Consejo de la Unión Europea

Bruselas, 14 de diciembre de 2017
(OR. en)

15119/17

Expediente interinstitucional: 2017/0351 (COD)

COSI 336	VISA 458
FRONT 507	FAUXDOC 73
ASIM 142	COPEN 419
DAPIX 430	JAI 1212
ENFOPOL 622	CT 164
ENFOCUSTOM 285	CSCI 79
SIRIS 217	SAP 28
SCHENGEN 88	COMIX 840
DATAPROTECT 220	

NOTA DE TRANSMISIÓN

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	12 de diciembre de 2017
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2017) 793 final
Asunto:	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (fronteras y visados) y por el que se modifican la Decisión 2004/512/CE del Consejo, el Reglamento (CE) n.º 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226

Adjunto se remite a las Delegaciones el documento – COM(2017) 793 final.

Adj.: COM(2017) 793 final

COMISIÓN
EUROPEA

Estrasburgo, 12.12.2017
COM(2017) 793 final

2017/0351 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (fronteras y visados) y por el que se modifican la Decisión 2004/512/CE del Consejo, el Reglamento (CE) n.º 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226

{SWD(2017) 473 final} - {SWD(2017) 474 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Antecedentes de la propuesta

En los tres últimos años, la Unión Europea ha experimentado un aumento de los cruces irregulares de fronteras y una amenaza continua y en auge a la seguridad interior, como ha quedado demostrado por una serie de atentados terroristas. Los ciudadanos de la UE esperan que los controles de personas en las fronteras exteriores y en el espacio Schengen sean eficaces, para que permitan una gestión eficiente de la migración y contribuyan a la seguridad interior. Estos retos han puesto abruptamente de relieve la necesidad urgente de aunar y reforzar de manera global las herramientas de información de la UE para la gestión de las fronteras, la migración y la seguridad.

La gestión de la información de la UE puede y debe ser más eficiente y eficaz, en el pleno respeto de los derechos fundamentales, en particular el derecho a la protección de los datos personales, a fin de proteger mejor las fronteras exteriores de la UE, mejorar la gestión de los flujos migratorios y reforzar la seguridad interior, en beneficio de todos los ciudadanos. Existen ya varios sistemas de información a escala de la UE y se están desarrollando otros nuevos para proporcionar información pertinente sobre las personas a la guardia de fronteras y a los agentes de inmigración y de policía. Para que esta ayuda sea eficaz, la información proporcionada por los sistemas de información de la UE debe ser completa, exacta y fiable. Sin embargo, existen deficiencias estructurales en la arquitectura de gestión de la información de la UE. Las autoridades nacionales se enfrentan a un panorama complejo de sistemas de información gestionados de manera diferente. Por otra parte, la arquitectura de gestión de los datos de las fronteras y la seguridad es fragmentaria, ya que la información se almacena por separado en sistemas desconectados, lo que origina zonas de sombra. Como consecuencia de ello, **los distintos sistemas de información a escala de la UE no son interoperables**, es decir, capaces de intercambiar datos y compartir información de modo que las autoridades y los funcionarios competentes dispongan de la información necesaria, cuando y donde la necesiten. La interoperabilidad de los sistemas de información a escala de la UE puede contribuir significativamente a suprimir las actuales zonas de sombra que permiten que cualquier persona, incluidas aquellas que puedan estar implicadas en actividades terroristas, pueda estar registrada en distintas bases de datos, desconectadas entre sí, con diferentes nombres.

En abril de 2016, la Comisión presentó una Comunicación titulada *Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad*[1] con el fin de solucionar una serie de deficiencias estructurales relativas a los sistemas de información[2]. El objetivo de la Comunicación de abril de 2016 era abrir un debate sobre cómo pueden los sistemas de información de la Unión Europea mejorar la gestión de las fronteras, la migración y la seguridad interior. El **Consejo**, por su parte, también reconoció la necesidad urgente de actuar en este ámbito. En junio de 2016, aprobó una **Hoja de ruta para mejorar el intercambio y la gestión de la información**, con inclusión de soluciones de interoperabilidad

[1] COM(2016) 205 de 6 de abril de 2016.

[2] 1) Funcionalidades insuficientes en algunos de los sistemas de información existentes; 2) lagunas de información en la arquitectura de gestión de datos de la UE; 3) un panorama complejo de sistemas de información gestionados de manera diferente y 4) una arquitectura fragmentaria de gestión de datos de las fronteras y la seguridad, porque la información se almacena por separado en sistemas desconectados, lo que origina zonas de sombra.

en el ámbito de la Justicia y los Asuntos de Interior[3]. El objetivo de la Hoja de ruta era apoyar las investigaciones operativas y proporcionar rápidamente a los profesionales de primera línea -agentes de policía, guardas de fronteras, fiscales, funcionarios de inmigración y otros- una información global, actual y de alta calidad para cooperar y actuar de forma eficaz. El **Parlamento Europeo** también instó a actuar en este ámbito. En su Resolución de julio de 2016[4] sobre el programa de trabajo de la Comisión para 2017, solicitó «propuestas para mejorar y desarrollar los sistemas de información existentes, abordar las lagunas de información y avanzar hacia la interoperabilidad, así como propuestas sobre la obligación de intercambiar información a escala de la UE, en conjunción con las salvaguardias necesarias en materia de protección de datos». El discurso del Presidente Juncker sobre el estado de la Unión de septiembre de 2016[5] y las conclusiones del Consejo Europeo de diciembre de 2016[6] destacaron la importancia de superar las deficiencias actuales en la gestión de datos y de mejorar la interoperabilidad de los sistemas de información existentes.

En junio de 2016, como continuación de la Comunicación de abril de 2016, la Comisión creó un **Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad**[7] para abordar los retos jurídicos, técnicos y operativos de la mejora de la interoperabilidad de los sistemas centrales de la UE para las fronteras y la seguridad, incluidas su necesidad, viabilidad técnica, proporcionalidad e incidencia en la protección de datos. El **informe final** del Grupo de Expertos de Alto Nivel, que se publicó en mayo de 2017[8], estableció una serie de recomendaciones destinadas a reforzar y desarrollar los sistemas de información de la UE y su interoperabilidad. La Agencia Europea de los Derechos Fundamentales, el Supervisor Europeo de Protección de Datos y el Coordinador de la lucha contra el terrorismo de la UE participaron activamente en los trabajos del Grupo de Expertos. Cada uno de ellos presentó declaraciones de apoyo, reconociendo al mismo tiempo que las cuestiones más amplias en materia de derechos fundamentales y protección de datos deben tratarse a la vez que se sigue avanzando. Representantes de la Secretaría de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo y de la Secretaría General del Consejo asistieron en calidad de observadores. El Grupo de Expertos de Alto Nivel llegó a la conclusión de que es **necesario y técnicamente viable trabajar en pro de soluciones prácticas de interoperabilidad** y que estas, en principio, pueden ofrecer ventajas operativas y ser conformes a los requisitos de protección de datos.

Sobre la base del informe y las recomendaciones del grupo de expertos, la Comisión expuso, en su *Séptimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva*[9], un **nuevo enfoque para la gestión de los datos** de las fronteras, la seguridad y la migración en el que todos los sistemas centralizados de información de la UE para la gestión de la seguridad, las fronteras y la migración sean interoperables, con pleno respeto de los derechos fundamentales. La Comisión anunció su intención de seguir trabajando para crear un portal

---

3 Hoja de ruta de 6 de junio de 2016 para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior (9368/1/16 REV 1).

4 Resolución del Parlamento Europeo, de 6 de julio de 2016, sobre las prioridades estratégicas para el programa de trabajo de la Comisión para 2017 [2016/2773 (RSP)].

5 Estado de la Unión en 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_es.

6 Conclusiones del Consejo Europeo (15.12.2016), http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

7 Decisión de la Comisión, de 17 de junio de 2016, por la que se crea el Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad (2016/C 257/03).

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

europeo de búsqueda que consulte simultáneamente todos los sistemas de la UE pertinentes en materia de gestión de la seguridad, las fronteras y la migración, al que posiblemente se apliquen normas racionalizadas para el acceso de los cuerpos policiales, y de desarrollar para estos sistemas un servicio de correspondencia biométrica compartido (posiblemente con una funcionalidad de aviso de respuesta positiva[10]) y un registro común de datos de identidad. Comunicó asimismo su intención de presentar, lo antes posible, una propuesta legislativa relativa a la interoperabilidad.

Las conclusiones del Consejo Europeo de junio de 2017[11] reiteraron la necesidad de actuar. Basándose en las conclusiones del Consejo de Justicia y Asuntos de Interior de junio de 2017[12], el Consejo Europeo invitó a la Comisión a presentarle, lo antes posible, un proyecto de legislación que promulgase las recomendaciones formuladas por el Grupo de Expertos de Alto Nivel. Esta iniciativa responde también a la petición del Consejo de un marco exhaustivo para el acceso de los cuerpos policiales a las distintas bases de datos en el ámbito de la justicia y los asuntos de interior, con vistas a una mayor racionalización, coherencia, eficacia y atención a las necesidades operativas[13]. A fin de intensificar los esfuerzos para hacer de la Unión Europea una sociedad más segura, respetando plenamente los derechos fundamentales, la Comisión anunció, en el marco de su Programa de Trabajo para 2018[14], una propuesta sobre la interoperabilidad de los sistemas de información que debía presentarse a finales de 2017.

- **Objetivos de la propuesta**

Los objetivos generales de esta iniciativa se derivan de los del Tratado de mejorar la gestión de las fronteras exteriores del espacio Schengen y contribuir a la seguridad interior de la Unión Europea. Asimismo, se fundan en las decisiones políticas de la Comisión y las conclusiones pertinentes del Consejo (Europeo). Estos objetivos se detallan en la Agenda Europea de Migración y las comunicaciones posteriores, incluida la Comunicación sobre la protección y el refuerzo de Schengen[15], la Agenda Europea de Seguridad[16] y los informes de situación relativos a una Unión de la Seguridad genuina y efectiva[17] de la Comisión.

Al mismo tiempo, basándose en particular en la Comunicación de abril de 2016 y en las conclusiones del Grupo de Expertos de Alto Nivel, los objetivos de la presente propuesta están intrínsecamente relacionados con lo anteriormente expuesto.

Los objetivos específicos de la presente propuesta son:

---

[10] Nuevo concepto de protección de la privacidad por el diseño que limita el acceso a la totalidad de los datos, reduciéndolo a una mera notificación de «respuesta positiva/negativa», que indique la presencia (o la ausencia) de los datos.

[11] Conclusiones del Consejo Europeo, 22 y 23 de junio de 2017.

[12] Resultados de la 3546ª reunión del Consejo de Justicia y Asuntos de Interior de 8 y 9 de junio de 2017, 10136/17.

[13] El Comité de Representantes Permanentes del Consejo (Coreper), una vez otorgado el mandato a la Presidencia del Consejo para iniciar las negociaciones interinstitucionales sobre el Sistema de Entradas y Salidas de la UE, con fecha de 2 de marzo de 2017, acordó un proyecto de declaración del Consejo que invitaba a la Comisión a proponer un marco general para el acceso de los cuerpos policiales a las distintas bases de datos en el ámbito de la justicia y los asuntos de interior, con vistas a una mayor racionalización, coherencia, eficacia y atención a las necesidades operativas (acta resumida 7177/17, 21.3.2017).

[14] COM(2017) 650 final.

[15] COM(2017) 570 final.

[16] COM(2015) 185 final.

[17] COM(2016) 230 final.

1) asegurarse de que los usuarios finales, en particular la guardia de fronteras, la policía, los funcionarios de inmigración y las autoridades judiciales, disfruten de un **acceso rápido, ininterrumpido, sistemático y controlado** a la información que necesitan para desempeñar sus tareas;

2) asegurarse de que los usuarios finales, en particular la guardia de fronteras, la policía, los funcionarios de inmigración y las autoridades judiciales, disfruten de un **acceso rápido, ininterrumpido, sistemático y controlado** a la información que necesitan para desempeñar sus tareas;

3) facilitar los **controles de identidad de los nacionales de terceros países**, en el territorio de un Estado miembro, por las autoridades policiales, y

4) facilitar y **racionalizar el acceso de los cuerpos policiales** a los sistemas de información no policiales a escala de la UE, cuando sea necesario con fines de prevención, investigación, detección o enjuiciamiento de delitos graves y de terrorismo.

Además de estos objetivos operativos principales, esta propuesta contribuirá a:

- facilitar la **aplicación** técnica y operativa **por parte de los Estados miembros** de los sistemas de información existentes y futuros;
- reforzar y racionalizar las **condiciones de seguridad y protección de datos** que rigen los sistemas respectivos, y
- mejorar y armonizar los requisitos de **calidad de los datos** de los respectivos sistemas.

Por último, la presente propuesta incluye disposiciones para la creación y gobernanza del formato universal de mensajes (UMF), como una norma de la UE para el desarrollo de sistemas de información en el ámbito de la justicia y los asuntos de interior, y para la creación de un repositorio central para la presentación de informes y estadísticas.

- **Ámbito de aplicación de la propuesta**

Junto con su propuesta hermana, presentada el mismo día, la presente propuesta de interoperabilidad se centra en los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración administrados a nivel central, tres de ellos ya existentes, uno en vías de desarrollo y otros dos en la fase de propuestas objeto de debate entre los colegisladores. Cada sistema tiene sus propios objetivos, finalidades, bases jurídicas, normas, grupos de usuarios y contexto institucional.

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

- el **Sistema de Información de Schengen (SIS)**, con un amplio espectro de descripciones de personas (denegaciones de entrada o de estancia en la UE, órdenes de detención europeas, personas desaparecidas, procedimientos de asistencia judicial,

controles discretos y específicos) y objetos (incluidos los documentos de identidad o de viaje perdidos, robados o invalidados)[18];

- el sistema **Eurodac**, con los datos dactiloscópicos de los solicitantes de asilo y nacionales de terceros países que han cruzado las fronteras exteriores de forma irregular o que se encuentran en situación ilegal en un Estado miembro, y
- el **Sistema de Información de Visados (VIS)**, con datos sobre los visados para estancias de corta duración.

Además de estos sistemas existentes, la Comisión propuso, en 2016-2017, tres nuevos sistemas centralizados de información de la UE:

- el **Sistema de Entradas y Salidas (SES)**, cuya base jurídica acaba de ser aprobada, que sustituirá al actual sistema de sellado manual de los pasaportes y registrará electrónicamente el nombre, el tipo de documento de viaje, los datos biométricos y la fecha y el lugar de entrada y salida de los nacionales de terceros países que visiten el espacio Schengen para estancias de corta duración;
- el propuesto **Sistema Europeo de Información y Autorización de Viajes (SEIAV)**, que, una vez adoptado, será un sistema en gran medida automatizado que recopilará y verificará la información presentada por los nacionales de terceros países exentos de la obligación de visado antes de su viaje al espacio Schengen, y
- el propuesto **Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (sistema ECRIS-TCN)**, un sistema electrónico de intercambio de información sobre las condenas dictadas contra nacionales de terceros países por los tribunales penales en la UE.

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. Los sistemas 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 estos sistemas de información gestionados de forma centralizada a escala de la UE, el ámbito de aplicación de la presente propuesta incluye también las bases de datos de **Interpol** sobre documentos de viaje robados y perdidos (DVRP), que, de conformidad con las disposiciones del Código de fronteras Schengen, se consulta sistemáticamente en las fronteras exteriores de la UE, y sobre documentos de viaje asociados a notificaciones (TDAWN). Integra asimismo los datos de **Europol**, en la medida en que sean pertinentes para el funcionamiento del sistema SEIAV propuesto y para asistir a los Estados miembros que consulten datos relativos a la delincuencia grave y el terrorismo.

Los sistemas de información nacionales y los sistemas de información de la UE descentralizados quedan fuera del ámbito de aplicación de la presente iniciativa. Siempre que se demuestre la necesidad, sistemas descentralizados como los administrados en el marco de Prüm[19], la Directiva relativa al registro de nombres de los pasajeros (PNR)[20] y la Directiva

[18] Los proyectos de Reglamento de la Comisión, de diciembre de 2016, sobre el SIS proponen su prórroga a fin de incluir las decisiones de retorno y las investigaciones.

[19] http://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.

[20] http://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1508936384641&uri=CELEX:32016L06 81.

relativa a la información anticipada sobre los pasajeros[21] podrán conectarse en una fase posterior a uno o más de los componentes propuestos en el marco de esta iniciativa[22].

Por lo que respecta a la distinción entre los elementos que constituyen un desarrollo del acervo de Schengen en materia de fronteras y visados, por una parte, y los demás sistemas que afectan al acervo de Schengen en materia de cooperación policial o no están relacionados con el acervo de Schengen, por otra, la presente propuesta regula el acceso al Sistema de Información de Visados, el Sistema de Información de Schengen actualmente regulado por el Reglamento (CE) n.º 1987/2006, el Sistema de Entradas y Salidas y el Sistema Europeo de Información y Autorización de Viajes.

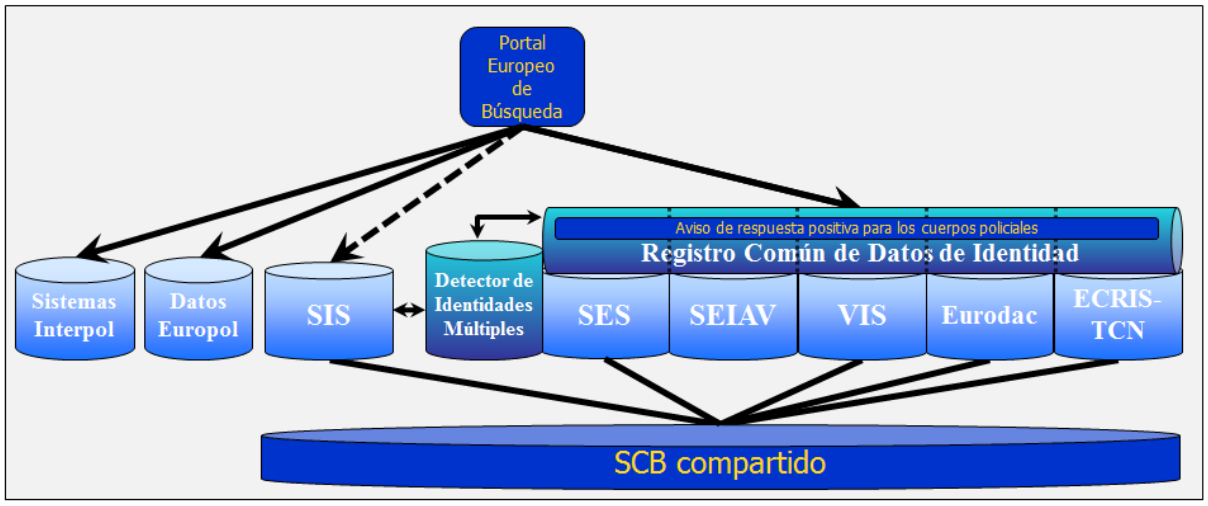
- **Componentes técnicos necesarios para lograr la interoperabilidad**

A fin de alcanzar los objetivos de la presente propuesta, deberán crearse cuatro componentes de interoperabilidad:

- Portal europeo de búsqueda - PEB
- Servicio de correspondencia biométrica compartido - SCB compartido
- Registro común de datos de identidad - RCDI
- Detector de identidades múltiples - DIM

Cada uno de estos componentes se describe detalladamente en el documento de trabajo de los servicios de la Comisión sobre la evaluación de impacto que acompaña a la presente propuesta.

Los cuatro componentes de interoperabilidad conducen a la siguiente solución:



Los objetivos y el funcionamiento de estos cuatro componentes pueden resumirse como sigue:

1) El **portal europeo de búsqueda (PEB)** es el componente que permitiría la búsqueda simultánea en múltiples sistemas (SIS Central, Eurodac, VIS, el futuro SES y los

[21] Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

[22] Del mismo modo por lo que se refiere a los sistemas aduaneros, el Consejo, en sus conclusiones de junio de 2017, invitó a la Comisión a emprender un estudio de viabilidad para seguir explorando los aspectos legales, operativos y técnicos de la interoperabilidad de los sistemas de seguridad y gestión de fronteras con los sistemas de gestión aduanera, y a presentar sus conclusiones para su examen por el Consejo a más tardar a finales de 2018.

propuestos SEIAV y ECRIS-TCN, así como los correspondientes sistemas de Interpol y datos de Europol) utilizando datos de identidad (biográficos y biométricos). Aseguraría a los usuarios de los sistemas de información de la UE un acceso rápido, ininterrumpido, eficiente, sistemático y controlado a toda la información que necesiten para desempeñar sus tareas.

Una consulta a través del portal europeo de búsqueda proporcionaría inmediatamente, en cuestión de segundos, información de los diversos sistemas a los que el usuario tenga acceso legal. Según la finalidad de la consulta y los derechos de acceso correspondientes, el PEB estaría dotado de configuraciones específicas.

El PEB no realiza ningún tratamiento de nuevos datos ni almacena ningún dato; actuaría como ventanilla única o «intermediario de mensajes» para consultar varios sistemas centrales y obtener la información necesaria sin solución de continuidad, y ello en el pleno respeto de las normas de protección de datos y de control del acceso a los sistemas subyacentes. El PEB facilitaría el uso autorizado y correcto de cada uno de los sistemas de información de la UE existentes, y haría más sencilla y barata para los Estados miembros la consulta y utilización de los sistemas, en consonancia con los instrumentos jurídicos que los rigen.

2) El **servicio de correspondencia biométrica compartido (SCB compartido)** permitiría la consulta y la comparación de datos biométricos (impresiones dactilares e imágenes faciales) de varios sistemas centrales (en particular, el SIS, el VIS, Eurodac, el SES y el propuesto ECRIS-TCN). El propuesto SEIAV no contendrá datos biométricos, por lo que no estaría vinculado al SCB compartido.

Como cada uno de los sistemas centrales (SIS, Eurodac, VIS) dispone actualmente de un motor de búsqueda de datos biométricos[23] específico propio, un servicio de correspondencia biométrica compartido proporcionaría una plataforma común en la que los datos se consultarían y compararían simultáneamente. El SCB compartido generaría importantes beneficios en términos de seguridad, costes, mantenimiento y funcionamiento al basarse en un único componente tecnológico en lugar de cinco diferentes. Los datos biométricos (impresiones dactilares e imágenes faciales) se conservarían exclusivamente en los sistemas subyacentes. El SCB compartido crearía y conservaría una representación matemática de las muestras biométricas (una plantilla), pero se desprendería de los datos reales, que seguirían, por lo tanto, almacenándose en un lugar, una sola vez.

El SCB compartido sería una ayuda fundamental para detectar conexiones entre conjuntos de datos y las diferentes identidades asumidas por una misma persona en distintos sistemas centrales. Sin un SCB compartido, ninguno de los otros tres componentes podría funcionar.

3) El **registro común de datos de identidad (RCDI)** sería el componente compartido para almacenar los datos de identidad biográficos[24] y biométricos de los nacionales de terceros

[23] Estos motores de búsqueda de datos biométricos se denominan técnicamente sistemas automáticos de identificación dactilar (SAID) o sistemas de identificación biométrica automática (SIBA).

[24] Los datos biográficos que figuran en el documento de viaje incluyen: apellidos, nombre, sexo, fecha de nacimiento y número de documento de viaje. No se incluyen las direcciones, nombres anteriores, datos biométricos, etc.

países registrados en Eurodac, el VIS, el futuro SES y los propuestos SEIAV y ECRIS-TCN. Cada uno de estos cinco sistemas centrales registra o registrará los datos biográficos de personas concretas por motivos específicos. Esto no cambiaría. Los datos de identidad pertinentes se almacenarían en el RCDI, pero seguirían «perteneciendo» a los respectivos sistemas subyacentes que hubieran registrado estos datos.

El RCDI no contendría datos del SIS. La compleja arquitectura técnica del SIS, que contiene copias nacionales, copias nacionales parciales y posibles sistemas nacionales de correspondencia de datos biométricos, haría que el RCDI fuera muy complejo, hasta un punto en el que podría no ser técnica ni económicamente viable.

