.eu/home-affairs/what-we-do/policies/interoperability_en, 2020.
- [67] R. G. J. & K. S. Böhme, «"Advanced Encryption and Multi-Factor Authentication in Cybersecurity",» *International Journal of Network Security*, vol. 12, nº 4, pp. 225-237, 2015.
- [68] A. Cavoukian, «"Privacy by Design: The 7 Foundational Principles",» 2011.
- [69] ISO, «"ISO/IEC 27001:2018 - Information technology — Security techniques — Information security management systems — Requirements",» 2018.
- [70] FRONTEX, «"Risk Analysis for 2023",» 2023.
- [71] S. y. R. M. Lloyd, «"The Role of Reusable Services and Hardware in Facilitating System Interoperability",» *International Journal of Information Technology Systems*, vol. 12, nº 2, pp. 145-160, 2021.

- [72] T. Benson, «"Optimizing Information Systems Interoperability: Foundations and Key Principles",» *Journal of Information Systems and Technology Management*, vol. 17, nº 3, pp. 231-245, 2020.
- [73] Deloitte, «Data Migration Strategy: Best Practices for Successful Data Migration,» 2019.
- [74] T. H. y. H. J. G. Davenport, *Competing on Analytics: The New Science of Winning*, 2018.
- [75] A. y. J. B. Smith, «"Message Replication for Information Consistency in Distributed Systems",» *Journal of Distributed Computing*, vol. 18, nº 4, pp. 89-102, 2022.
- [76] W. M. y. L. D. A. Cohen, «Absorptive Capacity: A New Perspective on Learning and Innovation,» *Administrative Science Quarterly*, vol. 35, nº 1, pp. 128-152, 1990.
- [77] D. Williams, «"Ensuring Data Integrity Through Message Replication in Web Systems",» *Journal of Network Architecture*, vol. 15, nº 3, pp. 215-230, 2021.
- [78] J. y. T. R. Miller, «"Network Communication Protocols for Service-Oriented Architectures",» *Journal of Network Services*, vol. 22, nº 2, pp. 145-160, 2023.
- [79] P. Davis, «"Facilitating Information Exchange in Distributed Systems",» *International Journal of Information Systems*, vol. 19, nº 1, pp. 75-89, 2020.
- [80] A. Lloyd, «"Core Principles of Enterprise Service Bus for System Integration",» *Journal of Enterprise Architecture*, vol. 18, nº 3, pp. 45-60, 2021.
- [81] S. Martin, «"Key Strategies for Addressing Interoperability Deficiencies in Border Security",» *Journal of Border Management and Security*, vol. 15, nº 2, pp. 85-98, 2020.
- [82] Comisión Europea, *Normas de Ejecución (UE) 2017/884 y 2018/559*, 2017-2018.
- [83] Comisión Europea, *Decisión (UE, Euratom) 2017/46*, 2017.
- [84] Comisión Europea, *Propuestas de reglamentos de interoperabilidad," 2017/0351 y 2017/0352*, 2017, 2017.
- [85] M. L. y. S. C. Katz, «Network Externalities, Competition, and Compatibility,» *American Economic Review*, vol. 75, nº 3, pp. 424-440, 1985.
- [86] A. Smith, *Estrategias de Colaboración en el Entorno Digital*, 2019.
- [87] Supervisor Europea de Protección de Datos, *Opinion 9/2021 on the EU's interoperability strategy for information systems in the field of borders and security*, 2021.
- [88] Unión Europea, *Charter of Fundamental Rights of the European Union*, 2020.
- [89] Union Europea, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, 2016.
- [90] Supervisor Europeo de Protección de Datos, *Opinion 4/2020 on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems*, 2020.
- [91] Parlamento Europeo y Consejo, *Reglamento (UE) 2016/679*, 2016.