El principal objetivo del RCDI consiste en facilitar la identificación biográfica de los nacionales de terceros países. Ofrecería un aumento de la rapidez de las operaciones, una mejora de la eficacia y economías de escala. La creación del RCDI es necesaria para posibilitar el desarrollo efectivo de los controles de identidad de los nacionales de terceros países, también en el territorio de los Estados miembros. Además, añadiendo una «funcionalidad de aviso de respuesta positiva» al RCDI, sería posible comprobar la presencia (o la ausencia) de datos en cualquiera de los sistemas cubiertos por el RCDI mediante una notificación simple de respuesta positiva/negativa. De esta forma, el RCDI también contribuiría a la racionalización del acceso de los cuerpos policiales a los sistemas de información no policiales, manteniendo al mismo tiempo un elevado nivel de protección de datos (véase la sección sobre el planteamiento en dos fases para el acceso de los cuerpos policiales, a continuación).

De los cinco sistemas que quedarán cubiertos por el RCDI, el futuro SES y los propuestos SEIAV y ECRIS-TCN son los nuevos sistemas que todavía deben desarrollarse. El actual Eurodac no contiene datos biográficos; esta extensión se desarrollará una vez que se haya adoptado la nueva base jurídica de Eurodac. El VIS actual contiene datos biográficos, pero la interacción necesaria entre el futuro SES y el VIS requerirá una mejora del VIS existente. La creación del RCDI, por tanto, llegaría en el debido momento. No implicaría en modo alguno una duplicación de los datos existentes. Técnicamente, el RCDI se desarrollaría sobre la base de la plataforma SES/SEIAV.

4) El **detector de identidades múltiples (DIM)** verificaría si los datos de identidad consultados existen en más de uno de los sistemas conectados. El DIM cubre los sistemas que almacenarían datos de identidad en el RCDI (Eurodac, el VIS, el futuro SES y los propuestos SEIAV y ECRIS-TCN), así como el SIS. El DIM permitiría la detección de identidades múltiples vinculadas con el mismo conjunto de datos biométricos, con la doble finalidad de garantizar la identificación correcta de las personas de buena fe y de luchar contra la usurpación de identidad.

El DIM permitiría establecer que diferentes nombres corresponden a la misma identidad. Se trata de una innovación necesaria para resolver de manera eficaz la usurpación de identidad, que constituye una grave violación de la seguridad. El DIM solo mostraría los registros de identidad biográficos que tengan un vínculo en diferentes sistemas centrales. Estos vínculos se detectarían mediante el servicio de correspondencia biométrica compartido sobre la base de datos biométricos y tendrían que ser confirmados o descartados por la autoridad que hubiera registrado los datos en el sistema de información que haya dado lugar a la creación del vínculo. Para ayudar a los usuarios autorizados del

DIM en esta tarea, el sistema tendría que etiquetar los vínculos identificados en cuatro categorías:

- Vínculo amarillo - identidades biográficas potencialmente diferentes de la misma persona.
- Vínculo blanco - confirmación de que las distintas identidades biográficas pertenecen a la misma persona de buena fe.
- Vínculo verde - confirmación de que diferentes personas de buena fe comparten la misma identidad biográfica.
- Vínculo rojo - sospecha de que una misma persona utiliza ilegalmente distintas identidades biográficas.

La presente propuesta describe los procedimientos que se implantarían para gestionar estas diferentes categorías. La identidad de las personas de buena fe afectadas se aclararía tan rápidamente como fuera posible, convirtiendo el vínculo amarillo en un vínculo verde o blanco confirmado, para garantizar que no sufran molestias innecesarias. En cambio, si la evaluación llevase a la confirmación de un vínculo rojo, o a un cambio de vínculo amarillo a vínculo rojo, sería necesario adoptar las medidas oportunas.

- **Planteamiento en dos fases del acceso de los cuerpos policiales previsto por el registro común de datos de identidad**

La consulta policial constituye un objetivo accesorio o secundario de Eurodac, el VIS, el futuro SES y el propuesto SEIAV. Como consecuencia de ello, la posibilidad de acceder a los datos almacenados en dichos sistemas a efectos policiales es limitada. Los cuerpos policiales solo pueden consultar directamente estos sistemas de información no policiales con fines de prevención, investigación, detección o enjuiciamiento de actos de terrorismo y otros delitos graves. Por otro lado, los sistemas respectivos se rigen por diferentes condiciones de acceso y salvaguardias, y algunas de esas normas podrían aminorar la velocidad del uso legítimo de los sistemas por parte de dichos cuerpos. En términos más generales, el principio de búsqueda previa limita la posibilidad de consultar los sistemas por parte de las autoridades de los Estados miembros a los fines policiales justificados y podría, por tanto, dar lugar a la pérdida de oportunidades para descubrir información necesaria.

En su Comunicación de abril de 2016, la Comisión reconoció la necesidad de optimizar las herramientas existentes a efectos policiales, respetando los requisitos de protección de datos. Esta necesidad fue confirmada y reiterada por los Estados miembros y las agencias competentes en el marco del Grupo de Expertos de Alto Nivel.

A la luz de cuanto precede, mediante la creación del RCDI con una denominada «funcionalidad de aviso de respuesta positiva», la presente propuesta introduce la posibilidad de acceder al SES, el VIS, el SEIAV y Eurodac utilizando un **planteamiento de consulta de datos en dos fases**. Este planteamiento en dos fases no modificaría el hecho de que la

consulta policial es un objetivo puramente accesorio de estos sistemas y, por lo tanto, tiene que cumplir unas normas estrictas de acceso.

En una primera fase, un agente de policía iniciaría una consulta sobre una persona concreta, utilizando los datos de identidad, el documento de viaje o los datos biométricos de esa persona, para comprobar si el RCDI almacena información sobre la persona buscada. Cuando haya información, el funcionario recibirá una **respuesta que indique qué sistema o sistemas de información de la UE contienen datos sobre esa persona** (el **aviso de respuesta positiva**). El funcionario no tendría acceso a los datos contenidos en ninguno de los sistemas subyacentes.

En una segunda fase, el agente podría solicitar el acceso a cada uno de los sistemas que, según las indicaciones, contengan datos, con el fin de obtener el expediente completo de la persona objeto de la consulta, **en consonancia con la normativa vigente y los procedimientos establecidos por cada sistema**. Esta segunda fase de acceso permanecería sujeta a la autorización previa de una autoridad designada, y seguiría exigiendo una identificación de usuario y un registro de acceso específicos.

Este nuevo planteamiento también aportaría un valor añadido a los cuerpos policiales debido a la **existencia de vínculos potenciales** en el DIM. El DIM ayudaría al RCDI a identificar los vínculos existentes, haciendo todavía más precisa la búsqueda. El DIM podría indicar si la persona es **conocida bajo diferentes identidades** en diferentes sistemas de información.

El planteamiento de consulta de datos en dos fases resulta especialmente útil en aquellos casos en que el sospechoso, el autor o la víctima de un delito de terrorismo u otro delito grave **son desconocidos**. En efecto, en estos casos, el RCDI permitiría identificar el sistema de información en el que esté registrada esa persona en una única búsqueda. De este modo, las condiciones dadas de búsquedas previas en las bases de datos nacionales y de una búsqueda previa en el sistema automático de identificación dactilar de otros Estados miembros de conformidad con la Decisión 2008/615/JAI («control Prüm») son redundantes.

El nuevo planteamiento de consulta en dos fases solo **entraría en vigor una vez que los componentes de interoperabilidad necesarios sean plenamente operativos**.

- **Elementos adicionales de la presente propuesta en apoyo de los componentes de interoperabilidad**

1) Además de los componentes mencionados anteriormente, el presente proyecto de Reglamento también incluye la propuesta de crear un **repositorio central para la presentación de informes y estadísticas (RCIE)**. Este repositorio es necesario para la creación y el intercambio de informes con datos estadísticos (anónimos) a efectos políticos, operativos y de calidad de los datos. La práctica actual de recoger datos estadísticos exclusivamente de los sistemas de información individuales es perjudicial para la seguridad de los datos y los resultados, y no permite la correlación de datos entre los diferentes sistemas.

   El RCIE constituiría un repositorio independiente dedicado específicamente a contener estadísticas anónimas extraídas del SIS, el VIS, Eurodac, el futuro SES, los propuestos SEIAV y ECRIS-TCN, el registro común de datos de identidad, el detector de identidades múltiples y el servicio de correspondencia biométrica compartido. El repositorio ofrecería

la posibilidad de un intercambio seguro de informes (regulado por los instrumentos jurídicos respectivos) a los Estados miembros, la Comisión (incluida Eurostat) y las agencias de la UE.

Desarrollar un repositorio central en lugar de distintos repositorios para cada uno de los sistemas reduciría el coste y el esfuerzo de su creación, funcionamiento y mantenimiento. Asimismo, ofrecería un nivel más elevado de seguridad de los datos, al gestionarse el almacenamiento de los datos y el control de acceso en un único repositorio.

2) El presente proyecto de Reglamento propone asimismo establecer el **formato universal de mensajes (UMF)** como la norma que se utilizaría a escala de la UE para la interacción entre múltiples sistemas de forma interoperable, incluidos los sistemas desarrollados y gestionados por eu-LISA. Se fomentaría además el uso de esta norma por Europol e Interpol.

   La norma UMF introduce un lenguaje técnico común y unificado para describir y vincular elementos de datos, en particular los elementos relativos a las personas y los documentos (de viaje). Utilizar la norma UMF al desarrollar nuevos sistemas de información garantiza una integración más fácil y la interoperabilidad con otros sistemas, en particular a los Estados miembros que necesiten crear interfaces para comunicarse con estos nuevos sistemas. A este respecto, el uso obligatorio de la norma UMF al desarrollar nuevos sistemas puede considerarse una condición previa necesaria para la introducción de los componentes de interoperabilidad propuestos en el presente Reglamento.

   A fin de garantizar la plena implantación en toda la UE de la norma UMF, se propone una estructura de gobernanza adecuada. La Comisión sería responsable de establecer y desarrollar la norma UMF, en el marco de un procedimiento de examen con los Estados miembros. También participarían los Estados asociados a Schengen, las agencias de la UE y los organismos internacionales integrados en los proyectos UMF (como eu-LISA, Europol e Interpol). La estructura de gobernanza propuesta es vital para el UMF, a fin de extender y difundir la norma garantizando al mismo tiempo su utilidad y aplicabilidad.

3) El presente proyecto de Reglamento introduce también los conceptos de **mecanismos automáticos de control de calidad de los datos** y de indicadores comunes de calidad, así como la necesidad de que los Estados miembros garanticen el más alto nivel de calidad de los datos a la hora de alimentar y utilizar los sistemas. Si los datos no son de la máxima calidad, puede haber consecuencias no solo para la identificación de las personas buscadas, sino también para los derechos fundamentales de personas inocentes. Unas normas de validación automáticas pueden impedir que los operadores cometan errores, de manera que se solucionen los problemas que pueden surgir como consecuencia de la introducción de datos por operadores humanos. El objetivo sería identificar automáticamente las presentaciones de datos aparentemente incorrectas o incoherentes, a fin de que el Estado miembro de origen pueda verificar los datos y adoptar las medidas correctoras necesarias. Este mecanismo se complementaría con informes periódicos sobre la calidad de los datos, elaborados por eu-LISA.

- **Consecuencias para otros instrumentos jurídicos**

  Junto con su propuesta hermana, el presente proyecto de Reglamento introduce innovaciones que requerirán la modificación de otros instrumentos jurídicos:

- Reglamento (UE) n.º 2016/399 (Código de fronteras Schengen).

- Reglamento (UE) n.º 2017/2226 (Reglamento SES).
- Reglamento (CE) n.º 767/2008 (Reglamento VIS).
- Decisión 2004/512/CE del Consejo (Decisión VIS).
- Decisión 2008/633/JAI del Consejo (Decisión VIS / acceso de los cuerpos policiales).
- [Reglamento SEIAV].
- [Reglamento Eurodac].
- [Reglamentos sobre el SIS].
- [Reglamento ECRIS-TCN, incluidas las disposiciones correspondientes del Reglamento (UE) n.º 2016/1624 (Reglamento de la Guardia Europea de Fronteras y Costas)].
- [Reglamento eu-LISA].

La presente propuesta y su propuesta hermana incluyen disposiciones detalladas de los cambios necesarios en los instrumentos jurídicos que son actualmente textos estables adoptados por los colegisladores: el Código de fronteras Schengen, el Reglamento SES, el Reglamento VIS, la Decisión 2008/633/JAI del Consejo y la Decisión 2004/512/CE del Consejo.

Los demás instrumentos enumerados (Reglamentos SEIAV, Eurodac, sobre el SIS, ECRIS-TCN y eu-LISA) se hallan actualmente en fase de negociación en el Parlamento Europeo y el Consejo. En el caso de estos instrumentos, no es posible introducir las necesarias enmiendas en esta fase. La Comisión presentará las modificaciones de cada uno de estos instrumentos en el plazo de dos semanas a partir de la fecha en que se alcance un acuerdo político sobre los respectivos proyectos de Reglamento.

- **Coherencia con las disposiciones vigentes en la política sectorial**

La presente propuesta se inscribe en el marco del proceso más amplio puesto en marcha por la Comunicación *Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad*, de abril de 2016, y el posterior trabajo del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad. Se persiguen tres objetivos:

a) fortalecer y maximizar los beneficios de los **sistemas de información existentes**;

b) cubrir las lagunas de información mediante el desarrollo de nuevos sistemas de información;

c) aumentar la interoperabilidad entre dichos sistemas.

En relación con el primer objetivo, la Comisión adoptó en diciembre de 2016 propuestas para reforzar el actual Sistema de Información de Schengen (SIS)[25]. En cuanto a Eurodac, tras la propuesta de la Comisión de mayo de 2016[26], se aceleraron las negociaciones para la revisión de la base jurídica. También está en preparación una propuesta de una nueva base jurídica del Sistema de Información de Visados (VIS), que se presentará en el segundo trimestre de 2018.

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.

Por lo que respecta al segundo objetivo, las negociaciones sobre la propuesta de la Comisión de abril de 2016 para establecer un Sistema de Entradas y Salidas (SES)[27] concluyeron a principios de julio de 2017, cuando los colegisladores llegaron a un acuerdo político, confirmado por el Parlamento Europeo en octubre de 2017 y adoptado formalmente por el Consejo en noviembre de 2017. La base jurídica entrará en vigor en diciembre de 2017. Han comenzado las negociaciones sobre la propuesta de noviembre de 2016 para el establecimiento de un Sistema Europeo de Información y Autorización de Viajes (SEIAV)[28] y se espera que concluyan en los próximos meses. En junio de 2017, la Comisión propuso una base jurídica para llenar otro vacío de información: el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)[29]. También en este caso, los colegisladores han indicado que pretenden adoptar rápidamente esta base jurídica.

La presente propuesta aborda el tercer objetivo indicado en la Comunicación de abril de 2016.

- **Coherencia con otras políticas de la Unión en el ámbito de la justicia y los asuntos de interior**

Esta propuesta, junto con su propuesta hermana, responde y está en consonancia con la Agenda Europea de Migración y comunicaciones posteriores, incluida la Comunicación sobre la protección y el refuerzo de Schengen[30], así como la Agenda Europea de Seguridad[31] y los trabajos y los informes de situación hacia una Unión de la Seguridad genuina y efectiva[32] de la Comisión. Es coherente con otras políticas de la Unión, en particular:

- Seguridad interior: la Agenda Europea de Seguridad establece que unas estrictas normas comunes de gestión de las fronteras son esenciales para prevenir la delincuencia y el terrorismo transfronterizos. La presente propuesta contribuye a lograr un alto nivel de seguridad interior al ofrecer los medios para que las autoridades tengan un acceso rápido, ininterrumpido, sistemático y controlado a la información que precisen.
- Asilo: la propuesta incluye Eurodac como uno de los sistemas centrales de la UE cubiertos por la interoperabilidad.
- Gestión de las fronteras exteriores y seguridad: esta propuesta refuerza los sistemas SIS y VIS, que contribuyen al control eficiente de las fronteras exteriores de la Unión, así como el futuro SES y los propuestos SEIAV y ECRIS-TCN.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- **Base jurídica**

La base jurídica principal serán los artículos siguientes del Tratado de Funcionamiento de la Unión Europea: artículo 16, apartado 2; artículo 74 y artículo 77, apartado 2, letras a), b), d) y e).

Con arreglo al artículo 16, apartado 2, la Unión está facultada para adoptar medidas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la UE y por parte de los Estados miembros cuando

[27] COM(2016) 194 final.
[28] COM(2016) 731 final.
[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.
[32] COM(2016) 230 final.

lleven a cabo actividades comprendidas dentro del ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. Con arreglo al artículo 74, el Consejo puede adoptar medidas para garantizar la cooperación administrativa entre los servicios de los Estados miembros en el ámbito de la justicia, la libertad y la seguridad. En virtud del artículo 77, apartado 2, letras a), b), d) y e), el Parlamento Europeo y el Consejo pueden adoptar medidas relativas a, respectivamente, la política común de visados y otros permisos de residencia de corta duración, los controles a las personas que crucen las fronteras exteriores, cualquier medida necesaria para el establecimiento progresivo de un sistema integrado de gestión de las fronteras exteriores y la ausencia de controles de las personas, con independencia de su nacionalidad, cuando crucen las fronteras interiores.

- **Subsidiariedad**

La libertad de circulación dentro de la UE requiere que las fronteras exteriores de la Unión se gestionen de forma eficaz para garantizar la seguridad. Los Estados miembros han acordado, por consiguiente, abordar estos retos de forma colectiva, especialmente mediante el intercambio de información a través de los sistemas centralizados de la UE en el ámbito de la justicia y los asuntos de interior. Este principio ha sido confirmado por las diferentes conclusiones adoptadas por el Consejo Europeo y el Consejo, especialmente a partir de 2015.

La ausencia de controles en las fronteras interiores exige una buena gestión de las fronteras exteriores del espacio Schengen, en el que cada Estado miembro o país asociado a Schengen ha de controlar la frontera exterior en nombre de los demás Estados Schengen. Por consiguiente, ningún Estado miembro puede hacer frente por sí solo y de forma aislada a la migración irregular y la delincuencia transfronteriza. Los nacionales de terceros países que entran en el espacio sin controles en las fronteras interiores pueden viajar libremente dentro de este. En un espacio sin fronteras interiores, las medidas contra la migración irregular y la delincuencia y el terrorismo internacionales, por ejemplo, a través de la detección de la usurpación de identidad, deben emprenderse en común, y solo pueden dar resultado si se abordan a escala de la UE.

Los principales sistemas de información comunes de la UE existen ya o se hallan en fase de implementación. Una mejor interoperabilidad de estos sistemas de información exige una acción a escala de la Unión. El núcleo de la propuesta es la mejora de la eficiencia y el uso de los sistemas centralizados gestionados por eu-LISA. Debido a la escala, los efectos y el impacto de las medidas previstas, los objetivos fundamentales solo pueden alcanzarse de manera eficaz y sistemática a nivel de la UE.

- **Proporcionalidad**

Como se explica en detalle en la evaluación de impacto que acompaña a la presente propuesta de Reglamento, las opciones políticas presentadas se consideran proporcionadas. No van más allá de lo necesario para alcanzar los objetivos acordados.

El **portal europeo de búsqueda (PEB)** es una herramienta necesaria para reforzar el uso autorizado de los sistemas de información de la UE existentes y futuros. El impacto del PEB en términos de tratamiento de datos es muy limitado. No almacenará ningún dato, salvo la información sobre los distintos perfiles de usuario del PEB y los datos y sistemas de información a los que tenga acceso, y conservará un historial de uso por medio de registros. El papel del PEB como intermediario de mensajes, capacitador y facilitador es proporcionado, necesario y limitado en términos de búsquedas y derechos de acceso conforme a los mandatos de las bases jurídicas relativas a los sistemas de información y a la propuesta de Reglamento relativo a la interoperabilidad.

El **servicio de correspondencia biométrica compartido (SCB compartido)** es necesario para el funcionamiento del PEB, el registro común de datos de identidad y el detector de identidades múltiples, y facilita el uso y el mantenimiento de los sistemas de información pertinentes de la UE existentes y futuros. Su funcionalidad permite la realización de búsquedas sobre los datos biométricos en distintas fuentes de manera eficiente, ininterrumpida y sistemática. Los datos biométricos se almacenan y conservan en los sistemas subyacentes. El SCB compartido crea plantillas comunes, pero descartará las imágenes reales. Los datos se almacenarán en un lugar, una sola vez.

El **registro común de datos de identidad (RCDI)** es necesario para alcanzar el objetivo de la identificación correcta de los nacionales de terceros países, por ejemplo, durante un control de identidad en el espacio Schengen. El RCDI también apoya el funcionamiento del detector de identidades múltiples y constituye, por lo tanto, un componente necesario para alcanzar el doble objetivo de facilitar los controles de identidad de los viajeros de buena fe y luchar contra la usurpación de identidad. El acceso al RCDI a tal efecto estará limitado a aquellos usuarios que necesiten esa información para desempeñar sus tareas (lo que exige que dichos controles se conviertan en un nuevo objetivo accesorio de Eurodac, el VIS, el futuro SES y los propuestos SEIAV y ECRIS-TCN). El tratamiento de datos se limita a lo estrictamente necesario para lograr este objetivo, y se establecerán garantías adecuadas de que se respetarán los derechos de acceso y que los datos almacenados en el RCDI serán los mínimos necesarios. Con el fin de garantizar la minimización de los datos y evitar duplicidades injustificadas de datos, el RCDI contendrá los datos biográficos de cada uno de los sistemas subyacentes - almacenados, añadidos, modificados y eliminados de conformidad con sus respectivas bases jurídicas- sin copiarlos. Los plazos de conservación de los datos son plenamente acordes con las disposiciones de conservación de datos de los sistemas de información subyacentes que proporcionan los datos de identidad.

El **detector de identidades múltiples (DIM)** es necesario para ofrecer una solución a la detección de identidades múltiples, con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y de luchar contra la usurpación de identidad. El DIM contendrá los vínculos entre las personas presentes en más de un sistema central de información, limitados estrictamente a los datos necesarios para comprobar si una persona está registrada legal o ilegalmente con diferentes identidades biográficas en diferentes sistemas, pero también para aclarar si dos personas con similares datos biográficos pueden no ser la misma persona. El tratamiento de datos mediante el DIM y el SCB compartido para vincular expedientes individuales a través de sistemas individuales se mantendrá en un mínimo absoluto. El DIM incluirá salvaguardias contra posibles discriminaciones o decisiones desfavorables para las personas con múltiples identidades legales.

- **Elección del instrumento**

Se propone un Reglamento del Parlamento Europeo y del Consejo. La legislación propuesta regula directamente el funcionamiento de los sistemas de información centralizados de la UE para la gestión de las fronteras y la seguridad, todos los cuales han sido, o se propone que sean, creados en virtud de Reglamentos. Asimismo, eu-LISA, que será responsable del diseño y el desarrollo, y a su debido tiempo de la gestión técnica, de los componentes se establece también en virtud de un Reglamento. El Reglamento constituye, pues, el instrumento adecuado.

3. RESULTADOS DE LAS CONSULTAS DE LAS PARTES INTERESADAS Y EVALUACIONES DE IMPACTO

• Consulta pública

Como parte de la preparación de la presente propuesta, la Comisión abrió en julio de 2017 una consulta pública para recabar los puntos de vista de las partes interesadas sobre la interoperabilidad. La consulta recibió dieciocho respuestas de una amplia gama de partes interesadas, incluidos los gobiernos de los Estados miembros, organizaciones del sector privado, otras organizaciones, como ONG y grupos de reflexión, así como de ciudadanos particulares[33]. En general, las respuestas eran favorables a los principios subyacentes de esta propuesta de interoperabilidad. La gran mayoría de los participantes se mostraron de acuerdo en que las cuestiones que la consulta ponía de relieve eran las correctas, y que los objetivos que pretende alcanzar el paquete legislativo en materia de interoperabilidad son acertados. En concreto, los participantes consideraron que las opciones presentadas en el documento de consulta:

- proporcionarían a los agentes sobre el terreno el acceso a la información que necesitan;
- evitarían la duplicación de datos, reducirían los solapamientos y pondrían de manifiesto las discrepancias en los datos;
- identificarían a las personas de forma más fiable, incluidas las personas con múltiples identidades, y reducirían la usurpación de identidad.

Una clara mayoría de participantes se mostró partidaria de cada una de las opciones propuestas, que consideró necesarias para alcanzar los objetivos de la presente iniciativa, subrayando en sus respuestas la necesidad de medidas de protección de datos fuertes y claras, especialmente en lo que se refiere al acceso a la información almacenada en los sistemas y la conservación de los datos, así como la necesidad de contar con datos de alta calidad y actualizados en los sistemas, y con medidas para garantizar esas características.

Todos los puntos mencionados se han tenido en cuenta en la elaboración de la presente propuesta.

• Encuesta Eurobarómetro

En junio de 2017, se llevó a cabo una encuesta del Eurobarómetro especial[34], que mostró que la estrategia de la UE de puesta en común de información a escala de la UE para luchar contra la delincuencia y el terrorismo tiene un amplio respaldo público: casi todos los encuestados (92 %) estuvieron de acuerdo en que las autoridades nacionales deben intercambiar información con las autoridades de otros Estados miembros para luchar mejor contra la delincuencia y el terrorismo.

Una clara mayoría (69 %) de los encuestados expresó la opinión de que la policía y otros cuerpos de seguridad nacionales deben intercambiar información con otros países de la UE de

[33] Para más detalles, véase el informe de síntesis adjunto a la evaluación de impacto.

[34] El *Informe sobre las actitudes de los europeos hacia la seguridad* analiza los resultados de la encuesta de opinión pública del Eurobarómetro especial (464b) en lo que respecta a la concienciación, las experiencias y las percepciones globales de la seguridad por parte de los ciudadanos. La encuesta fue realizada por la red política y social TNS en los 28 Estados miembros entre el 13 y el 26 de junio de 2017. Se entrevistó a 28 093 ciudadanos de la UE pertenecientes a distintos medios sociales y grupos demográficos.

manera sistemática. En todos los Estados miembros, una mayoría de los encuestados cree que la información debería compartirse en todos los casos.

- **Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad**

Como ya se ha indicado en la introducción, la presente propuesta se basa en las recomendaciones del **Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad**[35]. Este grupo fue creado en junio de 2016 con el objetivo de abordar los retos jurídicos, técnicos y operativos de todas las opciones disponibles para lograr la interoperabilidad entre los sistemas centrales de la UE para la gestión de las fronteras y la seguridad. El Grupo adoptó una perspectiva amplia y global sobre la arquitectura de gestión de datos para la gestión de las fronteras y la actuación policial, teniendo en cuenta asimismo las funciones, responsabilidades y sistemas pertinentes de las autoridades aduaneras.

El Grupo estaba compuesto por expertos de los Estados miembros y los países asociados a Schengen, así como de varias agencias de la UE: eu-LISA, Europol, la Oficina Europea de Apoyo al Asilo, la Agencia Europea de la Guardia de Fronteras y Costas y la Agencia Europea de los Derechos Fundamentales. El Coordinador de la lucha contra el terrorismo de la UE y el Supervisor Europeo de Protección de Datos también participaron como miembros de pleno derecho del Grupo de Expertos. Además, representantes de la Secretaría de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo y de la Secretaría General del Consejo asistieron en calidad de observadores.

El **informe final del Grupo de Expertos de Alto Nivel** se publicó en mayo de 2017[36]. En él se subraya la necesidad de actuar para solucionar las deficiencias estructurales indicadas en la Comunicación de abril de 2016. Se propone una serie de recomendaciones destinadas a reforzar y desarrollar la capacidad y la interoperabilidad de los sistemas de información de la UE. La conclusión es que es **necesario y técnicamente viable trabajar en pro del portal europeo de búsqueda, el servicio de correspondencia biométrica compartido y el registro común de datos de identidad como soluciones para la interoperabilidad**, y que estas herramientas, en principio, pueden ofrecer ventajas operativas y cumplir los requisitos sobre protección de datos. El Grupo también recomienda considerar la opción adicional de un planteamiento en dos fases para el acceso de los cuerpos policiales, sobre la base de una funcionalidad de aviso de respuesta positiva.

El presente proyecto de Reglamento responde a las recomendaciones del Grupo de Expertos de Alto Nivel sobre la calidad de los datos, el formato universal de mensajes (UMF) y la creación de un depósito de datos [presentado como el repositorio central para la presentación de informes y estadísticas (RCIE)].

El cuarto componente de interoperabilidad propuesto en el presente proyecto de Reglamento (el detector de identidades múltiples) no fue propuesto por el Grupo de Expertos de Alto Nivel, pero surgió en el curso de los análisis técnicos adicionales y la evaluación de la proporcionalidad llevados a cabo por la Comisión.

[35] Decisión de la Comisión, de 17 de junio de 2016, por la que se crea el Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad (2016/C 257/03).

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

- **Estudios técnicos**

Se encargaron tres estudios en apoyo a la preparación de la propuesta. Contratada por la Comisión, Unisys emitió un informe sobre un estudio de viabilidad del portal de búsqueda europeo. A su vez, eu-LISA encargó un informe técnico a Gartner (junto con Unisys) para apoyar el desarrollo del servicio de correspondencia biométrica compartido. PwC entregó a la Comisión un informe técnico sobre un registro común de datos de identidad.

• Evaluación de impacto

La presente propuesta está acompañada de una evaluación de impacto, que se presenta en el documento de trabajo de los servicios de la Comisión adjunto [SWD(2017) 473].

El Comité de Control Reglamentario revisó el proyecto de evaluación de impacto en su reunión de 6 de diciembre de 2017 y emitió su dictamen (positivo con reservas) el 8 de diciembre, en el que indicaba que la evaluación de impacto deberá ajustarse para integrar las recomendaciones del Comité sobre aspectos específicos. Dichos ajustes se refieren, en primer lugar, a la adopción de medidas adicionales en el marco de la opción preferida de racionalización de los derechos de acceso de los usuarios finales a los datos existentes en los sistemas de información de la UE, así como a la explicitación de las garantías conexas en materia de protección de datos y derechos fundamentales. La segunda consideración principal consistía en aclarar la integración del Sistema de Información de Schengen en la opción 2, incluidos los aspectos de eficacia y costes para facilitar su comparación con la opción preferida 3. La Comisión actualizó su evaluación de impacto para responder a estas consideraciones principales y dar respuesta a una serie de observaciones formuladas por el Comité.

En la evaluación de impacto se valora si y cómo podría alcanzarse cada uno de los objetivos utilizando uno o varios de los componentes técnicos identificados por el Grupo de Expertos de Alto Nivel y a través de posteriores análisis. En su caso, también se estudian las subopciones necesarias para alcanzar estos objetivos, respetando siempre el marco de protección de datos. La evaluación de impacto concluye que:

- Para cumplir el objetivo de proporcionar a los usuarios autorizados un acceso rápido, ininterrumpido, sistemático y controlado a los sistemas de información pertinentes, debe crearse un portal europeo de búsqueda (PEB) a partir de un servicio de correspondencia biométrica compartido (SCB compartido) para acceder a todas las bases de datos.
- Para cumplir el objetivo de facilitar los controles de identidad de los nacionales de terceros países, en el territorio de un Estado miembro, por funcionarios autorizados, debe crearse un registro común de datos de identidad (RCDI), con el conjunto mínimo de datos de identificación, sobre la base también del SCB compartido.
- Para cumplir el objetivo de detectar identidades múltiples vinculadas con el mismo conjunto de datos biométricos, con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y de luchar contra la usurpación de identidad, debe crearse un detector de identidades múltiples (DIM), con vínculos entre múltiples identidades entre los distintos sistemas.
- Para cumplir el objetivo de facilitar y racionalizar el acceso de los cuerpos policiales a los sistemas de información no policiales, con el fin de prevenir, investigar, detectar o enjuiciar delitos graves y de terrorismo, debe incluirse en el RCDI la funcionalidad de «aviso de respuesta positiva».

Dado que todos los objetivos deben cumplirse, la **solución completa es la combinación de PEB, RCDI (con aviso de respuesta positiva) y DIM, basados todos ellos en el SCB compartido**.

El impacto positivo principal será una mejora de la gestión de las fronteras y un aumento de la seguridad interior en el seno de la Unión Europea. Los nuevos componentes racionalizarán y acelerarán el acceso de las autoridades nacionales a la información necesaria y la identificación de los nacionales de terceros países. Permitirán a las autoridades establecer vínculos cruzados con la información necesaria, ya existente, sobre las personas durante los controles fronterizos a efectos de las solicitudes de asilo o de visado, así como para la labor policial. Darán acceso a información que pueda respaldar decisiones fiables, bien relativas a la investigación de delitos graves y de terrorismo o bien en el ámbito de la migración y el asilo. Aunque no afectan directamente a los ciudadanos de la UE (las medidas propuestas atañen principalmente a los nacionales de terceros países cuyos datos estén registrados en un sistema de información centralizado a escala de la UE), se espera que las propuestas generen una mayor confianza pública, garantizando que su diseño y utilización aumenten la seguridad de los ciudadanos de la UE.

El impacto económico y financiero inmediato de la propuesta se limitará al diseño, el desarrollo y el funcionamiento de las nuevas herramientas. Los gastos se imputarán al presupuesto de la UE y a las autoridades de los Estados miembros que administren los sistemas. La repercusión en el turismo será positiva, ya que las medidas propuestas mejorarán la seguridad de la Unión Europea y deberían acelerar también los controles fronterizos. Del mismo modo, se espera que el impacto sobre los aeropuertos, los puertos marítimos y los transportistas sea positivo, debido, en particular, a la aceleración de los controles fronterizos.

- **Derechos fundamentales**

La evaluación de impacto examina, en particular, el impacto de las medidas propuestas sobre los derechos fundamentales, en particular el derecho a la protección de datos.

De conformidad con la Carta de los Derechos Fundamentales de la UE, que las instituciones de la Unión y los Estados miembros deben observar cuando aplican el Derecho de la Unión (artículo 51, apartado 1, de la Carta), las oportunidades que brinda la interoperabilidad como medida para mejorar la seguridad y la protección de las fronteras exteriores deben conciliarse con la obligación de garantizar que las interferencias con los derechos fundamentales que pudieran derivarse del nuevo entorno de interoperabilidad se limiten a lo estrictamente necesario para alcanzar realmente los objetivos de interés general perseguidos, respetando el principio de proporcionalidad (artículo 52, apartado 1, de la Carta).

Las soluciones de interoperabilidad propuestas son componentes complementarios de los sistemas existentes. Como tales, no alterarían el equilibrio ya garantizado por cada uno de los sistemas centrales existentes en cuanto a su impacto positivo en los derechos fundamentales.

No obstante, la interoperabilidad puede tener una incidencia indirecta adicional en varios derechos fundamentales. En efecto, la identificación correcta de una persona tiene un impacto positivo en el derecho al respeto de la vida privada, y en particular el derecho a la identidad (artículo 7 de la Carta), ya que puede contribuir a evitar confusiones de identidad. Por otra parte, la realización de controles basados en datos biométricos puede percibirse como una interferencia con el derecho de la persona a la dignidad humana, en particular, si esos controles se perciben como humillantes (artículo 1). Sin embargo, en una encuesta[37] realizada

[37] *Encuesta de la FRA en el marco del proyecto piloto sobre fronteras inteligentes de eu-LISA - opiniones y experiencias de los viajeros sobre «fronteras inteligentes»,* Informe de la Agencia de Derechos

por la Agencia de los Derechos Fundamentales de la UE, se preguntó concretamente a los encuestados si creían que el conocimiento de sus datos biométricos en el contexto del control de fronteras podría resultar humillante: la mayoría de los encuestados consideró que no lo sería.

Los componentes de interoperabilidad propuestos ofrecen la oportunidad de adoptar medidas preventivas destinadas a mejorar la seguridad. De este modo, pueden contribuir a la protección del derecho de las personas a la vida (artículo 2 de la Carta), lo que también implica una obligación positiva de las autoridades de adoptar medidas operativas preventivas para proteger a las personas cuyas vidas corran peligro, si supieran o debieran haber sabido de la existencia de un riesgo inminente[38], así como para mantener la efectividad de la prohibición de la esclavitud y del trabajo forzado (artículo 5). Mediante una identificación fiable, más accesible y más fácil, la interoperabilidad puede ayudar a detectar niños desaparecidos o niños objeto de la trata de seres humanos, y facilitar respuestas rápidas y certeras.

Una identificación fiable, más accesible y más fácil podría contribuir también a garantizar que se respeten realmente el derecho de asilo (artículo 18 de la Carta) y el principio de no devolución (artículo 19 de la Carta). La interoperabilidad podría evitar situaciones en las que los solicitantes de asilo sean detenidos ilegalmente, internados y expulsados de forma indebida. Además, gracias a la interoperabilidad, la usurpación de identidad se determinará más fácilmente. También reduciría la necesidad de compartir datos e información sobre los solicitantes de asilo con terceros países (especialmente los países de origen) con el fin de establecer la identidad de la persona y de obtener documentos de viaje, lo que podría poner en peligro al interesado.

- **Protección de datos de carácter personal**

Dada la utilización de datos personales que conlleva, la interoperabilidad tendrá un impacto particular en el derecho a la protección de los datos personales. Este derecho se establece en el artículo 8 de la Carta, el artículo 16 del Tratado de Funcionamiento de la Unión Europea y el artículo 8 del Convenio Europeo de Derechos Humanos. Tal y como subraya el Tribunal de Justicia de la Unión Europea[39], el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad[40]. La protección de datos está estrechamente ligada al respeto de la vida privada y familiar, protegido por el artículo 7 de la Carta.

De conformidad con el Reglamento general de protección de datos[41], la libre circulación de datos dentro de la UE no se restringirá por causa de la protección de datos. Sin embargo, debe observarse una serie de principios. En efecto, para ser legal, cualquier limitación del ejercicio

---

Fundamentales de la UE: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

38 Tribunal Europeo de Derechos Humanos, Osman/Reino Unido, n.º 87/1997/871/1083, 28 de octubre de 1998, apartado 116.

39 Tribunal de Justicia de la Unión Europea, sentencia de 9.11.2010, asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke y Eifert, Rec. 2010, I-0000.

40 En consonancia con el artículo 52, apartado 1, de la Carta, pueden imponerse limitaciones al ejercicio del derecho a la protección de datos, siempre que esas limitaciones se dispongan por ley, respeten el contenido esencial de los derechos y libertades, y, respetando el principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

41 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

de los derechos fundamentales protegidos por la Carta debe cumplir los siguientes criterios, establecidos en el artículo 52, apartado 1:

- debe ser establecida por la ley;
- debe respetar el contenido esencial de los derechos;
- debe responder efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás;
- debe ser necesaria y
- debe ser proporcional.

La presente propuesta integra todas estas normas de protección de datos, como se expone en detalle en la evaluación de impacto que acompaña a la presente propuesta de Reglamento. La propuesta se basa en los principios de protección de datos desde el diseño y por defecto. Incluye todas las disposiciones apropiadas que limitan el tratamiento de datos a lo necesario para el propósito específico y conceden acceso a los datos únicamente a aquellas entidades que «necesitan saber». Los plazos de conservación de datos (en su caso) son adecuados y limitados. El acceso a los datos está reservado exclusivamente al personal debidamente autorizado de las administraciones de los Estados miembros o de los organismos de la UE competentes para los fines específicos de cada sistema de información, y se limita a la medida en que los datos sean necesarios para el desempeño de las tareas conformes a dichos fines.

4. REPERCUSIONES PRESUPUESTARIAS

Las repercusiones presupuestarias figuran en la ficha financiera adjunta, que cubre el tiempo restante del actual marco financiero plurianual (hasta 2020) y los siete años del siguiente marco (2021-2027). El presupuesto propuesto para 2021 y los años siguientes se incluye a efectos ilustrativos y no prejuzga el próximo marco financiero plurianual.

La puesta en práctica de esta propuesta requerirá asignaciones presupuestarias para:

1) El **desarrollo** y la integración por parte de eu-LISA de los cuatro componentes de interoperabilidad y el repositorio central para la presentación de informes y estadísticas, y su posterior **mantenimiento y funcionamiento**.

2) La **migración de datos** al servicio de correspondencia biométrica compartido (SCB compartido) y el registro común de datos de identidad (RCDI). En el caso del SCB compartido, las plantillas biométricas de los datos correspondientes a los tres sistemas que utilizan actualmente la biometría (el SIS, el VIS y Eurodac) deben ser reelaboradas en el SCB compartido. En el caso del RCDI, los datos personales del VIS deben migrarse al RCDI, y los posibles vínculos entre identidades hallados en el SIS, el VIS y Eurodac deberán validarse. Este último proceso, en particular, requiere una gran cantidad de recursos.

3) La actualización por parte de eu-LISA de la **interfaz nacional uniforme** (INU) ya incluida en el Reglamento SES para convertirla en un componente genérico que permita el intercambio de mensajes entre los Estados miembros y el sistema o los sistemas centrales.

4) La **integración de los sistemas nacionales de los Estados miembros** con la INU, que transmitirá los mensajes intercambiados con el RCDI/detector de identidades múltiples a través del portal europeo de búsqueda.

5) La **formación** sobre el uso de los componentes de interoperabilidad por los usuarios finales, también a través de la Agencia de la Unión Europea para la Formación Policial (CEPOL).

Los componentes de interoperabilidad se construirán y mantendrán como programa. Mientras que el portal europeo de búsqueda (PEB) y el detector de identidades múltiples son componentes completamente nuevos, al igual que el repositorio central para la presentación de informes y estadísticas (RCIE), el SCB compartido y el RCDI son componentes comunes que combinan los datos existentes (o que existirán) en sistemas existentes o nuevos con sus actuales previsiones presupuestarias.

El **PEB** aplicará interfaces actuales y conocidas al SIS, el VIS y Eurodac, y se extenderá, a su debido tiempo, a nuevos sistemas.

El PEB será utilizado por los Estados miembros y las agencias sirviéndose de una interfaz basada en el formato universal de mensajes (UMF). Esta nueva interfaz requerirá cambios, adaptaciones, integraciones y pruebas por parte de los Estados miembros, eu-LISA, Europol y la Agencia Europea de la Guardia de Fronteras y Costas. El PEB utilizaría los conceptos de la interfaz nacional uniforme (INU) introducida para el SES, lo que reduciría los esfuerzos de integración.

El PEB supondrá un coste adicional para Europol, con el fin de que la interfaz QUEST pueda usarse con el nivel de protección básico (NPB) de datos.

La base del **SCB compartido** se establecerá de hecho con la creación del nuevo SES, puesto que este constituye, con mucho, el mayor volumen de nuevos datos biométricos. El presupuesto requerido se ha reservado en el marco del instrumento jurídico del SES. Añadir otros datos biométricos del SIS, el VIS y Eurodac al SCB compartido generará un coste adicional relacionado principalmente con la migración de los datos existentes. Se estima en 10 millones EUR para los tres sistemas. La adición de los nuevos datos biométricos del sistema ECRIS-TCN propuesto representa unos costes adicionales limitados, que pueden cubrirse con los fondos reservados en el marco del instrumento jurídico propuesto ECRIS-TCN para establecer un sistema informatizado ECRIS-TCN de identificación de impresiones dactilares.

El **registro común de datos de identidad** se establecerá con la creación del futuro SES y se ampliará aún más con el desarrollo del SEIAV propuesto. El almacenamiento y los motores de búsqueda de estos datos se incluyeron en el presupuesto reservado para los instrumentos jurídicos del futuro SES y el SEIAV propuesto. Añadir nuevos datos biográficos de Eurodac y del ECRIS-TCN propuesto representa un coste adicional menor que ya estaba contemplado en el marco de los instrumentos jurídicos de Eurodac y el ECRIS-TCN propuesto.

El presupuesto total para nueve años (2019-2027) asciende a 424,7 millones EUR, que cubren los siguientes elementos:

1) Un presupuesto de 225 millones EUR para eu-LISA que cubre el coste total de ejecución del programa de desarrollo de los cinco componentes de interoperabilidad (68,3 millones EUR), el coste de mantenimiento desde el momento en que entren en funcionamiento los componentes hasta 2027 (56,1 millones EUR), un presupuesto específico de 25 millones EUR para la migración de los datos de los sistemas existentes al SCB compartido y los costes adicionales de actualización de la INU, redes, formación y reuniones. Un presupuesto específico de 18,7 millones EUR cubre el coste de actualización y funcionamiento de ECRIS-TCN en régimen de alta disponibilidad desde 2022.

2) Un presupuesto de 136,3 millones EUR para que los Estados miembros financien los cambios en sus sistemas nacionales con el fin de utilizar los componentes de

interoperabilidad, la INU desarrollada por eu-LISA y la formación de la comunidad de usuarios finales.

3) Un presupuesto de 48,9 millones EUR para financiar la mejora de los sistemas informáticos de Europol con el fin de adecuarlos al volumen de mensajes que deberán tratar y mejorar su rendimiento[42]. Los componentes de interoperabilidad serán utilizados por el SEIAV con el fin de consultar los datos de Europol.

4) Un presupuesto de 4,8 millones EUR para la Agencia Europea de la Guardia de Fronteras y Costas, para acoger a un equipo de especialistas que, durante un año, validarán los vínculos entre identidades en el momento en que el detector de identidades múltiples entre en funcionamiento.

5) Un presupuesto de 2,0 millones EUR para la Agencia de la Unión Europea para la Formación Policial (CEPOL) para la preparación y la impartición de formación al personal operativo.

6) Una provisión de 7,7 millones EUR para la DG HOME para cubrir un aumento limitado del personal y de los costes conexos durante el periodo de desarrollo de los diversos componentes, puesto que la Comisión también tendrá que desempeñar tareas adicionales durante dicho periodo y asumirá la responsabilidad del comité que se ocupe del formato universal de mensajes.

El Reglamento del Fondo de Seguridad Interior (FSI) Fronteras es el instrumento financiero en el que se ha incluido el presupuesto para la ejecución de la iniciativa de interoperabilidad. El artículo 5, letra b), dispone que 791 millones EUR se destinarán a un programa de desarrollo de sistemas informáticos basados en los sistemas informáticos existentes y nuevos en apoyo a la gestión de los flujos migratorios en las fronteras exteriores, a reserva de la adopción de los actos legislativos de la Unión pertinentes y con arreglo a las condiciones establecidas en el artículo 15, apartado 5. De esos 791 millones EUR, 480,2 millones EUR están reservados para el desarrollo del SES, 210 millones EUR para el SEIAV y 67,9 millones EUR para la revisión del SIS. El resto (32,9 millones EUR) se reasignará utilizando los mecanismos FSI-F. La propuesta actual requiere 32,1 millones EUR para el periodo del actual marco financiero plurianual (2019/20), que se pueden cubrir, por lo tanto, con el saldo presupuestario.

5. INFORMACIÓN ADICIONAL

- **Planes de ejecución y modalidades de seguimiento, valoración e información**

La agencia eu-LISA es responsable de la gestión operativa de los sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia. En calidad de tal, ya es responsable del funcionamiento y las mejoras técnicas y operativas de los sistemas existentes, así como del desarrollo de los futuros sistemas ya previstos. Con arreglo a la presente propuesta de Reglamento, definirá el diseño de la arquitectura física de los componentes de interoperabilidad, su desarrollo y su implementación, y finalmente los alojará. Los respectivos componentes se aplicarán de manera progresiva, según se desarrollen los sistemas subyacentes.

[42] La actual capacidad de tratamiento de información de Europol no es conforme con los importantes volúmenes (media de 100 000 consultas al día) y la reducción del tiempo de respuesta que exigirá el SEIAV.

La Comisión velará por que se establezcan sistemas para supervisar el desarrollo y el funcionamiento de los cuatro componentes (portal europeo de búsqueda, servicio de correspondencia biométrica compartido, registro común de datos de identidad y detector de identidades múltiples) y del repositorio central para la presentación de informes y estadísticas, y los valorará en relación con los principales objetivos estratégicos. Cuatro años después de la puesta en marcha de las funcionalidades, y posteriormente cada cuatro años, eu-LISA presentará al Parlamento Europeo, al Consejo y a la Comisión un informe sobre el funcionamiento técnico de los componentes de interoperabilidad. Además, cinco años después de la puesta en marcha de las funcionalidades, y posteriormente cada cuatro años, la Comisión realizará una valoración global de los componentes, incluido su propio impacto directo o indirecto y el de su aplicación sobre los derechos fundamentales. Deberá examinar los resultados en comparación con los objetivos y evaluar la vigencia de la validez de los fundamentos del sistema y las posibles consecuencias de futuras opciones. La Comisión presentará los informes de valoración al Parlamento Europeo y al Consejo.

- **Explicación detallada de las disposiciones específicas de la propuesta**

El capítulo I establece las disposiciones generales del presente Reglamento. Explica los principios en que se basa el Reglamento; los componentes que crea; los objetivos que pretende alcanzar la interoperabilidad; el ámbito de aplicación del presente Reglamento; las definiciones de los términos utilizados en el presente Reglamento y el principio de no discriminación por lo que se refiere al tratamiento de datos en virtud del presente Reglamento.

El capítulo II establece las disposiciones que regulan el portal europeo de búsqueda (PEB). Este capítulo dispone la creación del PEB y su arquitectura técnica, que desarrollará eu-LISA. Especifica el objetivo del PEB y determina quiénes pueden utilizarlo y el modo de utilización, de conformidad con los derechos de acceso existentes para cada uno de los sistemas centrales. Incluye una disposición por la que eu-LISA puede crear perfiles de usuario para cada categoría de usuario. Este capítulo establece el modo en que el PEB consultará los sistemas centrales, así como el contenido y el formato de las respuestas a los usuarios. El capítulo II establece asimismo que eu-LISA conservará registros de todas las operaciones de tratamiento y dispone el procedimiento alternativo en caso de que el PEB no pudiera acceder a uno o varios de los sistemas centrales.

El capítulo III establece las disposiciones aplicables al servicio de correspondencia biométrica compartido (SCB compartido). Dispone la creación del SCB compartido y su arquitectura técnica, que desarrollará eu-LISA. Especifica la finalidad del SCB compartido y determina qué datos almacena. Explica la relación entre el SCB compartido y los demás componentes. El capítulo III también dispone que el SCB compartido no continuará almacenando aquellos datos que ya no figuren en el sistema central respectivo y que eu-LISA conservará registros de todas las operaciones de tratamiento.

El capítulo IV establece las disposiciones reguladoras del registro común de datos de identidad (RCDI). Dispone la creación del RCDI y su arquitectura técnica, que desarrollará eu-LISA. Especifica la finalidad del RCDI y aclara el tipo de datos que se almacenarán y cómo, incluyendo disposiciones destinadas a garantizar la calidad de los datos almacenados. Este capítulo establece que el RCDI creará expedientes individuales sobre la base de los datos contenidos en los sistemas centrales, y que los expedientes se actualizarán en respuesta a los cambios en cada uno de los sistemas centrales. El capítulo IV también detalla cómo funcionará el RCDI en relación con el detector de identidades múltiples. Dispone quiénes tendrán acceso al RCDI y cómo podrán acceder a los datos de conformidad con los derechos de acceso, incluidas disposiciones más específicas en función de si se accede a efectos de identificación o, en una primera fase del planteamiento en dos etapas, para acceder al SES, el

VIS, el SEIAV y Eurodac a través del RCDI con fines policiales. Por último, dispone que eu-LISA conservará registros de todas las operaciones de tratamiento efectuadas en relación con el RCDI.

El capítulo V establece las disposiciones reguladoras del detector de identidades múltiples (DIM). Dispone la creación del DIM y su arquitectura técnica, que desarrollará eu-LISA. Explica la finalidad del DIM y regula su uso, de conformidad con los derechos de acceso a cada uno de los sistemas centrales. Establece cuándo y cómo iniciará el DIM una consulta para detectar identidades múltiples, así como la forma y el seguimiento de los resultados, incluso, en su caso, mediante verificación manual. Establece una clasificación de los tipos de vínculo que puede dar como resultado la búsqueda, en función de si el resultado muestra la existencia de una única identidad, de identidades múltiples o de identidades compartidas. Dispone que el DIM almacenará los datos vinculados que existan en los sistemas centrales, siempre que estos datos permanezcan en dos o más sistemas centrales. Dispone también que eu-LISA conservará registros de todas las operaciones de tratamiento efectuadas en relación con el DIM.

El capítulo VI dispone medidas de apoyo a la interoperabilidad. Prevé mejorar la calidad de los datos mediante el establecimiento del formato universal de mensajes como norma común para el intercambio de información en apoyo de la interoperabilidad y la creación de un repositorio central para la presentación de informes y estadísticas.

El capítulo VII regula la protección de datos. Establece disposiciones para garantizar que el tratamiento de datos realizado de conformidad con el presente Reglamento sea conforme con la ley y adecuado, de conformidad con las disposiciones del Reglamento n.º 45/2001. Define quién será el encargado del tratamiento de los datos para cada una de las medidas de interoperabilidad propuestas en el presente Reglamento y establece las medidas exigidas por eu-LISA y las autoridades de los Estados miembros para garantizar la seguridad del tratamiento de los datos, la confidencialidad de los datos, la gestión adecuada de los incidentes de seguridad y la adecuada supervisión del cumplimiento de las disposiciones del presente Reglamento. También contiene disposiciones relativas a los derechos de los interesados, entre ellas el derecho a ser informados sobre los datos personales que les conciernan y que hayan sido almacenados y tratados en virtud del presente Reglamento, así como el derecho de acceso, corrección y supresión de los datos personales que hayan sido tratados y almacenados con arreglo al presente Reglamento. Establece además el principio de que los datos tratados con arreglo al presente Reglamento no se transmitirán ni se pondrán a disposición de ningún tercer país, organización internacional o entidad privada, con excepción de Interpol para fines específicos y de los datos recibidos de Europol a través del portal europeo de búsqueda, cuando las normas del Reglamento 2016/794 sobre el tratamiento posterior de los datos sean de aplicación. Por último, contiene las disposiciones relativas al control y la auditoría en relación con la protección de datos.

El capítulo VIII establece las responsabilidades de eu-LISA, antes y después de la entrada en funcionamiento de las medidas previstas en la propuesta, y de los Estados miembros, Europol y la unidad central SEIAV.

El capítulo IX se refiere a las modificaciones de otros instrumentos jurídicos de la Unión. En este capítulo se presentan las modificaciones de otros instrumentos jurídicos que son necesarias para la correcta ejecución de esta propuesta de interoperabilidad. Incluye disposiciones detalladas de los cambios necesarios en los instrumentos legales que son actualmente textos estables adoptados por los colegisladores: el Código de fronteras Schengen, el Reglamento SES, el Reglamento (CE) VIS, la Decisión 2004/512/CE del

Consejo (Decisión VIS) y la Decisión 2008/633/JAI del Consejo (Decisión VIS / acceso de los cuerpos policiales).

El capítulo X detalla los requisitos de información y estadísticas sobre los datos tratados de conformidad con el presente Reglamento; las medidas transitorias que serán necesarias; disposiciones relativas a los costes derivados del presente Reglamento; requisitos relativos a las notificaciones; el proceso de puesta en marcha de las medidas propuestas en el presente Reglamento; mecanismos de gobernanza, incluida la creación de un comité y un grupo consultivo, la responsabilidad de eu-LISA en materia de formación y un manual práctico de apoyo a la aplicación y gestión de los componentes de interoperabilidad; los procedimientos de supervisión y valoración de las medidas propuestas en el presente Reglamento y la entrada en vigor del presente Reglamento.

2017/0351 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (fronteras y visados) y por el que se modifican la Decisión 2004/512/CE del Consejo, el Reglamento (CE) n.º 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16, apartado 2, su artículo 74 y su artículo 77, apartado 2, letras a), b), d) y e),

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Previa consulta al Supervisor Europeo de Protección de Datos,

Visto el dictamen del Comité Económico y Social Europeo[43],

Visto el dictamen del Comité de las Regiones[44],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) En su Comunicación de 6 de abril de 2016 titulada *Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad*[45], la Comisión subrayó la necesidad de mejorar la arquitectura de gestión de datos de la Unión para la gestión de las fronteras y la seguridad. La Comunicación puso en marcha un proceso destinado a lograr la interoperabilidad de los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración, con el objetivo de solucionar las deficiencias estructurales de estos sistemas que obstaculizan la labor de las autoridades nacionales y garantizar que los guardias de fronteras, las autoridades aduaneras, los agentes de policía y las autoridades judiciales tengan a su disposición la información necesaria.

(2) En su Hoja de ruta para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior, de 6 de junio de 2016[46], el Consejo identificó varios retos jurídicos, técnicos y operativos para la interoperabilidad de los sistemas de información de la UE e instó a la búsqueda de soluciones.

---

43 DO C […] de […], p. […].

44

45 COM(2016) 205 de 6.4.2016.

46 Hoja de ruta de 6 de junio de 2016 para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior (9368/1/16 REV 1).

(3) En su Resolución de 6 de julio de 2016 sobre las prioridades estratégicas para el programa de trabajo de la Comisión para 2017[47], el Parlamento Europeo pidió que se presentaran propuestas para mejorar y desarrollar los sistemas de información de la UE existentes, avanzar hacia su interoperabilidad y colmar las lagunas de información, así como para el intercambio obligatorio de información a nivel de la UE, junto con las salvaguardias necesarias en materia de protección de datos.

(4) El Consejo Europeo de 15 de diciembre de 2016[48] pidió continuidad en la obtención de resultados en materia de interoperabilidad de los sistemas de información y bases de datos de la UE.

(5) En su informe final de 11 de mayo de 2017[49], el Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad llegó a la conclusión de que es necesario y técnicamente viable trabajar para poner en marcha soluciones prácticas en materia de interoperabilidad y que estas, en principio, pueden producir beneficios operativos al tiempo que cumplen los requisitos sobre protección de datos.

(6) En su Comunicación de 16 de mayo de 2017 titulada *Séptimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva*[50], la Comisión diseñó, en consonancia con su Comunicación de 6 de abril de 2016 y confirmando las conclusiones y recomendaciones del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad, un nuevo planteamiento para la gestión de los datos relativos a las fronteras, la seguridad y la migración, en virtud del cual todos los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración serían interoperables sin menoscabo alguno de los derechos fundamentales.

(7) En sus Conclusiones de 9 de junio de 2017[51] sobre los siguientes pasos para mejorar el intercambio de información y garantizar la interoperabilidad de los sistemas de información de la UE, el Consejo invitó a la Comisión a buscar soluciones de interoperabilidad según lo propuesto por el Grupo de Expertos de Alto Nivel.

(8) El Consejo Europeo de 23 de junio de 2017[52] puso de relieve la necesidad de mejorar la interoperabilidad de las bases de datos e invitó a la Comisión a preparar, lo antes posible, proyectos legislativos para hacer efectivas las propuestas formuladas por el Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad.

(9) Con objeto de mejorar la gestión de las fronteras exteriores, de prevenir y combatir la migración irregular y de alcanzar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, lo que incluye el mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros, debe establecerse la interoperabilidad de los sistemas de información de la UE, es decir [el Sistema de Entradas y Salidas (SES)], el Sistema de Información de Visados (VIS), [el Sistema Europeo de Información y Autorización de Viajes (SEIAV)], Eurodac, el Sistema de Información de Schengen (SIS), y el [Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)], para que estos sistemas de información y sus datos se complementen mutuamente. Para ello, deben crearse, como componentes de

---

47 Resolución del Parlamento Europeo de 6 de julio de 2016 sobre las prioridades estratégicas para el programa de trabajo de la Comisión para 2017 [2016/2773 (RSP)].

48 http://www.consilium.europa.eu/es/press/press-releases/2016/12/15/euco-conclusions-final/

49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

50 COM(2017) 261 final, de 16.5.2017.

51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf

52 Conclusiones del Consejo Europeo de 22 y 23 de junio de 2017.

interoperabilidad, un portal europeo de búsqueda (PEB), un servicio de correspondencia biométrica compartido (SCB compartido), un registro común de datos de identidad (RCDI) y un detector de identidades múltiples (DIM).

(10) La interoperabilidad de los sistemas de información de la UE debe permitirles complementarse a fin de facilitar la identificación correcta de las personas, contribuir a luchar contra la usurpación de identidad, mejorar y armonizar los requisitos de calidad de los datos de los respectivos sistemas de información de la UE, facilitar la aplicación técnica y operativa por los Estados miembros de los sistemas de información de la UE existentes y futuros, reforzar y simplificar las garantías de seguridad de los datos y de protección de datos que rigen en los respectivos sistemas de información de la UE, racionalizar el acceso de los cuerpos policiales al SES, el VIS, [el SEIAV] y Eurodac, y apoyar los objetivos del SES, el VIS, el [SEIAV], Eurodac, el SIS y el [sistema ECRIS-TCN].

(11) Los componentes de interoperabilidad deben abarcar el SES, el VIS, el [SEIAV], Eurodac, el SIS y el [sistema ECRIS-TCN]. Asimismo, deben incluir los datos de Europol en tal medida que permita consultarlos al mismo tiempo que estos sistemas de información de la UE.

(12) Los componentes de interoperabilidad deben referirse a las personas cuyos datos personales puedan ser tratados por los sistemas de información de la UE y por Europol, es decir, los nacionales de terceros países cuyos datos personales sean tratados por los sistemas de información de la UE y por Europol y los ciudadanos de la Unión cuyos datos personales sean tratados en el SIS y por Europol.

(13) Debe crearse un portal europeo de búsqueda (PEB) con el fin de facultar técnicamente a las autoridades de los Estados miembros y los organismos de la Unión Europea para tener un acceso rápido, ininterrumpido, eficiente, sistemático y controlado, de conformidad con sus derechos de acceso, a los sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol necesarios para llevar a cabo sus tareas, así como para apoyar los objetivos del SES, el VIS, [el SEIAV], Eurodac, el SIS, [el sistema ECRIS-TCN] y los datos de Europol. Al permitir la consulta simultánea de todos los sistemas de información de la UE relevantes en paralelo, así como de los datos de Europol y las bases de datos de Interpol, el PEB debe actuar como una ventanilla única o «intermediario de mensajes» a distintos sistemas centrales de búsqueda y recabar la información necesaria de forma ininterrumpida y en el pleno respeto de las normas de control de acceso y los requisitos de protección de datos de los sistemas subyacentes.

(14) La base de datos de documentos de viaje robados y perdidos (DVRP) de la Organización Internacional de Policía Criminal (Interpol) permite a los cuerpos de seguridad autorizados en los Estados miembros, incluidos los funcionarios de inmigración y de control de las fronteras, determinar la validez de un documento de viaje. El [SEIAV] consulta la DVRP y la base de datos, también de Interpol, de documentos de viaje asociados a notificaciones (TDAWN) para valorar la probabilidad de que una persona que solicite una autorización de viaje esté migrando de manera irregular o pueda suponer una amenaza a la seguridad. El portal europeo de búsqueda (PEB) centralizado debe permitir la consulta de los datos de identidad de una persona física en las bases de datos DVRP y TDAWN. Cuando se transmitan datos personales desde la Unión a Interpol a través del PEB, deben aplicarse las disposiciones sobre transmisiones internacionales que contempla el capítulo V del

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[53] o las disposiciones nacionales de transposición del capítulo V de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[54], sin perjuicio de las normas específicas establecidas en la Posición Común 2005/69/JAI del Consejo[55] y en la Decisión 2007/533/JAI del Consejo[56].

(15) El portal europeo de búsqueda (PEB) debe desarrollarse y configurarse de tal forma que no permita la utilización para la consulta de campos de datos que no estén relacionados con personas o documentos de viaje o que no estén presentes en el sistema de información de la UE, en los datos de Europol o en la base de datos de Interpol.

(16) Para garantizar un uso rápido y sistemático de todos los sistemas de información de la UE, el portal europeo de búsqueda (PEB) debe utilizarse para consultar el registro común de datos de identidad, el SES, el VIS, [el SEIAV], Eurodac y [el sistema ECRIS-TCN]. Sin embargo, debe mantenerse la conexión nacional a los diferentes sistemas de información de la UE, a fin de proporcionar una alternativa técnica. También los organismos de la Unión han de utilizar el PEB para consultar el SIS Central de conformidad con sus derechos de acceso, en el ejercicio de sus funciones. El PEB debe ser un medio suplementario para consultar el SIS Central, los datos de Europol y los sistemas de Interpol, como complemento de las interfaces específicas existentes.

(17) Los datos biométricos, como las impresiones dactilares y las imágenes faciales, son únicos y, por tanto, mucho más fiables para la identificación de una persona que los datos alfanuméricos. El servicio de correspondencia biométrica compartido (SCB compartido) debe ser un instrumento técnico para reforzar y facilitar la labor de los sistemas de información de la UE relevantes y los demás componentes de interoperabilidad. El objetivo principal del SCB compartido debe ser facilitar la identificación de una persona que pueda estar registrada en bases de datos diferentes, cotejando sus datos biométricos entre diferentes sistemas y sobre la base de un único componente tecnológico, en lugar de cinco componentes diferentes en cada uno de los sistemas subyacentes. El SCB compartido debe contribuir a la seguridad, así como aportar beneficios desde el punto de vista financiero, operativo y de mantenimiento, sobre la base de un único componente tecnológico en lugar de componentes diferentes en cada uno de los sistemas subyacentes. Todos los sistemas automáticos de identificación mediante impresiones dactilares, incluidos los utilizados actualmente para Eurodac, el VIS y el SIS, utilizan plantillas biométricas compuestas por los datos obtenidos mediante una extracción de características de muestras biométricas reales. El SCB compartido debe agrupar y almacenar todas estas plantillas biométricas en un

---

[53] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

[54] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

[55] Posición Común 2005/69/JAI del Consejo, de 24 de enero de 2005, relativa al intercambio de determinados datos con Interpol (DO L 27 de 29.1.2005, p. 61).

[56] Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 205 de 7.8.2007, p. 63).

único lugar, facilitar las comparaciones cruzadas entre sistemas por medio de los datos biométricos y permitir economías de escala en el desarrollo y el mantenimiento de los sistemas centrales de la UE.

(18) Los datos biométricos constituyen datos personales sensibles. El presente Reglamento debe establecer las bases y las salvaguardias para el tratamiento de dichos datos a los únicos efectos de la identificación inequívoca de las personas afectadas.

(19) Para poder ser eficaces, los sistemas creados por el Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo[57], el Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo[58], [el Reglamento SEIAV] para la gestión de las fronteras de la Unión, el sistema creado por [el Reglamento Eurodac] para identificar a los solicitantes de protección internacional y luchar contra la migración irregular y el sistema creado por el [Reglamento del sistema ECRIS-TCN] necesitan apoyarse en una identificación exacta de los nacionales de terceros países cuyos datos personales están almacenados en ellos.

(20) El registro común de datos de identidad (RCDI) debe, por consiguiente, facilitar la identificación correcta de las personas registradas en el SES, el VIS, [el SEIAV], Eurodac y [el sistema ECRIS-TCN] y ayudar a ella.

(21) Los datos personales almacenados en los citados sistemas de información de la UE pueden referirse a las mismas personas, pero con identidades distintas o incompletas. Los Estados miembros disponen de métodos eficaces para identificar a sus ciudadanos o a los residentes permanentes registrados en su territorio, pero no sucede lo mismo con los nacionales de terceros países. La interoperabilidad de los sistemas de información de la UE debe contribuir a la identificación correcta de los nacionales de terceros países. El registro común de datos de identidad (RCDI) debe almacenar aquellos datos personales, relativos a los ciudadanos de terceros países presentes en los sistemas, que sean necesarios para permitir la identificación más precisa de dichas personas, es decir, al menos su identidad, su documento de viaje y sus datos biométricos, independientemente del sistema en el que se recogieran originalmente los datos. Solamente deben almacenarse en el RCDI los datos personales estrictamente necesarios para llevar a cabo un control de identidad adecuado. Los datos personales registrados en el RCDI no deben conservarse durante más tiempo del estrictamente necesario para los fines de los sistemas subyacentes y deben eliminarse automáticamente cuando se eliminen los datos en los sistemas subyacentes, con arreglo a su separación lógica.

(22) La nueva operación de tratamiento consistente en el almacenamiento de dichos datos en el registro común de datos de identidad (RCDI), en lugar de su almacenamiento en cada uno de los diferentes sistemas, es necesaria para mejorar la exactitud de la identificación, que se hace posible gracias a la comparación automatizada y las correspondencias de dichos datos. El hecho de que la identidad y los datos biométricos de los nacionales de terceros países se almacenen en el RCDI no debe obstaculizar en modo alguno el tratamiento de datos para los fines de los Reglamentos del SES, el

57 Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n.º 767/2008 y (UE) n.º 1077/2011 (DO L 327 de 9.12.2017, p. 20).

58 Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS) (DO L 218 de 13.8.2008, p. 60).

VIS, el SEIAV, Eurodac o el sistema ECRIS-TCN, ya que el RCDI debe ser un nuevo componente compartido de dichos sistemas subyacentes.

(23) En este contexto, crear un expediente individual en el registro común de datos de identidad (RCDI) para cada persona que se registre en el SES, el VIS, el SEIAV, Eurodac o el sistema ECRIS-TCN es necesario para alcanzar el objetivo de una identificación correcta de los nacionales de terceros países en el espacio Schengen y para apoyar al detector de identidades múltiples con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y luchar contra la usurpación de identidad. El expediente individual debe almacenarse en un único lugar, dando acceso a los usuarios finales debidamente autorizados a todas las posibles identidades vinculadas a una persona.

(24) El registro común de datos de identidad (RCDI) debe, por lo tanto, apoyar el funcionamiento del detector de identidades múltiples y facilitar y racionalizar el acceso de los cuerpos policiales a los sistemas de información de la UE que no se hayan creado exclusivamente con fines de prevención, investigación, detección o enjuiciamiento de delitos graves.

(25) El registro común de datos de identidad (RCDI) debe proporcionar un repositorio común de los datos de identidad y biométricos de los nacionales de terceros países registrados en el SES, el VIS, [el SEIAV], Eurodac y [el sistema ECRIS-TCN], como componente compartido entre estos sistemas para el almacenamiento de esos datos y para permitir su consulta.

(26) Todas las anotaciones presentes en el registro común de datos de identidad (RCDI) deben tener una separación lógica consistente en etiquetar automáticamente cada anotación con el sistema subyacente que lo contenga. El control de acceso del RCDI debe utilizar estas etiquetas para permitir o no el acceso a la anotación en cuestión.

(27) Con objeto de garantizar la identificación correcta de una persona, las autoridades de los Estados miembros competentes para prevenir y combatir la migración irregular y las autoridades competentes en el sentido del artículo 3, apartado 7, de la Directiva 2016/680 deben poder consultar el registro común de datos de identidad (RCDI) con los datos biométricos de esa persona que se hayan tomado durante un control de identidad.

(28) Cuando no puedan utilizarse los datos biométricos de la persona o si la consulta de esos datos es infructuosa, la consulta debe llevarse a cabo con los datos de identificación de dicha persona en combinación con los datos del documento de viaje. Cuando la consulta indique que los datos sobre la persona están almacenados en el registro común de datos de identidad (RCDI), las autoridades de los Estados miembros deben tener acceso a los datos de identidad de esa persona almacenados en el RCDI, sin proporcionar ninguna indicación relativa al sistema de información de la UE al que pertenezcan los datos.

(29) Los Estados miembros deben adoptar medidas legislativas nacionales que designen a las autoridades competentes para llevar a cabo controles de identidad mediante el uso del registro común de datos de identidad (RCDI) y establezcan los procedimientos, las condiciones y los criterios de dichos controles en consonancia con el principio de proporcionalidad. En particular, la facultad de recoger datos biométricos durante el control de identidad de una persona presente ante el representante de dichas autoridades debe preverse mediante medidas legislativas nacionales.

(30) El presente Reglamento debe también introducir una nueva posibilidad de acceso racional a datos diferentes de los datos de identidad registrados en el SES, el VIS, [el SEIAV] y Eurodac por parte de los cuerpos policiales designados de los Estados miembros y de Europol. Los datos, incluidos los datos distintos de los datos de identidad contenidos en estos sistemas, pueden ser necesarios para la prevención, la detección, la investigación y el enjuiciamiento de delitos de terrorismo o delitos graves en un caso concreto.

(31) El pleno acceso a los datos contenidos en los sistemas de información de la UE necesarios para los fines de prevención, detección e investigación de los delitos de terrorismo u otros delitos graves y distintos de los datos de identidad relevantes cubiertos por el registro común de datos de identidad (RCDI) que se hayan obtenido mediante el uso de los datos biométricos de la persona tomados con ocasión de un control de identidad debe seguir rigiéndose por lo dispuesto en los instrumentos jurídicos respectivos. Los cuerpos policiales designados y Europol no saben de antemano cuáles de los sistemas de información de la UE contienen datos de las personas respecto de las cuales necesitan investigar. Esto da lugar a ineficiencias y retrasos en la realización de sus tareas. El usuario final autorizado por la autoridad designada debe, por lo tanto, estar autorizado a ver en cuál de los sistemas de información de la UE están contenidos los datos que corresponden a la consulta introducida. El sistema correspondiente, por tanto, se señalaría con una indicación tras la verificación automatizada de la presencia de una respuesta positiva en el sistema (la denominada funcionalidad de aviso de respuesta positiva).

(32) Los registros de las consultas del registro común de datos de identidad deben indicar la finalidad de la consulta. Cuando dicha consulta se haya llevado a cabo utilizando el planteamiento de consulta de datos en dos fases, los registros deben incluir una referencia al expediente nacional de la investigación o del caso e indicar, consecuentemente, que dicha consulta ha sido iniciada con fines de prevención, detección e investigación de delitos de terrorismo u otros delitos graves.

(33) La consulta del registro común de datos de identidad (RCDI) por parte de las autoridades designadas por los Estados miembros y Europol para obtener un aviso de respuesta positiva que muestre que los datos están contenidos en el SES, el VIS, [el SEIAV] o Eurodac exige el tratamiento automatizado de datos personales. Un aviso de respuesta positiva no revela datos personales de la persona de que se trate, aparte de la indicación de que algunos de sus datos están almacenados en uno de los sistemas. El usuario final autorizado no debe tomar ninguna decisión perjudicial para la persona de que se trate basándose únicamente en la presencia de un aviso de respuesta positiva. El acceso del usuario final a un aviso de respuesta positiva supone, por lo tanto, una interferencia muy limitada con el derecho a la protección de los datos personales de la persona de que se trate, puesto que sería necesario permitir a la autoridad designada y a Europol dirigir su solicitud de acceso a los datos personales, en aras de una mayor eficacia, directamente al sistema del que provenga el aviso.

(34) El planteamiento de consulta de datos en dos fases resulta especialmente beneficioso en los casos en que el sospechoso, el autor o la víctima de un delito de terrorismo u otro delito grave sean desconocidos. En tales casos, el registro común de datos de identidad (RCDI) debe permitir identificar en una única búsqueda el sistema de información en que esté presente esa persona. Al establecer la obligación de utilizar este nuevo planteamiento de acceso policial en estos casos, el acceso a los datos personales almacenados en el SES, el VIS, [el SEIAV] y Eurodac debe llevarse a cabo sin las exigencias de una búsqueda previa en bases de datos nacionales y del inicio de

una búsqueda previa en el sistema automático de identificación dactilar de otros Estados miembros de conformidad con la Decisión 2008/615/JAI. El principio de búsqueda previa limita efectivamente la posibilidad de que las autoridades del Estado miembro consulten los sistemas por motivos policiales justificados y podría, por tanto, dar lugar a que se pierdan oportunidades de descubrir la información necesaria. Los requisitos de una búsqueda previa en las bases de datos nacionales y el inicio de una búsqueda previa en el sistema automático de identificación dactilar de otros Estados miembros de conformidad con la Decisión 2008/615/JAI solo deben dejar de aplicarse sea efectiva la salvaguardia alternativa del planteamiento en dos fases para el acceso de los cuerpos policiales a través del RCDI.

(35) Debe crearse un detector de identidades múltiples (DIM) a fin de respaldar el funcionamiento del registro común de datos de identidad y de apoyar los objetivos del SES, el VIS, [el SEIAV], Eurodac, el SIS y [el sistema ECRIS-TCN]. Para ser eficaces en el cumplimiento de sus respectivos objetivos, todos los sistemas de información de la UE exigen la identificación exacta de las personas cuyos datos personales almacenan.

(36) La posibilidad de alcanzar los objetivos de los sistemas de información de la UE se ve socavada por la actual incapacidad de las autoridades de utilizar estos sistemas para llevar a cabo verificaciones suficientemente fiables de las identidades de los nacionales de terceros países cuyos datos estén almacenados en sistemas diferentes. Esa incapacidad viene determinada por el hecho de que el conjunto de datos de identidad almacenados en un sistema individual concreto puede ser fraudulento, incorrecto o incompleto, y de que actualmente no existe ninguna posibilidad de detectar tales datos de identidad fraudulentos, incorrectos o incompletos por medio de una comparación con los datos almacenados en otro sistema. Para resolver esta situación, es necesario disponer de un instrumento técnico a escala de la Unión que permita la identificación correcta de los nacionales de terceros países a esos efectos.

(37) El detector de identidades múltiples (DIM) debe crear y almacenar vínculos entre los datos de los distintos sistemas de información de la UE para detectar las identidades múltiples, con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y de luchar contra la usurpación de identidad. Solamente debe contener los vínculos entre las personas presentes en más de un sistema de información de la UE, estrictamente limitados a los datos necesarios para verificar que una persona está registrada, ya sea legal o ilegalmente, con diferentes identidades biográficas en diferentes sistemas, o para aclarar que dos personas con similares datos biográficos no pueden ser la misma persona. El tratamiento de datos a través del portal europeo de búsqueda (PEB) y del servicio de correspondencia biométrica compartido (SCB compartido), destinado a vincular expedientes individuales a través de sistemas individuales, debe quedar restringido a un mínimo absoluto y, por lo tanto, limitarse a la detección de identidades múltiples en el momento en que se añadan nuevos datos a uno de los sistemas de información incluidos en el registro común de datos de identidad y en el SIS. El DIM debe incluir salvaguardias de las personas con múltiples identidades legales contra una posible discriminación o decisiones que les sean desfavorables.

(38) El presente Reglamento establece nuevas operaciones de tratamiento de datos destinadas a identificar correctamente a las personas de que se trate. Esto constituye una injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales. Dado que la aplicación eficaz de los sistemas de información de la UE depende de la identificación correcta de las personas

afectadas, tal injerencia está justificada por los mismos objetivos para los que se ha creado cada uno de estos sistemas: la gestión eficaz de las fronteras de la Unión, la seguridad interna de la Unión, la aplicación efectiva de las políticas de la Unión en materia de visados y asilo y la lucha contra la migración irregular.

(39) El portal europeo de búsqueda (PEB) y el servicio de correspondencia biométrica compartido (SCB compartido) deben comparar los datos sobre personas contenidos en el registro común de datos de identidad (RCDI) y en el SIS cuando una autoridad nacional o un organismo de la UE creen nuevas anotaciones. Dicha comparación debe estar automatizada. El RCDI y el SIS deben utilizar el SCB compartido para detectar posibles vínculos basados en datos biométricos. El RCDI y el SIS deben utilizar el PEB para detectar posibles vínculos basados en datos alfanuméricos. El RCDI y el SIS deben poder identificar datos idénticos o similares relativos a un nacional de un tercer país almacenados en varios sistemas. Cuando ese sea el caso, debe establecerse un vínculo que indique que se trata de la misma persona. El RCDI y el SIS deben configurarse de manera que detecten los pequeños errores de transliteración o de deletreo, da fin de que no sean fuentes de inconvenientes injustificados para el nacional de un tercer país de que se trate.

(40) La autoridad nacional o el organismo de la UE que haya registrado los datos en el sistema de información de la UE respectivo debe confirmar o modificar esos vínculos. Esa autoridad debe tener acceso a los datos almacenados en el registro común de datos de identidad (RCDI) o el SIS y en el detector de identidades múltiples (DIM), a efectos de la verificación manual de la identidad.

(41) El acceso al detector de identidades múltiples (DIM) por las autoridades de los Estados miembros y los organismos de la UE que tengan acceso, como mínimo, a un sistema de información de la UE incluido en el registro común de datos de identidad (RCDI) o al SIS debe limitarse a los denominados vínculos rojos, que se indicarán cuando los datos vinculados consistan en los mismos datos biométricos pero diferentes datos de identidad y la autoridad responsable de verificar las diferentes identidades concluya que aquellos se refieren a la misma persona de forma ilegal, o cuando los datos vinculados consistan en datos de identidad similares y la autoridad responsable de verificar las diferentes identidades concluya que se refieren a la misma persona de forma ilegal. Cuando los datos de identidad vinculados no sean similares, debe establecerse un vínculo amarillo y procederse a una verificación manual para confirmar el vínculo o cambiar su color convenientemente.

(42) La verificación manual de identidades múltiples debe ser garantizada por la autoridad que haya creado o actualizado los datos que hayan generado la respuesta positiva expresada mediante un vínculo con datos ya almacenados en otro sistema de información de la UE. La autoridad responsable de verificar las identidades múltiples debe evaluar si existen múltiples identidades legales o ilegales. Dicha evaluación debe llevarse a cabo, cuando sea posible, en presencia del nacional de un tercer país y, en caso necesario, solicitando aclaraciones o información adicionales. Dicha evaluación debe realizarse sin demora, de conformidad con los requisitos legales para la exactitud de la información que contemplen la legislación nacional y la de la Unión.

(43) Para los vínculos obtenidos en relación con el Sistema de Información de Schengen (SIS) y relacionados con las descripciones de personas buscadas para su detención, su entrega voluntaria o su extradición; personas desaparecidas o vulnerables; personas buscadas para que presten asistencia en un procedimiento judicial; personas buscadas a efectos de controles discretos o de controles específicos; o personas buscadas

desconocidas, la autoridad responsable de verificar las identidades múltiples debe ser la oficina SIRENE del Estado miembro que haya creado la descripción. De hecho, dichas categorías de descripciones del SIS son sensibles y no deben necesariamente ser compartidas con las autoridades que hayan creado o actualizado los datos en uno de los otros sistemas de información de la UE. La creación de un vínculo con datos del SIS debe realizarse sin perjuicio de las medidas que deban adoptarse en virtud de lo dispuesto en los [Reglamentos SIS].

(44) La agencia eu-LISA debe establecer mecanismos automatizados de control de calidad de los datos e indicadores comunes de calidad de los datos. Debe ser responsable del desarrollo de una capacidad central de supervisión de la calidad de los datos y de la elaboración de informes periódicos de análisis de datos para mejorar el control de la implementación y la aplicación por los Estados miembros de los sistemas de información de la UE. Los indicadores comunes de calidad deben incluir las normas mínimas de calidad aplicables al almacenamiento de datos en los sistemas de información de la UE o en los componentes de interoperabilidad. El objetivo de dichas normas de calidad de los datos debe ser que los sistemas de información de la UE y los componentes de interoperabilidad identifiquen de forma automática presentaciones de datos aparentemente incorrectas o incoherentes, de modo que el Estado miembro que haya generado los datos pueda verificarlos y tomar las medidas correctoras que sean necesarias.

(45) La Comisión debe evaluar los informes de calidad de eu-LISA y formular recomendaciones a los Estados miembros cuando proceda. Los Estados miembros deben ser responsables de la preparación de un plan de acción que describa las medidas destinadas a corregir cualquier deficiencia en la calidad de los datos y deben informar periódicamente sobre sus progresos.

(46) El formato universal de mensajes (UMF) debe establecer una norma para el intercambio de información transfronterizo y estructurado entre sistemas de información, autoridades y organizaciones en el ámbito de la justicia y los asuntos de interior. El UMF debe definir un vocabulario común y estructuras lógicas para la información intercambiada habitualmente con el objetivo de facilitar la interoperabilidad y permitir la creación y la lectura del contenido del intercambio de forma coherente y equivalente desde el punto de vista semántico.

(47) Debe crearse un repositorio central para la presentación de informes y estadísticas (RCIE) para generar datos estadísticos entre sistemas e informes de análisis relativos a la formulación de políticas, la operatividad y la calidad de los datos. La agencia eu-LISA debe crear e implementar el RCIE y alojarlo en sus sitios técnicos que contengan datos estadísticos anónimos procedentes de los sistemas mencionados anteriormente, el registro común de datos de identidad, el detector de identidades múltiples y el servicio de correspondencia biométrica compartido. Los datos contenidos en el RCIE no deben permitir la identificación de personas. La agencia eu-LISA debe anonimizar los datos y registrar los datos anónimos en el RCIE. El proceso para anonimizar los datos debe ser automatizado y no debe concederse al personal de eu-LISA acceso a ninguno de los datos personales almacenados en los sistemas de información de la UE o en los componentes de interoperabilidad.

(48) El Reglamento (UE) 2016/679 debe ser de aplicación al tratamiento de datos personales por las autoridades nacionales en virtud del presente Reglamento, a menos que sean las autoridades designadas o los puntos de acceso central de los Estados miembros quienes lleven a cabo dicho tratamiento por razones de prevención,

detección o investigación de los delitos de terrorismo u otros delitos graves, caso en el que será de aplicación la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.

(49) Las disposiciones específicas sobre protección de datos del [Reglamento SES], el Reglamento (CE) n.º 767/2008, [el Reglamento SEIAV] y [el Reglamento sobre el SIS en el ámbito de las inspecciones fronterizas] deben ser de aplicación al tratamiento de datos personales en esos respectivos sistemas.

(50) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo[59] debe ser de aplicación al tratamiento de los datos personales por eu-LISA y otras instituciones y organismos de la Unión en el ejercicio de sus responsabilidades con arreglo al presente Reglamento, sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/794, aplicable al tratamiento de datos personales por parte de Europol.

(51) Las autoridades nacionales de control creadas de conformidad con el [Reglamento (UE) 2016/679] deben supervisar la legalidad del tratamiento de los datos personales por los Estados miembros, mientras que el Supervisor Europeo de Protección de Datos, instituido por el Reglamento (CE) n.º 45/2001, debe supervisar las actividades que llevan a cabo las instituciones y organismos de la Unión en relación con el tratamiento de datos personales. El Supervisor Europeo de Protección de Datos y las autoridades de control deben cooperar en la supervisión del tratamiento de los datos personales que se realice mediante los componentes de interoperabilidad.

(52) «(...) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, se consultó al Supervisor Europeo de Protección de Datos, que emitió su dictamen el ...»

(53) En lo que respecta a la confidencialidad, las disposiciones pertinentes del Estatuto de los funcionarios y el régimen aplicable a los otros agentes de la Unión Europea deben aplicarse a los funcionarios y otros agentes de la Unión Europea que trabajen en ámbitos relacionados con el SIS.

(54) Los Estados miembros y eu-LISA deben disponer de planes de seguridad para facilitar el cumplimiento de las obligaciones en materia de seguridad y deben cooperar entre sí para solucionar los problemas de seguridad. La agencia eu-LISA también debe asegurarse de que se haga un uso continuo de los avances tecnológicos más recientes a fin de garantizar la integridad de los datos en relación con el desarrollo, el diseño y la gestión de los componentes de interoperabilidad.

(55) La aplicación de los componentes de interoperabilidad previstos en el presente Reglamento tendrá repercusiones sobre la manera en que se llevan a cabo las inspecciones en los pasos fronterizos. Estas repercusiones serán el resultado de la aplicación combinada de las disposiciones vigentes del Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo[60] y de las normas sobre interoperabilidad dispuestas en el presente Reglamento.

(56) Como consecuencia de esta aplicación combinada de las normas, el portal europeo de búsqueda (PEB) debe constituir el principal punto de acceso para la consulta

[59] Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

[60] Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (DO L 77 de 23.3.2016, p. 1).

sistemática obligatoria de las bases de datos sobre nacionales de terceros países en los pasos fronterizos, prevista por el Código de fronteras Schengen. Además, los guardias de fronteras deben tener en cuenta los datos de identidad que hayan dado lugar a la clasificación como vínculo rojo de un vínculo en el detector de identidades múltiples (DIM), para evaluar si el interesado cumple o no las condiciones de entrada definidas en el Código de fronteras Schengen. Sin embargo, la presencia de un vínculo rojo no constituye en sí misma un motivo de denegación de entrada y, por lo tanto, los motivos de denegación de entrada que actualmente se enumeran en el Código de fronteras Schengen no deben modificarse.

(57) Resulta oportuno actualizar el Manual práctico para guardias de fronteras a fin de formular de forma explícita estas aclaraciones.

(58) Sin embargo, es necesaria una modificación del Reglamento (UE) 2016/399 para añadir la obligación para el guardia de fronteras de enviar a un nacional de un tercer país a una inspección de segunda línea en caso de que la consulta del detector de identidades múltiples (DIM) a través del portal europeo de búsqueda (PEB) indique la existencia de un vínculo amarillo o un vínculo rojo, a fin de no prolongar el tiempo de espera en la inspección de primera línea.

(59) En caso de que la consulta del detector de identidades múltiples (DIM) a través del portal europeo de búsqueda (PEB) resulte en un vínculo amarillo o detecte un vínculo rojo, el guardia de fronteras de segunda línea debe consultar el registro común de datos de identidad, el Sistema de Información de Schengen o ambos, a fin de evaluar la información relativa a la persona objeto de la inspección, verificar manualmente su identidad diferente y, si procede, adaptar el color del vínculo.

(60) Para apoyar los objetivos en materia de estadísticas e informes, es necesario conceder al personal autorizado de las autoridades competentes, las instituciones y los organismos determinados en el presente Reglamento acceso para consultar determinados datos relativos a determinados componentes de interoperabilidad sin permitir la identificación individual.

(61) A fin de permitir a las autoridades competentes y los organismos de la UE adaptarse a los nuevos requisitos sobre el uso del portal europeo de búsqueda (PEB), es necesario prever un periodo transitorio. Del mismo modo, a fin de garantizar la coherencia y el funcionamiento óptimo del detector de identidades múltiples (DIM), deben adoptarse medidas transitorias para su entrada en funcionamiento.

(62) Los costes aparejados al desarrollo de los componentes de interoperabilidad previsto durante la vigencia del actual Marco Financiero Plurianual son menores que el saldo presupuestario asignado a las fronteras inteligentes con arreglo al Reglamento (UE) n.º 515/2014 del Parlamento Europeo y del Consejo[61]. Por consiguiente, el presente Reglamento, de conformidad con el artículo 5, apartado 5, letra b), del Reglamento (UE) n.º 515/2014, debe reasignar el importe actualmente atribuido al desarrollo de sistemas informáticos de apoyo a la gestión de los flujos migratorios en las fronteras exteriores.

(63) Para complementar ciertos aspectos técnicos concretos del presente Reglamento, debe delegarse a la Comisión la competencia de adoptar actos de conformidad con el

[61] Reglamento (UE) n ° 515/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014 , por el que se establece, como parte del Fondo de Seguridad Interior, el instrumento de apoyo financiero a las fronteras exteriores y los visados y por el que se deroga la Decisión n ° 574/2007/CE (DO L 150 de 20.5.2014, p. 143).

artículo 290 del Tratado de Funcionamiento de la Unión Europea, en lo que se refiere a los perfiles de los usuarios del portal europeo de búsqueda (PEB) y el contenido y el formato de las respuestas que el PEB ofrezca. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016[62]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo deben recibir toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos deben poder asistir sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(64) A fin de garantizar la aplicación uniforme del presente Reglamento, deben otorgarse a la Comisión competencias de ejecución para adoptar normas detalladas relativas a: los mecanismos, procedimientos e indicadores de control automatizado de la calidad de los datos; el desarrollo de la norma UMF; los procedimientos para determinar los casos de similitud de identidades; el funcionamiento del repositorio central para la presentación de informes y estadísticas, y el procedimiento de cooperación en caso de incidentes de seguridad. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[63].

(65) El Reglamento 2016/794 debe ser de aplicación a todo tratamiento de datos que lleve a cabo Europol a los efectos del presente Reglamento.

(66) El presente Reglamento se entiende sin perjuicio de la aplicación de la Directiva 2004/38/CE.

(67) El presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen.

(68) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la adopción del presente Reglamento y no queda vinculada por este ni sujeta a su aplicación. Dado que el presente Reglamento desarrolla el acervo de Schengen, Dinamarca, de conformidad con lo dispuesto en el artículo 4 del mencionado Protocolo, debe decidir, en un plazo de seis meses a partir de la adopción del presente Reglamento, si lo incorpora o no a su Derecho nacional.

(69) El presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen en las que el Reino Unido no participa, de conformidad con la Decisión 2000/365/CE del Consejo[64]; el Reino Unido no participa, en consecuencia, en la aprobación del presente Reglamento ni está vinculado por este ni sujeto a su aplicación.

---

62 http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016Q0512(01)

63 Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

64 Decisión 2000/365/CE del Consejo, de 29 de mayo de 2000, sobre la solicitud del Reino Unido de Gran Bretaña e Irlanda del Norte de participar en algunas de las disposiciones del acervo de Schengen (DO L 131 de 1.6.2000, p. 43).

(70) El presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen en las que Irlanda no participa de conformidad con la Decisión 2002/192/CE del Consejo[65]. Irlanda no participa, en consecuencia, en la aprobación del presente Reglamento ni está vinculada por este ni sujeta a su aplicación.

(71) En lo que respecta a Islandia y Noruega, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del acuerdo celebrado por el Consejo de la Unión Europea con la República de Islandia y el Reino de Noruega sobre la asociación de esos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen[66], que entran dentro del ámbito mencionado en el artículo 1, puntos A, B y G, de la Decisión 1999/437/CE del Consejo, de 17 de mayo de 1999, relativa a determinadas normas de desarrollo de dicho acuerdo[67].

(72) En lo que respecta a Suiza, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen, en el sentido del Acuerdo firmado entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen[68], que entran dentro del ámbito previsto en el artículo 1, puntos A, B y G, de la Decisión 1999/437/CE, leído en relación con el artículo 3 de la Decisión 2008/146/CE del Consejo[69].

(73) En lo que respecta a Liechtenstein, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del Protocolo entre la Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein sobre la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, la aplicación y el desarrollo del acervo de Schengen[70], que entran dentro del ámbito mencionado en el artículo 1, puntos A, B y G, de la Decisión 1999/437/CE del Consejo, leído en relación con el artículo 3 de la Decisión 2011/350/UE del Consejo[71].

(74) En lo que respecta a Chipre, las disposiciones relacionadas con el SIS y el VIS constituyen disposiciones que desarrollan el acervo de Schengen o están relacionadas con él en el sentido del artículo 3, apartado 2, del Acta de adhesión de 2003.

(75) En lo que respecta a Bulgaria y Rumanía, las disposiciones relacionadas con el SIS y el VIS constituyen disposiciones que desarrollan el acervo de Schengen o están relacionadas con él en el sentido del artículo 4, apartado 2, del Acta de adhesión de 2005, leído en relación con la Decisión 2010/365/UE del Consejo[72] y la Decisión (UE) 2017/1908 del Consejo[73].

---

[65] Decisión 2002/192/CE del Consejo, de 28 de febrero de 2002, sobre la solicitud de Irlanda de participar en algunas de las disposiciones del acervo de Schengen (DO L 64 de 7.3.2002, p. 20).

[66] DO L 176 de 10.7.1999, p. 36.

[67] DO L 176 de 10.7.1999, p. 31.

[68] DO L 53 de 27.2.2008, p. 52.

[69] DO L 53 de 27.2.2008, p. 1.

[70] DO L 160 de 18.6.2011, p. 21.

[71] DO L 160 de 18.6.2011, p. 19.

[72] Decisión 2010/365/UE del Consejo, de 29 de junio de 2010, relativa a la aplicación de las disposiciones del acervo de Schengen sobre el Sistema de Información de Schengen en la República de Bulgaria y Rumanía (DO L 166 de 1.7.2010, p. 17).

[73] Decisión (UE) 2017/1908 del Consejo, de 12 de octubre de 2017, relativa a la puesta en aplicación de determinadas disposiciones del acervo de Schengen relacionadas con el Sistema de Información de Visados en la República de Bulgaria y Rumanía (DO L 269 de 19.10.2017, p. 39).

(76) En lo que respecta a Croacia, las disposiciones relacionadas con el SIS y el VIS constituyen disposiciones que desarrollan el acervo de Schengen o están relacionadas con él en el sentido del artículo 4, apartado 2, del Acta de adhesión de 2011, leído en relación con la Decisión (UE) 2017/733 del Consejo[74].

(77) El presente Reglamento respeta los derechos fundamentales y cumple los principios reconocidos, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea, por lo que debe ser aplicado de conformidad con tales derechos y principios.

(78) A fin de que el presente Reglamento encaje en el marco jurídico vigente, el Reglamento (UE) 2016/399, el Reglamento (UE) 2017/2226, la Decisión 2008/633/JAI del Consejo, el Reglamento (CE) n.º 767/2008 y la Decisión 2004/512/CE del Consejo deben modificarse en consecuencia.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1
Objeto

1. El presente Reglamento, junto con el [Reglamento 2018/xx sobre interoperabilidad, cooperación policial y judicial, asilo y migración], establece un marco para garantizar la interoperabilidad del Sistema de Entradas y Salidas (SES), el Sistema de Información de Visados (VIS), [el Sistema Europeo de Información y Autorización de Viajes (SEIAV)], Eurodac, el Sistema de Información de Schengen (SIS) y [el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)], con el fin de que dichos sistemas y datos se complementen entre sí.

2. El marco incluirá los siguientes componentes de interoperabilidad:

   1) un portal europeo de búsqueda (PEB);

   2) un servicio de correspondencia biométrica compartido (SCB compartido);

   3) un registro común de datos de identidad (RCDI);

   4) un detector de identidades múltiples (DIM).

3. El presente Reglamento establece también disposiciones sobre los requisitos de calidad de los datos, sobre un formato universal de mensajes (UMF) y sobre un repositorio central de presentación de informes y estadísticas (RCIE), además de las responsabilidades de los Estados miembros y de la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), en lo que respecta al diseño y el funcionamiento de los componentes de interoperabilidad.

[74] Decisión (UE) 2017/733 del Consejo, de 25 de abril de 2017, relativa a la aplicación de las disposiciones del acervo de Schengen relativas al Sistema de Información de Schengen en la República de Croacia (DO L 108 de 26.4.2017, p. 31).

4. El presente Reglamento también adapta los procedimientos y condiciones para el acceso de los cuerpos policiales de los Estados miembros y de la Agencia de la Unión Europea para la Cooperación Policial (Europol) al Sistema de Entradas y Salidas (SES), al Sistema de Información de Visados (VIS), [al Sistema Europeo de Información y Autorización de Viajes (SEIAV)] y a Eurodac con fines de prevención, detección e investigación de los delitos de terrorismo u otros delitos graves incluidos en su ámbito de competencias.

Artículo 2
Objetivos de la interoperabilidad

1. Mediante la garantía de la interoperabilidad, el presente Reglamento tendrá los siguientes objetivos:

   a) mejorar la gestión de las fronteras exteriores;

   b) contribuir a la prevención de la migración irregular y a la lucha contra ella;

   c) contribuir a un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, lo que incluye el mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros;

   d) mejorar la aplicación de la política común de visados; y

   e) prestar asistencia en el examen de las solicitudes de protección internacional.

2. Los objetivos de la garantía de la interoperabilidad se alcanzarán:

   a) garantizando la identificación correcta de las personas;

   b) contribuyendo a la lucha contra la usurpación de identidad;

   c) mejorando y armonizando los requisitos de calidad de los datos de los respectivos sistemas de información de la UE;

   d) facilitando la aplicación técnica y operativa por parte de los Estados miembros de los sistemas de información de la UE existentes y futuros;

   e) reforzando, simplificando y uniformizando las condiciones de seguridad de los datos y de protección de datos que rigen en los respectivos sistemas de información de la UE;

   f) racionalizando las condiciones de acceso de los cuerpos policiales al SES, al VIS, [al SEIAV] y a Eurodac;

   g) apoyando los objetivos del SES, el VIS, [el SEIAV], Eurodac, el SIS y [el sistema ECRIS-TCN].

Artículo 3
Ámbito de aplicación

1. El presente Reglamento es aplicable [al Sistema de Entradas y Salidas (SES)], el Sistema de Información de Visados (VIS), [el Sistema Europeo de Información y Autorización de Viajes (SEIAV)] y el Sistema de Información de Schengen (SIS).

2. El presente Reglamento es aplicable a las personas cuyos datos personales puedan ser objeto de tratamiento en los sistemas de información de la UE a que se refiere el apartado 1.

Artículo 4
Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «fronteras exteriores»: las fronteras exteriores tal como se definen en el artículo 2, punto 2, del Reglamento (UE) 2016/399;

2) «inspecciones fronterizas»: las inspecciones fronterizas tal como se definen en el artículo 2, punto 11, del Reglamento (UE) 2016/399;

3) «autoridad fronteriza»: la guardia de fronteras encargada de llevar a cabo las inspecciones fronterizas de conformidad con la normativa nacional;

4) «autoridades de control»: las autoridades de control establecidas de conformidad con el artículo 51, apartado 1, del Reglamento (UE) 2016/679 y las autoridades de control establecidas de conformidad con el artículo 41, apartado 1, punto 1, de la Directiva (UE) 2016/680;

5) «verificación»: el proceso de comparación de conjuntos de datos para establecer la validez de una identidad declarada (control simple);

6) «identificación»: el proceso de determinación de la identidad de una persona por comparación con múltiples conjuntos de datos de una base de datos (control múltiple);

7) «nacional de un tercer país»: cualquier persona que no sea ciudadano de la Unión en el sentido del artículo 20, apartado 1, del Tratado de la Unión Europea, o un apátrida, o una persona con nacionalidad desconocida;

8) «datos alfanuméricos»: datos representados por letras, dígitos, caracteres especiales, espacios y signos de puntuación;

9) «datos de identidad»: los datos a que se refiere el artículo 27, apartado 3, letras a) a h);

10) «datos dactiloscópicos»: los datos relativos a las impresiones dactilares de una persona;

11) «imagen facial»: las imágenes digitales del rostro;

12) «datos biométricos»: los datos dactiloscópicos y la imagen facial;

13) «plantilla biométrica»: una representación matemática obtenida por extracción de características de los datos biométricos, limitada a las características necesarias para llevar a cabo identificaciones y verificaciones;

14) «documento de viaje»: el pasaporte o cualquier otro documento equivalente que permita a su titular cruzar las fronteras exteriores y en el que pueda insertarse el visado;

15) «datos del documento de viaje»: el tipo, el número y el país de expedición del documento de viaje, la fecha de expiración de su validez y el código de tres letras del país de expedición;

16) «autorización de viaje»: la autorización de viaje tal como se define en el artículo 3 del [Reglamento SEIAV];

17) «visado de corta duración»: el visado tal como se define en el artículo 2, punto 2, letra a), del Reglamento (CE) n.º 810/2009;

18) «sistemas de información de la UE»: los sistemas informáticos de gran magnitud gestionados por eu-LISA;

19) «datos de Europol»: los datos personales facilitados a Europol a efectos de lo dispuesto en el artículo 18, apartado 2, letra a), del Reglamento (UE) 2016/794;

20) «bases de datos de Interpol»: la base de datos sobre documentos de viaje robados y perdidos (DVRP) de Interpol y la base de datos de documentos de viaje asociados a notificaciones de Interpol (TDAWN de Interpol);

21) «correspondencia»: la existencia de una coincidencia establecida al comparar dos o más anotaciones de datos personales que hayan sido o estén siendo registrados en un sistema de información o una base de datos;

22) «respuesta positiva»: la confirmación de una o varias correspondencias;

23) «cuerpos policiales»: las «autoridades competentes» tal como se definen en el artículo 3, punto 7, de la Directiva 2016/680;

24) «autoridades designadas»: las autoridades designadas por el Estado miembro a que se refieren el artículo 29, apartado 1, del Reglamento (UE) 2017/2226, el artículo 3, apartado 1, de la Decisión 2008/633/JAI del Consejo, [el artículo 43 del Reglamento SEIAV] y [el artículo 6 del Reglamento Eurodac];

25) «delito de terrorismo»: un delito con arreglo a la legislación nacional que corresponda o sea equivalente a alguno de los delitos a que se refiere la Directiva (UE) 2017/541;

26) «delito grave»: un delito que corresponda o sea equivalente a alguno de los delitos a los que se refiere el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI, si está penado en la legislación nacional con una pena privativa de libertad o de internamiento con una duración máxima no inferior a tres años;

27) «SES»: el Sistema de Entradas y Salidas a que se refiere el Reglamento (UE) 2017/2226;

28) «VIS»: el Sistema de Información de Visados a que se refiere el Reglamento (CE) n.º 767/2008;

29) [«SEIAV»: el Sistema Europeo de Información y Autorización de Viajes a que se refiere el Reglamento SEIAV];

30) «Eurodac»: Eurodac tal como se contempla en el [Reglamento Eurodac];

31) «SIS»: el Sistema de Información de Schengen a que se refieren [el Reglamento sobre el SIS en el ámbito de los controles fronterizos, el Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial y el Reglamento sobre el SIS para el retorno de nacionales de terceros países en situación irregular];

32) [«sistema ECRIS-TCN»: el Sistema Europeo de Información de Antecedentes Penales que contiene información sobre las condenas de nacionales de terceros países y apátridas a que se refiere el Reglamento del sistema ECRIS-TCN];

33) «PEB»: el portal europeo de búsqueda a que se refiere el artículo 6;

34) «SCB compartido»: el servicio de correspondencia biométrica compartido a que se refiere el artículo 15;

35) «RCDI»: el registro común de datos de identidad a que se refiere el artículo 17;

36) «DIM»: el detector de identidades múltiples a que se refiere el artículo 25;

37) «RCIE»: el repositorio central para la presentación de informes y estadísticas a que se refiere el artículo 39.

Artículo 5
No discriminación

El tratamiento de datos personales a los efectos del presente Reglamento no dará lugar a discriminación contra las personas por motivos tales como el sexo, el origen racial o étnico, la religión o las creencias, la discapacidad, la edad o la orientación sexual. Deberá respetar plenamente la dignidad y la integridad humanas. Se prestará especial atención a los niños, las personas mayores y las personas con discapacidad.

CAPÍTULO II
Portal europeo de búsqueda

Artículo 6
Portal europeo de búsqueda

1. Se crea un portal europeo de búsqueda (PEB) con objeto de garantizar que las autoridades de los Estados miembros y los organismos de la Unión Europea tengan un acceso rápido, ininterrumpido, eficiente, sistemático y controlado a los sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol que necesiten para llevar a cabo sus tareas, de conformidad con sus derechos de acceso, así como con objeto de apoyar los objetivos del SES, el VIS, [el SEIAV], Eurodac, el SIS, [el sistema ECRIS-TCN] y los datos de Europol.

2. El PEB se compondrá de:

   a) una infraestructura central, incluido un portal de búsqueda que permita la consulta simultánea del SES, el VIS, [el SEIAV], el SIS, Eurodac y [el sistema ECRIS-TCN], así como de los datos de Europol y las bases de datos de Interpol;

   b) un canal de comunicación seguro entre el PEB, los Estados miembros y los organismos de la UE que tengan derecho a utilizar el PEB de conformidad con la legislación de la Unión;

   c) una infraestructura de comunicación segura entre el PEB y el SES, el VIS, [el SEIAV], Eurodac, el SIS Central, [el sistema ECRIS-TCN], los datos de Europol y las bases de datos de Interpol, así como entre el PEB y las infraestructuras centrales del registro común de datos de identidad (RCDI) y el detector de identidades múltiples.

3. La agencia eu-LISA desarrollará el PEB y garantizará su gestión técnica.

Artículo 7
Utilización del portal europeo de búsqueda

1. La utilización del PEB se reservará a las autoridades de los Estados miembros y los organismos de la UE que tengan acceso al SES, [el SEIAV], el VIS, el SIS, Eurodac

y [el sistema ECRIS-TCN], al RCDI y al detector de identidades múltiples, así como a los datos de Europol y las bases de datos de Interpol de conformidad con la legislación nacional o de la Unión que regule dicho acceso.

2. Las autoridades a que se refiere el apartado 1 utilizarán el PEB para consultar datos relativos a personas o sus documentos de viaje en los sistemas centrales del SES, el VIS y [el SEIAV] de conformidad con los derechos de acceso que les otorguen la legislación nacional y la de la Unión. Asimismo, utilizarán el PEB para consultar el RCDI, de conformidad con sus derechos de acceso con arreglo al presente Reglamento, para los fines mencionados en los artículos 20, 21 y 22.

3. Las autoridades de los Estados miembros a que se refiere el apartado 1 pueden utilizar el PEB para buscar datos relativos a las personas o sus documentos de viaje en el SIS Central a que se refieren el [Reglamento sobre el SIS en el ámbito de los controles fronterizos y el Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial]. El acceso al SIS Central mediante el PEB se realizará mediante el sistema nacional (N.SIS) de cada Estado miembro, de conformidad con el [artículo 4, apartado 2, del Reglamento sobre el SIS en el ámbito de los controles fronterizos y el Reglamento sobre el SIS en el ámbito de la cooperación judicial y policial].

4. Los organismos de la UE utilizarán el PEB para consultar datos relativos a personas o sus documentos de viaje en el SIS Central.

5. Las autoridades a que se refiere el apartado 1 utilizarán el PEB para consultar datos relativos a personas o sus documentos de viaje en las bases de datos de Interpol, de conformidad con los derechos de acceso que les otorguen la legislación nacional y la de la Unión.

Artículo 8
Perfiles de los usuarios del portal europeo de búsqueda

1. A los efectos de permitir el uso del PEB, eu-LISA creará un perfil para cada categoría de usuario del PEB, de conformidad con los detalles técnicos y derechos de acceso a que se refiere el apartado 2, que incluya, de conformidad con la legislación de la Unión y nacional:

   a) los campos de datos que deberán utilizarse para llevar a cabo una consulta;

   b) los sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol que deban y puedan consultarse y que proporcionen una respuesta al usuario, y

   c) los datos facilitados en cada respuesta.

2. La Comisión adoptará actos delegados de conformidad con el artículo 63 para especificar los detalles técnicos de los perfiles a que se refiere el apartado 1 en relación con los usuarios del PEB a que se refiere el artículo 7, apartado 1, de conformidad con sus derechos de acceso.

Artículo 9
Consultas

1. Los usuarios del PEB iniciarán una consulta mediante la introducción de datos en el PEB, de conformidad con su perfil de usuario y derechos de acceso. Cuando se haya

iniciado una consulta, el PEB consultará al mismo tiempo, conforme a los datos introducidos por el usuario del PEB, el SES*, [el SEIAV], el VIS, el SIS, Eurodac, [el sistema ECRIS-TCN] y el RCDI, así como los datos de Europol y las bases de datos de Interpol.*

2. Los campos de datos utilizados para iniciar una consulta a través del PEB corresponderán a los campos de datos relacionados con personas o documentos de viaje que puedan utilizarse para consultar los distintos sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol, de conformidad con los instrumentos jurídicos que los regulen.

3. La agencia eu-LISA desarrollará un documento de control de interfaces (DCI) sobre la base del UMF a que se refiere el artículo 38 para el PEB.

4. El SES, [el SEIAV], el VIS, el SIS, Eurodac, [el sistema ECRIS-TCN], el RCDI y el detector de identidades múltiples, así como los datos de Europol y *las bases de datos de Interpol*, proporcionarán los datos contenidos en ellos que se obtengan de la consulta del PEB.

5. Cuando se consulten las bases de datos de Interpol, el diseño del PEB garantizará que los datos utilizados por el usuario del PEB para iniciar una consulta no se compartan con los propietarios de los datos de Interpol.

6. La respuesta al usuario del PEB será única y contendrá todos los datos a los que tenga acceso el usuario de conformidad con la legislación de la Unión. En caso necesario, la respuesta facilitada por el PEB indicará a qué sistema de información o base de datos pertenecen los datos.

7. La Comisión adoptará un acto delegado, de conformidad con el artículo 63, para especificar el contenido y el formato de las respuestas del PEB.

Artículo 10
Conservación de registros

1. Sin perjuicio del [artículo 46 del Reglamento SES], el artículo 34 del Reglamento (CE) n.º 767/2008, [el artículo 59 de la propuesta del SEIAV] y los artículos 12 y 18 del Reglamento sobre el SIS en el ámbito de los controles fronterizos, eu-LISA conservará los registros de todas las operaciones de tratamiento de datos dentro del PEB. Dichos registros incluirán, en particular, lo siguiente:

   a) la autoridad del Estado miembro y el usuario individual del PEB, incluido el perfil de usuario del PEB utilizado, conforme a lo dispuesto en el artículo 8;

   b) la fecha y hora de la consulta;

   c) los sistemas de información de la UE y las bases de datos de Interpol consultados;

   d) la marca identificadora de la persona que haya realizado la consulta, de conformidad con las normas nacionales o, cuando proceda, con el Reglamento (UE) n.º 45/2001.

2. Los registros únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de los requisitos de la consulta y de la legalidad del tratamiento de datos, y para la garantía de la seguridad de los datos de conformidad con el artículo 42. Dichos registros estarán protegidos

por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación, salvo que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo.

Artículo 11
Procedimientos alternativos en caso de imposibilidad técnica de utilizar el portal europeo de búsqueda

1. Cuando por un fallo del PEB resulte técnicamente imposible utilizar el PEB para consultar uno o varios de los sistemas de información de la UE a que se refiere el artículo 9, apartado 1, o el RCDI, eu-LISA lo notificará a los usuarios del PEB.

2. Cuando por un fallo de la infraestructura nacional de un Estado miembro resulte técnicamente imposible utilizar el PEB para consultar uno o varios de los sistemas de información de la UE a que se refiere el artículo 9, apartado 1, o el RCDI, la autoridad competente de ese Estado miembro lo notificará a eu-LISA y a la Comisión.

3. En ambos casos, y hasta que el fallo técnico quede resuelto, no será de aplicación la obligación a que se refiere el artículo 7, apartados 2 y 4, y los Estados miembros podrán acceder a los sistemas de información a que se refiere el artículo 9, apartado 1, o al RCDI directamente, utilizando sus respectivas interfaces nacionales uniformes o sus infraestructuras de comunicación nacionales.

CAPÍTULO III
Servicio de correspondencia biométrica compartido

Artículo 12
Servicio de correspondencia biométrica compartido

1. Se crea un servicio de correspondencia biométrica compartido (SCB compartido), que almacenará plantillas biométricas y permitirá consultar datos biométricos a través de varios sistemas de información de la UE, a efectos de apoyar al RCDI y al detector de identidades múltiples y los objetivos del SES, el VIS, Eurodac, el SIS y [el sistema ECRIS-TCN].

2. El SCB compartido se compondrá de:

   a) una infraestructura central, incluidos un motor de búsqueda y el almacenamiento de los datos a que se refiere el artículo 13;

   b) una infraestructura de comunicación segura entre el SCB compartido, el SIS Central y el RCDI.

3. La agencia eu-LISA desarrollará el SCB compartido y garantizará su gestión técnica.

Artículo 13
Datos almacenados en el servicio de correspondencia biométrica compartido

1. El SCB compartido almacenará las plantillas biométricas que obtenga de los siguientes datos biométricos:

a) los datos a que se refieren el artículo 16, apartado 1, letra d), y el artículo 17, apartado 1, letras b) y c), del Reglamento (UE) 2017/2226;

b) los datos a que se refiere el artículo 9, apartado 6, del Reglamento (CE) n.º 767/2008;

c) [los datos a que se refiere el artículo 20, apartado 2, letras w) y x), del Reglamento sobre el SIS en el ámbito de los controles fronterizos;

d) los datos a que se refiere el artículo 20, apartado 3, letras w) y x), del Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial;

e) los datos a que se refiere el artículo 4, apartado 3, letras t) y u), del Reglamento sobre el SIS para el retorno de nacionales de terceros países en situación irregular];

f) [los datos a que se refiere el artículo 13, letra a), del Reglamento Eurodac];

g) [los datos a que se refieren el artículo 5, apartado 1, letra b), y el artículo 5, apartado 2, del Reglamento ECRIS-TCN].

2. El SCB compartido incluirá en cada plantilla biométrica una referencia a los sistemas de información en los que se almacenen los datos biométricos correspondientes.

3. Las plantillas biométricas solo podrán introducirse en el SCB compartido tras un control de calidad automatizado de los datos biométricos añadidos a uno de los sistemas de información con que cuenta el SCB compartido para cerciorarse de que se alcanza un estándar mínimo de calidad de los datos.

4. El almacenamiento de los datos mencionados en el apartado 1 cumplirá los estándares de calidad a que se refiere el artículo 37, apartado 2.

Artículo 14

Búsqueda de datos biométricos con el servicio de correspondencia biométrica compartido

A fin de buscar los datos biométricos almacenados en el RCDI y el SIS, estos utilizarán las plantillas biométricas almacenadas en el SCB compartido. Las consultas con datos biométricos tendrán lugar de conformidad con los fines previstos en el presente Reglamento y en el Reglamento SES, el Reglamento VIS, el Reglamento Eurodac, los [Reglamentos sobre el SIS] y [el Reglamento ECRIS-TCN].

Artículo 15

Conservación de datos en el servicio de correspondencia biométrica compartido

Los datos a que se refiere el artículo 13 quedarán almacenados en el SCB compartido tanto tiempo como los datos biométricos correspondientes estén almacenados en el RCDI o en el SIS.

Artículo 16

Conservación de registros

1. Sin perjuicio del [artículo 46 del Reglamento SES], el artículo 34 del Reglamento (CE) n.º 767/2008 y [los artículos 12 y 18 del Reglamento sobre el SIS en al ámbito de la cooperación policial y judicial], eu-LISA conservará los registros de todas las

operaciones de tratamiento de datos en el SCB compartido. Dichos registros incluirán, en particular, lo siguiente:

a) el historial de la creación y el almacenamiento de las plantillas biométricas;

b) una referencia a los sistemas de información de la UE consultados con las plantillas biométricas almacenadas en el SCB compartido;

c) la fecha y hora de la consulta;

d) el tipo de datos biométricos utilizados para iniciar la consulta;

e) la duración de la consulta;

f) los resultados de la consulta y la fecha y hora de los resultados.

g) la marca identificadora de la persona que haya realizado la consulta, de conformidad con las normas nacionales o, cuando proceda, con el Reglamento (UE) n.º 45/2001.

2. Los registros únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de los requisitos de la consulta y de la legalidad del tratamiento de datos, y para la garantía de la seguridad de los datos de conformidad con el artículo 42. Dichos registros estarán protegidos por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación, salvo que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo. Los registros a que se refiere el apartado 1, letra a), se suprimirán una vez que los datos se supriman.

CAPÍTULO IV
Registro común de datos de identidad

Artículo 17
Registro común de datos de identidad

1. Se crea un registro común de datos de identidad (RCDI), que creará un expediente individual para cada persona registrada en el SES, el VIS, [el SEIAV], Eurodac o [el sistema ECRIS-TCN] y contendrá los datos a que se refiere el artículo 18, con el fin de facilitar la identificación correcta de las personas registradas en el SES, el VIS, [el SEIAV], Eurodac y [el sistema ECRIS-TCN] y ayudar a ella, de apoyar el funcionamiento del detector de identidades múltiples y de facilitar y racionalizar el acceso de los cuerpos policiales a los sistemas de información no policiales a escala de la UE, cuando sea necesario con fines de prevención, investigación, detección o enjuiciamiento de delitos graves.

2. El RCDI se compondrá de:

a) una infraestructura central que sustituirá a los sistemas centrales del SES, el VIS, [el SEIAV], Eurodac y [el sistema ECRIS-TCN], respectivamente, en la medida en que deberá almacenar los datos a que se refiere el artículo 18;

b) un canal de comunicación seguro entre el RCDI, los Estados miembros y los organismos de la UE que tengan derecho a utilizar el portal europeo de búsqueda (PEB) de conformidad con la legislación de la Unión;

c) una infraestructura de comunicación segura entre el RCDI y el SES, [el SEIAV], el VIS, Eurodac y [el sistema ECRIS-TCN], así como las infraestructuras centrales del PEB, el SCB compartido y el detector de identidades múltiples.

3. La agencia eu-LISA desarrollará el RCDI y garantizará su gestión técnica.

Artículo 18
Datos del registro común de datos de identidad

1. El RCDI almacenará, separados de un modo lógico, los siguientes datos, según el sistema de información del que provengan:

a) los datos a que se refieren [el artículo 16, apartado 1, letras a) a d), y el artículo 17, apartado 1, letras a) a c), del Reglamento SES];

b) los datos a que se refiere el artículo 9, apartado 4, letras a) a c), apartado 5 y apartado 6, del Reglamento (CE) n.º 767/2008;

c) [los datos a que se refiere el artículo 15, apartado 2, letras a) a e), del Reglamento SEIAV;]

d) – (no procede);

e) – (no procede).

2. Para cada conjunto de datos contemplado en el apartado 1, el RCDI incluirá una referencia a los sistemas de información a los que los datos pertenecen.

3. El almacenamiento de los datos mencionados en el apartado 1 cumplirá los estándares de calidad a que se refiere el artículo 37, apartado 2.

Artículo 19
Adición, modificación y eliminación de datos en el registro común de datos de identidad

1. Cuando se añadan, modifiquen o eliminen datos en el SES, el VIS y [el SEIAV], los datos contemplados en el artículo 18 almacenados en el expediente individual del RCDI se añadirán, modificarán o eliminarán en consecuencia, de forma automatizada.

2. Cuando el detector de identidades múltiples cree un vínculo blanco o rojo, de conformidad con lo dispuesto en los artículos 32 y 33, entre los datos de dos o más de los sistemas de información de la UE que constituyen el RCDI, el RCDI añadirá los nuevos datos al expediente individual de los datos vinculados, en lugar de crear un nuevo expediente individual.

Artículo 20
Acceso al registro común de datos de identidad a efectos de identificación

1. Cuando las medidas legislativas nacionales a que se refiere el apartado 2 faculten a los cuerpos policiales de un Estado miembro, dichas autoridades podrán, únicamente para fines de identificación de una persona, consultar el RCDI con los datos biométricos de la persona tomados durante un control de identidad.

Cuando la búsqueda ponga de manifiesto que los datos de esa persona están almacenados en el RCDI, las autoridades de los Estados miembros tendrán acceso para consultar los datos a que se refiere el artículo 18, apartado 1.

Cuando no puedan utilizarse los datos biométricos de la persona o cuando la consulta de esos datos sea infructuosa, la consulta se llevará a cabo con los datos de identidad de dicha persona en combinación con los datos del documento de viaje, o con los datos de identidad facilitados por esa persona.

2. Los Estados miembros que deseen acogerse a la posibilidad prevista en el presente artículo adoptarán medidas legislativas nacionales al efecto. Esas medidas legislativas especificarán los objetivos precisos de los controles de identidad dentro de los fines mencionados en el artículo 2, apartado 1, letras b) y c). Designarán a los cuerpos policiales competentes y establecerán los procedimientos, condiciones y criterios de dichos controles.

Artículo 21

Acceso al registro común de datos de identidad para la detección de identidades múltiples

1. Cuando una consulta del RCDI resulte en un vínculo amarillo de conformidad con el artículo 28, apartado 4, la autoridad responsable de la verificación de identidades diferentes, determinada de conformidad con el artículo 29, podrá acceder, únicamente a efectos de dicha verificación, a los datos de identidad almacenados en el RCDI pertenecientes a los distintos sistemas de información conectados a un vínculo amarillo.

2. Cuando una consulta del RCDI resulte en un vínculo rojo de conformidad con el artículo 32, las autoridades a que se refiere el artículo 26, apartado 2, podrán acceder, únicamente a efectos de combatir la usurpación de identidad, a los datos de identidad almacenados en el RCDI pertenecientes a los distintos sistemas de información conectados a un vínculo rojo.

Artículo 22

Consulta del registro común de datos de identidad con fines policiales

1. Las autoridades designadas de los Estados miembros y Europol podrán consultar el RCDI con fines de prevención, detección e investigación de los delitos de terrorismo u otros delitos graves en un caso específico y a fin de obtener información sobre la existencia de datos relativos a una persona concreta en el SES, el VIS y [el SEIAV].

2. Las autoridades designadas de los Estados miembros y Europol no estarán facultadas para consultar datos pertenecientes al [sistema ECRIS-TCN] al consultar el RCDI para los fines enumerados en el apartado 1.

3. Cuando, en respuesta a una consulta, el RCDI indique que existen datos sobre esa persona en el SES, el VIS y [el SEIAV], el RCDI proporcionará a las autoridades designadas de los Estados miembros y a Europol una respuesta en forma de referencia que indique cuál de los sistemas de información contiene los datos objeto de correspondencia a que se refiere el artículo 18, apartado 2. El RCDI responderá de tal manera que la seguridad de los datos no se vea comprometida.

4. El pleno acceso a los datos contenidos en los sistemas de información de la UE para los fines de prevención, detección e investigación de los delitos de terrorismo u otros delitos graves seguirá estando sujeto a las condiciones y los procedimientos establecidos en los respectivos instrumentos legislativos que regulen dicho acceso.

Artículo 23
Conservación de los datos en el registro común de datos de identidad

1. Los datos a que se refiere el artículo 18, apartados 1 y 2, se eliminarán del RCDI de conformidad con las disposiciones de conservación de los datos del [Reglamento SES], el Reglamento VIS y el [Reglamento SEIAV], respectivamente.

2. El expediente individual se almacenará en el RCDI durante el mismo tiempo que los datos correspondientes permanezcan almacenados en al menos uno de los sistemas de información cuyos datos estén contenidos en el RCDI. La creación de un vínculo no afectará al periodo de conservación de cada uno de los datos vinculados.

Artículo 24
Conservación de registros

1. Sin perjuicio de lo dispuesto en el [artículo 46 del Reglamento SES], el artículo 34 del Reglamento (CE) n.º 767/2008 y [el artículo 59 de la propuesta del SEIAV], eu-LISA conservará los registros de todas las operaciones de tratamiento de datos dentro del RCDI de conformidad con los apartados 2, 3 y 4.

2. En lo que respecta al acceso al RCDI con arreglo al artículo 20, eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el RCDI. Dichos registros incluirán, en particular, lo siguiente:

   a) la finalidad del acceso del usuario que realice la consulta a través del RCDI;

   b) la fecha y hora de la consulta;

   c) el tipo de datos utilizados para iniciar la consulta;

   d) los resultados de la consulta;

   e) la marca identificadora de la persona que haya realizado la consulta, de conformidad con las normas nacionales, con el Reglamento (UE) 2016/794 o, cuando proceda, con el Reglamento (UE) n.º 45/2001.

3. En lo que respecta al acceso al RCDI con arreglo al artículo 21, eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el RCDI. Dichos registros incluirán, en particular, lo siguiente:

   a) la finalidad del acceso del usuario que realice la consulta a través del RCDI;

   b) la fecha y hora de la consulta;

   c) cuando proceda, el tipo de datos utilizados para iniciar la consulta;

   d) cuando proceda, los resultados de la consulta;

   e) la marca identificadora de la persona que haya realizado la consulta, de conformidad con las normas nacionales, con el Reglamento (UE) 2016/794 o, cuando proceda, con el Reglamento (UE) n.º 45/2001.

4. En lo que respecta al acceso al RCDI con arreglo al artículo 22, eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el RCDI. Dichos registros incluirán, en particular, lo siguiente:

   a) el número de referencia del expediente nacional;

   b) la fecha y hora de la consulta;

   c) el tipo de datos utilizados para iniciar la consulta;

   d) los resultados de la consulta;

   e) el nombre de la autoridad que consulte el RCDI;

   f) la marca identificadora del funcionario que haya realizado la consulta y la del funcionario que la haya ordenado, de conformidad con las normas nacionales, el Reglamento (UE) 2016/794 o, cuando proceda, el Reglamento (UE) n.º 45/2001.

   La autoridad de control competente, determinada de conformidad con el artículo 51 del Reglamento (UE) 2016/679 o con el artículo 41 de la Directiva 2016/680, verificará periódicamente los registros de dichos accesos, a intervalos no superiores a seis meses, con el fin de cerciorarse del cumplimiento de los procedimientos y condiciones establecidos en el artículo 22, apartados 1 a 3.

5. Cada Estado miembro conservará los registros de las consultas del personal debidamente autorizado para utilizar el RCDI con arreglo a los artículos 20, 21 y 22.

6. Los registros contemplados en los apartados 1 y 5 únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de las condiciones de la solicitud y de la legalidad del tratamiento de datos, y para la garantía de la seguridad de los datos de conformidad con el artículo 42. Dichos registros estarán protegidos por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación, salvo que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo.

7. La agencia eu-LISA conservará los registros relacionados con el historial de los datos almacenados en un expediente individual para los fines mencionados en el apartado 6. Los registros relacionados con el historial de los datos almacenados se suprimirán una vez que se hayan suprimido esos datos.

CAPÍTULO V
Detector de identidades múltiples

Artículo 25
Detector de identidades múltiples

1. A fin de apoyar el funcionamiento del RCDI y la consecución de los objetivos del SES, el VIS, [el SEIAV], Eurodac, el SIS y [el sistema ECRIS-TCN], se crea un detector de identidades múltiples (DIM), que generará y almacenará vínculos entre los datos de los sistemas de información de la UE incluidos en el registro común de datos de identidad (RCDI) y el SIS y, como consecuencia de ello, detectará identidades múltiples con el doble objetivo de facilitar los controles de identidad y combatir la usurpación de identidad.

2. El DIM se compondrá de:

a) una infraestructura central, que almacenará los vínculos y las referencias a los sistemas de información;

b) una infraestructura de comunicación segura que conecte el DIM con el SIS y las infraestructuras centrales del portal europeo de búsqueda y el RCDI.

3. La agencia eu-LISA desarrollará el DIM y garantizará su gestión técnica.

Artículo 26
Acceso al detector de identidades múltiples

4. A los efectos de la verificación manual de la identidad a que se refiere el artículo 29, se concederá el acceso a los datos contemplados en el artículo 34 almacenados en el DIM a:

a) las autoridades fronterizas, cuando creen o actualicen un expediente individual tal como se establece en el artículo 14 del [Reglamento SES];

b) las autoridades competentes a que se refiere el artículo 6, apartados 1 y 2, del Reglamento 767/2008, cuando creen o actualicen un expediente de solicitud en el VIS, de conformidad con el artículo 8 del Reglamento (CE) n.º 767/2008;

c) [la unidad central SEIAV y las unidades nacionales SEIAV, cuando lleven a cabo la evaluación contemplada en los artículos 20 y 22 del Reglamento SEIAV;]

d) – (no procede);

e) las oficinas SIRENE del Estado miembro que cree una [descripción en el SIS de conformidad con el Reglamento sobre el SIS en el ámbito de las inspecciones fronterizas];

f) – (no procede).

5. Las autoridades de los Estados miembros y los organismos de la UE que tengan acceso a, como mínimo, un sistema de información de la UE incluido en *el registro común de datos de identidad o al SIS* tendrán acceso a los datos a que se refiere el artículo 34, letras a) y b), en lo relativo a los vínculos rojos según lo dispuesto en el artículo 32.

Artículo 27
Detector de identidades múltiples

1. Se iniciará una detección de identidades múltiples en el registro común de datos de identidad y el SIS cuando:

a) se cree o actualice un expediente individual en [el SES de conformidad con el artículo 14 del Reglamento SES];

b) se cree o actualice un expediente individual en el VIS de conformidad con el artículo 8 del Reglamento (CE) n.º 767/2008;

c) [se cree o actualice un expediente de solicitud en el SEIAV de conformidad con el artículo 17 del Reglamento SEIAV];

d) – (no procede);

e) [se cree o actualice una descripción sobre una persona en el SIS de conformidad con el capítulo V del Reglamento sobre el SIS en el ámbito de las inspecciones fronterizas];

f) – (no procede).

2. Cuando los datos contenidos en un sistema de información mencionado en el apartado 1 contengan datos biométricos, el registro común de datos de identidad (RCDI) y el SIS Central utilizarán el servicio de correspondencia biométrica compartido (SCB compartido) para realizar la detección de identidades múltiples. El SCB compartido comparará las plantillas biométricas obtenidas a partir de cualquier nuevo dato biométrico con las plantillas biométricas ya contenidas en el SCB compartido, con el fin de verificar si los datos pertenecientes a un mismo nacional de un tercer país están ya almacenados en el RDCI o en el SIS Central.

3. Además del proceso mencionado en el apartado 2, el RDCI y el SIS Central utilizarán el portal europeo de búsqueda para buscar los datos almacenados en ellos, utilizando los datos siguientes:

(a) apellido(s), nombre(s) (de pila), fecha de nacimiento, sexo y nacionalidad(es) tal como se definen en el artículo 16, apartado 1, letra a), del [Reglamento SES];

(b) apellido(s), nombre(s) (de pila), fecha de nacimiento, sexo y nacionalidad(es) tal como se definen en el artículo 9, apartado 4, letra a), del Reglamento (CE) n.º 767/2008;

(c) [apellido(s), nombre(s) (de pila), apellido (s) de nacimiento, fecha de nacimiento, lugar de nacimiento y nacionalidad(es) tal como se definen en el artículo 15, apartado 2, del Reglamento SEIAV;]

(d) – (no procede);

(e) [apellido (s); nombre (s); apellido(s) de soltero, nombres usados con anterioridad y alias; fecha de nacimiento, lugar de nacimiento, nacionalidad(es) y sexo tal como se definen en el artículo 20, apartado 2, del Reglamento sobre el SIS en el ámbito de los controles fronterizos;]

(f) – (no procede);

(g) – (no procede);

(h) – (no procede).

4. La detección de identidades múltiples únicamente se iniciará con el fin de comparar los datos disponibles en un sistema de información con los datos disponibles en otros sistemas de información.

Artículo 28
Resultados de la detección de identidades múltiples

1. Si las consultas a que se refiere el artículo 27, apartados 2 y 3, no dan lugar a ninguna respuesta positiva, los procedimientos a que se refiere el artículo 27, apartado 1, continuarán de conformidad con los Reglamentos respectivos por los que se rigen.

2. Cuando la consulta establecida en el artículo 27, apartados 2 y 3, dé lugar a una o más respuestas positivas, el registro común de datos de identidad y, cuando proceda,

el SIS crearán un vínculo entre los datos utilizados para iniciar la consulta y los datos que hayan dado lugar a la respuesta positiva.

Cuando se registren varias respuestas positivas, se creará un vínculo entre todos los datos que hayan dado lugar a una respuesta positiva. Cuando los datos estén vinculados previamente, el vínculo existente se extenderá a los datos utilizados para iniciar la consulta.

3. Cuando la consulta a que se refiere el artículo 27, apartados 2 o 3, dé lugar a una o varias respuestas positivas y los datos de identidad de los expedientes vinculados sean idénticos o similares, se creará un vínculo blanco de conformidad con el artículo 33.

4. Cuando la consulta a que se refiere el artículo 27, apartados 2 o 3, dé lugar a una o varias respuestas positivas y los datos de identidad de los expedientes vinculados no puedan considerarse similares, se creará un vínculo amarillo de conformidad con el artículo 30 y será de aplicación el procedimiento a que se refiere el artículo 29.

5. La Comisión establecerá mediante actos de ejecución los procedimientos para determinar los casos en que los datos de identidad puedan considerarse idénticos o similares. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 64, apartado 2.

6. Los vínculos se almacenarán en el expediente de confirmación de identidad a que se refiere el artículo 34.

La Comisión establecerá mediante actos de ejecución las normas técnicas para vincular los datos de los distintos sistemas de información. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 64, apartado 2.

Artículo 29
Verificación manual de identidades diferentes

1. Sin perjuicio de lo dispuesto en el apartado 2, la autoridad responsable de la verificación de identidades diferentes será:

   a) la autoridad fronteriza, en caso de respuestas positivas que se produzcan al crear o actualizar un expediente individual en [el SES de conformidad con el artículo 14 del Reglamento SES];

   b) las autoridades competentes a que se refiere el artículo 6, apartados 1 y 2, del Reglamento 767/2008, en caso de respuestas positivas que se produzcan al crear o actualizar un expediente de solicitud en el VIS, de conformidad con el artículo 8 del Reglamento (CE) n.º 767/2008;

   c) [la unidad central SEIAV y las unidades nacionales SEIAV, en caso de respuestas positivas que se produzcan con arreglo a los artículos 18, 20 y 22 del Reglamento SEIAV;]

   d) – (no procede);

   e) las oficinas SIRENE del Estado miembro, en caso de respuestas positivas que se produzcan al crear una descripción en el SIS con arreglo al [Reglamento sobre el SIS en el ámbito de los controles fronterizos];

   f) – (no procede).

El detector de identidades múltiples indicará la autoridad responsable de la verificación de las identidades diferentes que figuren en el expediente de verificación de identidad.

2. La autoridad responsable de la verificación de las identidades diferentes en el expediente de confirmación de identidad será la oficina SIRENE del Estado miembro que haya creado la descripción, cuando se cree un vínculo a los datos contenidos:

   (a) en una descripción al respecto de personas buscadas para su detención o a efectos de su entrega o extradición, según lo dispuesto en el artículo 26 del [Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial];

   (b) en una descripción al respecto de personas desaparecidas o vulnerables, según lo dispuesto en el artículo 32 del [Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial];

   (c) en una descripción al respecto de personas buscadas para su participación en un proceso judicial, según lo dispuesto en el artículo 34 del [Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial];

   (d) [en una descripción sobre retorno de conformidad con el Reglamento sobre el SIS para el retorno de nacionales de terceros países en situación irregular];

   (e) en una descripción al respecto de personas para controles discretos, controles de investigación o controles específicos, según lo dispuesto en el artículo 36 del [Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial];

   (f) en una descripción al respecto de personas buscadas para su identificación con arreglo a la legislación nacional y búsqueda mediante datos biométricos, según lo dispuesto en el artículo 40 del [Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial].

3. Sin perjuicio de lo dispuesto en el apartado 4, la autoridad responsable de la verificación de las identidades diferentes tendrá acceso a los datos contenidos en el expediente de confirmación de identidad pertinente y a los datos de identidad vinculados en el registro común de datos de identidad, así como, cuando proceda, en el SIS, y evaluará las diferentes identidades, actualizará el vínculo en consonancia con los artículos 31, 32 y 33 y lo añadirá sin demora al expediente de confirmación de identidad.

4. Cuando la autoridad responsable de la verificación de las identidades diferentes en el expediente de confirmación de identidad sea la autoridad fronteriza que cree o actualice un expediente individual en el SES de conformidad con el artículo 14 del Reglamento SES, y se obtenga un vínculo amarillo, la autoridad fronteriza llevará a cabo verificaciones adicionales en el marco de una inspección de segunda línea. Durante esta inspección de segunda línea, las autoridades fronterizas tendrán acceso a los datos contenidos en el expediente de confirmación de identidad correspondiente, actualizarán el vínculo de conformidad con los artículos 31 a 33 y lo añadirán sin demora al expediente de confirmación de identidad.

5. Cuando se obtenga más de un vínculo, la autoridad responsable de la verificación de las identidades diferentes evaluará cada uno por separado.

6. Cuando los datos que den lugar a una respuesta positiva estén previamente vinculados, la autoridad responsable de la verificación de las identidades diferentes tendrá en cuenta los vínculos existentes al evaluar la creación de nuevos vínculos.

Artículo 30
Vínculo amarillo

1. Un vínculo entre datos procedentes de dos o más sistemas de información se clasificará como amarillo en cualquiera de los siguientes casos:

   a) cuando los datos vinculados compartan los mismos datos biométricos, pero distintos datos de identidad, y no haya tenido lugar una verificación manual de identidades diferentes;

   b) cuando los datos vinculados contengan distintos datos de identidad y no haya tenido lugar una verificación manual de identidades diferentes.

2. Cuando un vínculo se clasifique como amarillo con arreglo a lo dispuesto en el apartado 1, será de aplicación el procedimiento previsto en el artículo 29.

Artículo 31
Vínculo verde

1. Un vínculo entre datos procedentes de dos o más sistemas de información se clasificará como verde cuando los datos vinculados no compartan los mismos datos de identidad biométricos, pero contengan datos de identidad similares y la autoridad responsable de la verificación de las identidades diferentes concluya que hacen referencia a dos personas distintas.

2. Cuando se consulten el registro común de datos de identidad (RCDI) o el SIS y exista un vínculo verde entre dos o más de los sistemas de información que constituyen el RCDI o con el SIS, el detector de identidades múltiples indicará que los datos de identidad de los datos vinculados no corresponden a la misma persona. El sistema de información consultado responderá indicando únicamente los datos de la persona cuyos datos se hayan utilizado para la consulta, sin registrar una respuesta positiva en relación con los datos sujetos al vínculo verde.

Artículo 32
Vínculo rojo

1. Un vínculo entre datos procedentes de dos o más sistemas de información se clasificará como rojo en cualquiera de los siguientes casos:

   a) cuando los datos vinculados compartan los mismos datos biométricos, pero distintos datos de identidad, y la autoridad responsable de la verificación de las identidades diferentes concluya que hacen referencia de manera ilegal a la misma persona;

   b) cuando los datos vinculados compartan datos de identidad similares y la autoridad responsable de la verificación de las identidades diferentes concluya que hacen referencia de manera ilegal a la misma persona.

2. Cuando se consulten el registro común de datos de identidad (RCDI) o el SIS y exista un vínculo rojo entre dos o más de los sistemas de información que

constituyen el RCDI o con el SIS, el detector de identidades múltiples responderá indicando los datos a que se refiere el artículo 34. Las actuaciones subsiguientes a un vínculo rojo se realizarán de conformidad con la legislación nacional y de la Unión.

3. Cuando se cree un vínculo rojo entre datos del SES, el VIS, [el SEIAV], Eurodac o [el sistema ECRIS-TCN], se actualizará el expediente individual almacenado en el RCDI de conformidad con el artículo 19, apartado 1.

4. Sin perjuicio de las disposiciones relativas al tratamiento de las descripciones en el SIS a que se hace referencia en los [Reglamentos sobre el SIS en el ámbito de los controles fronterizos, en el ámbito de la cooperación policial y judicial y para el retorno de los nacionales de terceros países en situación irregular], y sin perjuicio de las limitaciones necesarias para proteger la seguridad y el orden público, prevenir la delincuencia y garantizar que ninguna investigación nacional corra peligro, cuando se cree un vínculo rojo, la autoridad encargada de la verificación de las identidades diferentes informará a la persona de la existencia ilegal de múltiples identidades.

5. Cuando se genere un vínculo rojo, la autoridad responsable de la verificación de las identidades diferentes facilitará una referencia a las autoridades responsables de los datos vinculados.

Artículo 33
Vínculo blanco

1. Un vínculo entre datos procedentes de dos o más sistemas de información se clasificará como blanco en cualquiera de los siguientes casos:

   a) cuando los datos vinculados compartan los mismos datos biométricos y los mismos o similares datos de identidad;

   b) cuando los datos vinculados compartan los mismos o similares datos de identidad y al menos uno de los sistemas de información no contenga datos biométricos de la persona;

   c) cuando los datos vinculados compartan los mismos datos biométricos, pero distintos datos de identidad, y la autoridad responsable de verificar las identidades diferentes concluya que hacen referencia a una misma persona que posee distintos datos de identidad de manera legal.

2. Cuando se consulten el RCDI o el SIS y exista un vínculo blanco entre dos o más de los sistemas de información que constituyen el RCDI o con el SIS, el detector de identidades múltiples indicará que los datos de identidad de los datos vinculados corresponden a la misma persona. Los sistemas de información consultados responderán indicando, si procede, todos los datos vinculados relativos a la persona y, por lo tanto, produciendo una respuesta positiva en relación con los datos sujetos al vínculo blanco, cuando la autoridad que inicie la consulta tenga acceso a los datos vinculados con arreglo a la legislación nacional o de la Unión.

3. Cuando se cree un vínculo blanco entre datos del SES, el VIS, [el SEIAV], Eurodac o [el sistema ECRIS-TCN], se actualizará el expediente individual almacenado en el RCDI de conformidad con el artículo 19, apartado 1.

4. Sin perjuicio de las disposiciones relativas al tratamiento de las descripciones en el SIS a que se hace referencia en los [Reglamentos sobre el SIS en el ámbito de los controles fronterizos, en el ámbito de la cooperación policial y judicial y para el retorno de los nacionales de terceros países en situación irregular], cuando se genere

un vínculo blanco a raíz de una verificación manual de identidades múltiples, la autoridad responsable de la verificación de las identidades diferentes informará a la persona de la existencia de discrepancias entre sistemas en lo que atañe a sus datos personales y facilitará una referencia a las autoridades responsables de los datos vinculados.

Artículo 34
Expediente de confirmación de identidad

El expediente de confirmación de identidad contendrá los datos siguientes:

a) los vínculos, incluida su naturaleza en forma de colores, según lo dispuesto en los artículos 30 a 33;

b) una referencia a los sistemas de información cuyos datos estén vinculados;

c) un número de identificación único que permita recuperar de los sistemas de información los datos de los expedientes vinculados correspondientes;

d) en su caso, la autoridad responsable de la verificación de las identidades diferentes.

Artículo 35
Conservación de los datos en el detector de identidades múltiples

Los expedientes de confirmación de identidad y sus datos, incluidos los vínculos, se almacenarán en el detector de identidades múltiples (DIM) únicamente durante el tiempo en que los datos vinculados permanezcan almacenados en dos o más sistemas de información de la UE.

Artículo 36
Conservación de registros

1. La agencia eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el DIM. Dichos registros incluirán, en particular, lo siguiente:

(a) el motivo del acceso del usuario y sus derechos de acceso;

(b) la fecha y hora de la consulta;

(c) el tipo de datos utilizados para iniciar la consulta o consultas;

(d) la referencia a los datos vinculados;

(e) el historial del expediente de confirmación de identidad;

(f) la marca identificadora de la persona que haya realizado la consulta.

2. Cada Estado miembro mantendrá un registro del personal debidamente autorizado para utilizar el DIM.

3. Los registros únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de los requisitos de la solicitud y de la legalidad del tratamiento de datos, y para la garantía de la seguridad

de los datos de conformidad con el artículo 42. Dichos registros estarán protegidos por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación, salvo que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo. Los registros relacionados con el historial del expediente de confirmación de identidad se suprimirán una vez que se haya suprimido dicho expediente.

CAPÍTULO VI
Medidas de apoyo a la interoperabilidad

Artículo 37
Calidad de los datos

1. La agencia eu-LISA establecerá mecanismos y procedimientos automatizados de control de la calidad de los datos almacenados en el SES, el [SEIAV], el VIS, el SIS, el servicio de correspondencia biométrica compartido (SCB compartido), el registro común de datos de identidad (RCDI) y el detector de identidades múltiples (DIM).

2. La agencia eu-LISA establecerá indicadores comunes de calidad de los datos y los estándares mínimos de calidad para el almacenamiento de datos en el SES, el [SEIAV], el VIS, el SIS, el SCB compartido, el RCDI y el DIM.

3. La agencia eu-LISA presentará a los Estados miembros informes periódicos sobre los mecanismos y procedimientos automatizados de control de la calidad de los datos. La agencia eu-LISA también presentará un informe periódico a la Comisión acerca de los problemas detectados y los Estados miembros a los que estos conciernan.

4. Los pormenores de los mecanismos y procedimientos automatizados de control de la calidad de los datos, los indicadores comunes de la calidad de los datos y los estándares mínimos de calidad para el almacenamiento de datos en el SES, el [SEIAV], el VIS, el SIS, el SCB compartido, el RCDI y el DIM, en particular en lo relativo a los datos biométricos, se establecerán mediante actos de ejecución. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 64, apartado 2.

5. Un año después de la creación de los mecanismos y procedimientos automatizados de control de la calidad de los datos y los indicadores comunes de calidad de los datos, y cada año en lo sucesivo, la Comisión valorará la implementación por los Estados miembros de la calidad de los datos y formulará las recomendaciones necesarias. Los Estados miembros presentarán a la Comisión un plan de acción para subsanar las deficiencias detectadas en el informe de valoración e informará sobre cualquier progreso relativo a dicho plan de acción hasta que este se aplique plenamente. La Comisión remitirá el informe de valoración al Parlamento Europeo, al Consejo, al Supervisor Europeo de Protección de Datos y a la Agencia de los Derechos Fundamentales de la Unión Europea, establecida por el Reglamento (CE) n.º 168/2007 del Consejo[75].

[75] Reglamento (CE) n.º 168/2007 del Consejo, de 15 de febrero de 2007, por el que se crea una Agencia de los Derechos Fundamentales de la Unión Europea (DO L 53 de 22.2.2007, p. 1).

Artículo 38
Formato universal de mensajes

1. Se establece la norma de formato universal de mensajes (UMF). El UMF define una norma para ciertos elementos del contenido del intercambio transfronterizo de información entre sistemas de información, autoridades y organizaciones en el ámbito de la justicia y los asuntos de interior.

2. La norma UMF se utilizará en el desarrollo del SES, el [SEIAV], el portal europeo de búsqueda, el RCDI, el DIM y, si procede, en el desarrollo por parte de eu-LISA o cualquier otro organismo de la UE de nuevos modelos de intercambio de información y sistemas de información en el ámbito de la justicia y los asuntos de interior.

3. Puede tomarse en consideración la aplicación de la norma UMF en el VIS, el SIS y cualquier modelo existente o nuevo de intercambio transfronterizo de información o sistema de información en el ámbito de la justicia y los asuntos de interior, desarrollado por los Estados miembros o los países asociados.

4. La Comisión adoptará un acto de ejecución para establecer y desarrollar la norma UMF a que se refiere el apartado 1. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 64, apartado 2.

Artículo 39
Repositorio central para la presentación de informes y estadísticas

1. Se crea un repositorio central para la presentación de informes y estadísticas (RCIE) con el fin de apoyar los objetivos del SES, el VIS, [el SEIAV] y el SIS y de generar datos estadísticos transversales entre sistemas e informes analíticos con fines operativos, de formulación de políticas y de calidad de los datos.

2. La agencia eu-LISA establecerá e implementará el RCIE y lo alojará en sus sitios técnicos que contengan los datos a que se hace referencia en [el artículo 63 del Reglamento SES], el artículo 17 del Reglamento (CE) n.º 767/2008, [el artículo 73 del Reglamento SEIAV] y [el artículo 54 del Reglamento sobre el SIS en el ámbito de los controles fronterizos], separados de forma lógica. Los datos contenidos en el RCIE no permitirán la identificación de personas. El acceso al repositorio se concederá por medio de un acceso seguro a través de la red de servicios transeuropeos seguros de telemática entre administraciones (s-TESTA), con un control de acceso y unos perfiles de usuario específicos, únicamente a efectos de la presentación de informes y estadísticas, a las autoridades a las que se refieren [el artículo 63 del Reglamento SES], el artículo 17 del Reglamento (CE) n.º 767/2008, [el artículo 73 del Reglamento SEIAV] y [el artículo 54 del Reglamento sobre el SIS en el ámbito de los controles fronterizos].

3. La agencia eu-LISA anonimizará los datos y registrará los datos anonimizados en el RCIE. El proceso por el que se anonimizarán los datos será automatizado.

4. El RCIE se compondrá de:

   a) una infraestructura central, consistente en un repositorio de datos que permita que se anonimicen los datos;

b) una infraestructura de comunicación segura entre el RCIE y el SES, [el SEIAV], el VIS, y el SIS, así como con las infraestructuras centrales del SCB compartido, el RCDI y el DIM.

5. La Comisión establecerá, mediante actos de ejecución, normas detalladas sobre el funcionamiento del RCIE, incluidas salvaguardias específicas para el tratamiento de los datos personales a que se refieren los apartados 2 y 3 y las normas de seguridad aplicables al repositorio. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 64, apartado 2.

CAPÍTULO VII
Protección de datos

Artículo 40
Responsable del tratamiento

1. En relación con el tratamiento de datos en el servicio de correspondencia biométrica compartido (SCB compartido), las autoridades de los Estados miembros que sean responsables del tratamiento en el VIS, el SES y el SIS, respectivamente, también se considerarán responsables del tratamiento, de conformidad con el artículo 4, apartado 7, del Reglamento (UE) 2016/679, en lo que respecta a las plantillas biométricas obtenidas a partir de los datos a que se refiere el artículo 13 que introduzcan en sus respectivos sistemas y tendrán responsabilidad en el tratamiento de las plantillas biométricas en el SCB compartido.

2. En relación con el tratamiento de datos en el registro común de datos de identidad (RCDI), las autoridades de los Estados miembros que sean responsables del tratamiento, en el VIS, el SES y el [SEIAV], respectivamente, también se considerarán responsables del tratamiento de conformidad con el artículo 4, apartado 7, del Reglamento (UE) 2016/679, en lo que respecta a los datos a que se refiere el artículo 18 que introduzcan en sus respectivos sistemas y tendrán responsabilidad en el tratamiento de esos datos personales en el RCDI.

3. En relación con el tratamiento de datos en el detector de identidades múltiples:

   a) la Agencia Europea de la Guardia de Fronteras y Costas será considerada responsable del tratamiento con arreglo al artículo 2, letra b), del Reglamento (CE) n.º 45/2001 en relación con el tratamiento de los datos personales en la unidad central SEIAV;

   b) las autoridades de los Estados miembros que añadan o modifiquen datos en el expediente de confirmación de identidad también serán consideradas responsables del tratamiento de acuerdo con el artículo 4, apartado 7, del Reglamento (UE) 2016/679 y tendrán responsabilidad en el tratamiento de los datos personales en el detector de identidades múltiples.

Artículo 41
Encargado del tratamiento

En relación con el tratamiento de los datos personales en el RCDI, eu-LISA será considerada encargada del tratamiento de conformidad con el artículo 2, letra e), del Reglamento (CE) n.º 45/2001.

Artículo 42
Seguridad del tratamiento

1. Tanto eu-LISA como las autoridades de los Estados miembros garantizarán la seguridad del tratamiento de los datos personales que tenga lugar en virtud de la aplicación del presente Reglamento. La agencia eu-LISA, [la unidad central SEIAV] y las autoridades de los Estados miembros cooperarán en las tareas relacionadas con la seguridad.

2. Sin perjuicio de lo dispuesto en el artículo 22 del Reglamento (CE) n.º 45/2001, eu-LISA adoptará las medidas necesarias para garantizar la seguridad de los componentes de interoperabilidad y de su infraestructura de comunicación conexa.

3. En particular, eu-LISA adoptará las medidas necesarias, incluidos un plan de seguridad, un plan de continuidad de las actividades y un plan de recuperación en caso de catástrofe, a fin de:

   a) proteger los datos físicamente, entre otras cosas mediante la elaboración de planes de emergencia para la protección de las infraestructuras críticas;

   b) impedir la lectura, copia, modificación o retirada no autorizadas de los soportes de datos;

   c) impedir la introducción no autorizada de datos y la inspección, modificación o eliminación no autorizadas de datos personales registrados;

   d) impedir el tratamiento no autorizado de datos y la copia, modificación o eliminación no autorizadas de datos;

   e) garantizar que las personas autorizadas para acceder a los componentes de interoperabilidad tengan únicamente acceso a los datos cubiertos por su autorización de acceso, exclusivamente mediante identidades de usuario individuales y modos de acceso confidenciales;

   f) garantizar la posibilidad de verificar y determinar a qué organismos pueden transmitirse datos personales mediante equipos de transmisión de datos;

   g) garantizar la posibilidad de verificar y determinar qué datos han sido tratados en los componentes de interoperabilidad, en qué momento, por quién y con qué fin;

   h) impedir la lectura, copia, modificación o eliminación no autorizadas de datos personales durante su transmisión hacia o desde los componentes de interoperabilidad o durante el transporte de soportes de datos, en particular mediante técnicas adecuadas de cifrado;

   i) controlar la eficacia de las medidas de seguridad mencionadas en el presente apartado y adoptar las medidas de organización del control interno necesarias para garantizar el cumplimiento del presente Reglamento.

4. Los Estados miembros adoptarán medidas equivalentes a las mencionadas en el apartado 3 en lo que respecta a la seguridad en relación con el tratamiento de datos personales por parte de las autoridades con derecho de acceso a cualquiera de los componentes de interoperabilidad.

Artículo 43
Confidencialidad de los datos del SIS

1. Cada Estado miembro aplicará sus normas sobre secreto profesional u otras obligaciones equivalentes de confidencialidad a todas las personas y todos los organismos que deban trabajar con datos del SIS a los que se acceda a través de cualquier componente de interoperabilidad, de conformidad con su legislación nacional. Dicha obligación seguirá siendo aplicable después del cese en el cargo o el empleo de dichas personas o tras la terminación de las actividades de dichos organismos.

2. Sin perjuicio de lo dispuesto en el artículo 17 del Estatuto de los funcionarios y el régimen aplicable a los otros agentes de la Unión Europea, eu-LISA aplicará normas adecuadas sobre secreto profesional u otras obligaciones equivalentes de confidencialidad con unas exigencias comparables a las establecidas en el apartado 1 a todos los miembros de su personal que deban trabajar con datos del SIS. Esta obligación seguirá siendo aplicable después del cese en el cargo o el empleo de dichas personas o tras la terminación de sus actividades.

Artículo 44
Incidentes de seguridad

1. Cualquier acontecimiento que repercuta o pueda repercutir en la seguridad de los componentes de interoperabilidad y pueda causar daños a los datos almacenados en ellos o la pérdida de dichos datos se considerará un incidente de seguridad, especialmente cuando pueda haber tenido lugar un acceso no autorizado a los datos o cuando la disponibilidad, integridad y confidencialidad de los datos haya sido o pueda haber sido comprometida.

2. Los incidentes de seguridad se gestionarán de forma que se garantice una respuesta rápida, eficaz y adecuada.

3. Sin perjuicio de la notificación y comunicación de una violación de la seguridad de un dato personal de conformidad con el artículo 33 del Reglamento (UE) 2016/679, con el artículo 30 de la Directiva (UE) 2016/680 o con ambos, los Estados miembros notificarán a la Comisión, eu-LISA y el Supervisor Europeo de Protección de Datos los incidentes de seguridad. En el caso de un incidente de seguridad relacionado con la infraestructura central de los componentes de interoperabilidad, eu-LISA lo notificará a la Comisión y al Supervisor Europeo de Protección de Datos.

4. La agencia eu-LISA transmitirá a los Estados miembros la información concerniente a un incidente de seguridad que repercuta o pueda repercutir en el funcionamiento de los componentes de interoperabilidad o en la disponibilidad, integridad y confidencialidad de los datos, y presentará un informe en cumplimiento del plan de gestión de incidentes.

5. Los Estados miembros afectados y eu-LISA cooperarán cuando se produzca un incidente de seguridad. La Comisión especificará los detalles de este procedimiento de cooperación mediante actos de ejecución. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 64, apartado 2.

Artículo 45
Autocontrol

Los Estados miembros y los organismos pertinentes de la UE velarán por que toda autoridad facultada para acceder a los componentes de interoperabilidad adopte las medidas necesarias para controlar su cumplimiento del presente Reglamento y coopere, en caso necesario, con la autoridad de control.

Los responsables del tratamiento de datos a que se refiere el artículo 40 adoptarán las medidas necesarias para controlar la conformidad del tratamiento de datos con el presente Reglamento, incluida la frecuencia de verificación de los registros, y cooperarán, cuando proceda, con las autoridades de control a que se refieren los artículos 49 y 50.

Artículo 46
Derecho de información

1. Sin perjuicio del derecho de información a que se hace referencia en los artículos 11 y 12 del Reglamento (CE) n.º 45/2001 y en los artículos 13 y 14 del Reglamento (UE) 2016/679, las personas cuyos datos se almacenen en el servicio de correspondencia biométrica compartido, el registro común de datos de identidad o el detector de identidades múltiples serán informadas por la autoridad que recoja sus datos, en el momento de la recogida, sobre el tratamiento de los datos personales a los efectos del presente Reglamento, lo que incluye la identidad y los datos de contacto de los respectivos responsables del tratamiento de datos y los procedimientos para el ejercicio de sus derechos de acceso, rectificación y supresión, así como los datos de contacto del Supervisor Europeo de Protección de Datos y de la autoridad de control del Estado miembro responsable de la recogida de los datos.
2. Las personas cuyos datos estén registrados en el SES, el VIS o [el SEIAV] serán informadas sobre el tratamiento de los datos transmitidos a efectos del presente Reglamento de conformidad con el apartado 1, cuando:
   a) [se cree o actualice un expediente individual en el SES de conformidad con el artículo 14 del Reglamento SES];
   b) se cree o actualice un expediente individual en el VIS de conformidad con el artículo 8 del Reglamento (CE) n.º 767/2008;
   c) [se cree o actualice un expediente de solicitud en el SEIAV de conformidad con el artículo 17 del Reglamento SEIAV;]
   d) – (no procede);
   e) – (no procede).

Artículo 47
Derechos de acceso, corrección y supresión

1. Con el fin de ejercer sus derechos en virtud de los artículos 13, 14, 15 y 16 del Reglamento (CE) n.º 45/2001 y de los artículos 15, 16, 17 y 18 del Reglamento (UE) 2016/679, cualquier persona tendrá derecho a dirigirse personalmente al Estado miembro responsable de la verificación manual de identidades diferentes, que deberá examinar la solicitud y darle respuesta.
2. El Estado miembro responsable de la verificación manual de identidades diferentes a que se refiere el artículo 29 o el Estado miembro al que se haya presentado la

solicitud dará respuesta a esas solicitudes en un plazo de cuarenta y cinco días a partir de la recepción de la solicitud.

3. Si se realiza una solicitud de corrección o supresión de datos personales a un Estado miembro distinto del Estado miembro responsable, el Estado miembro al que se haya realizado la solicitud contactará con las autoridades del Estado miembro responsable en el plazo de siete días y el Estado miembro responsable comprobará la exactitud de los datos y la legalidad de su tratamiento en el plazo de treinta días desde que se establezca el contacto.

4. Cuando, previo examen, se compruebe que los datos almacenados en el detector de identidades múltiples (DIM) son materialmente inexactos o han sido registrados ilegalmente, el Estado miembro responsable o, cuando proceda, el Estado miembro al que se haya presentado la solicitud corregirá o eliminará esos datos.

5. Cuando el Estado miembro responsable modifique los datos contenidos en el DIM durante su periodo de validez, el propio Estado miembro responsable llevará a cabo el tratamiento establecido en el artículo 27 y, en su caso, el artículo 29, a fin de determinar si se vincularán los datos modificados. Cuando el tratamiento no dé lugar a ninguna respuesta positiva, el Estado miembro responsable o, cuando proceda, el Estado miembro al que se haya presentado la solicitud eliminará los datos del expediente de confirmación de identidad. Cuando el tratamiento automatizado dé lugar a una o varias respuestas positivas, el Estado miembro responsable generará o actualizará el vínculo correspondiente de conformidad con las disposiciones pertinentes del presente Reglamento.

6. Cuando el Estado miembro responsable o, cuando proceda, el Estado miembro al que se haya presentado la solicitud no admita que los datos registrados en el DIM son materialmente inexactos o han sido ilegalmente registrados, dicho Estado miembro adoptará una decisión administrativa, en la que expondrá por escrito a la persona interesada, sin demora, los motivos para no corregir o eliminar los datos sobre ella.

7. En tal decisión también se informará a la persona interesada de la posibilidad de impugnar la decisión adoptada respecto de la solicitud a que se refiere el apartado 3, y en su caso se informará sobre cómo interponer una acción judicial o presentar una reclamación ante las autoridades u órganos jurisdiccionales competentes y sobre cualquier tipo de asistencia, en particular de las autoridades nacionales de control competentes.

8. Cualquier solicitud realizada de conformidad con el apartado 3 deberá contener la información necesaria para identificar a la persona en cuestión. Dicha información solo se utilizará para el ejercicio de los derechos a que se refiere el apartado 3, tras lo cual se procederá inmediatamente a su supresión.

9. El Estado miembro responsable o, en su caso, el Estado miembro al que se haya realizado la solicitud dejará constancia por escrito de la presentación de una solicitud en virtud del apartado 3 y del curso dado a la misma, y pondrá este documento sin demora a disposición de las autoridades nacionales de control de la protección de datos competentes.

Artículo 48
Comunicación de datos personales a terceros países, organizaciones internacionales y particulares

Los datos personales almacenados en los componentes de interoperabilidad o a los que se acceda a través de ellos no se transmitirán a ningún tercer país, organización internacional o particular ni se pondrán a su disposición, con la salvedad de las transmisiones a Interpol con el fin de llevar a cabo el tratamiento automatizado a que se refiere [el artículo 18, apartado 2, letras b) y m) del Reglamento SEIAV] o a los efectos de lo dispuesto en el artículo 8, apartado 2, del Reglamento (UE) 2016/399. Dichas transferencias de datos personales a Interpol cumplirán lo dispuesto en el artículo 9 del Reglamento (CE) n.º 45/2001 y en el capítulo V del Reglamento (UE) 2016/679.

Artículo 49
Control por parte de la autoridad nacional

1. La autoridad o autoridades de control designadas de conformidad con el artículo 49 del Reglamento (UE) 2016/679 velarán por que se lleve a cabo una auditoría de las operaciones de tratamiento de datos realizadas por las autoridades nacionales responsables, de conformidad con las normas internacionales de auditoría pertinentes, al menos cada cuatro años.
2. Los Estados miembros garantizarán que su autoridad de control disponga de medios suficientes para desempeñar las tareas que le encomienda el presente Reglamento.

Artículo 50
Control por parte del Supervisor Europeo de Protección de Datos

El Supervisor Europeo de Protección de Datos velará por que se lleve a cabo una auditoría de las actividades de tratamiento de datos personales de eu-LISA, con arreglo a las normas internacionales de auditoría pertinentes, al menos cada cuatro años. Se enviará un informe de la auditoría al Parlamento Europeo, el Consejo, eu-LISA, la Comisión y los Estados miembros. Se brindará a eu-LISA la oportunidad de formular observaciones antes de la adopción de los informes.

Artículo 51
Cooperación entre las autoridades nacionales de control y el Supervisor Europeo de Protección de Datos

1. El Supervisor Europeo de Protección de Datos actuará en estrecha cooperación con las autoridades nacionales de control en lo tocante a cuestiones específicas que requieran una intervención nacional, en particular si el Supervisor Europeo de Protección de Datos o una autoridad nacional de control detectan discrepancias importantes entre las prácticas de los Estados miembros o transferencias potencialmente ilegales en la utilización de los canales de comunicación de los componentes de interoperabilidad, o en el contexto de cuestiones planteadas por una o varias autoridades nacionales de control sobre la aplicación y la interpretación del presente Reglamento.
2. En los casos contemplados en el apartado 1, se velará por el control coordinado de conformidad con el artículo 62 del Reglamento (UE) XXXX/2018 [Reglamento n.º 45/2001 revisado].

CAPÍTULO VIII
Responsabilidades

Artículo 52
Responsabilidades de eu-LISA durante la fase de diseño y desarrollo

1. La agencia eu-LISA velará por que las infraestructuras centrales de los componentes de interoperabilidad funcionen de conformidad con el presente Reglamento.

2. Los componentes de interoperabilidad estarán alojados por eu-LISA en sus sitios técnicos y dispondrán de las funcionalidades establecidas en el presente Reglamento de conformidad con las condiciones de seguridad, disponibilidad, calidad y velocidad establecidas en el artículo 53, apartado 1.

3. La agencia eu-LISA será responsable del desarrollo de los componentes de interoperabilidad para todas las adaptaciones que exija la interoperabilidad de los sistemas centrales del SES, el VIS, [el SEIAV], el SIS, Eurodac, [el sistema ECRIS-TCN], el portal europeo de búsqueda, el servicio de correspondencia biométrica compartido, el registro común de datos de identidad y el detector de identidades múltiples.

   La agencia eu-LISA definirá el diseño de la arquitectura física de los componentes de interoperabilidad, incluidas sus infraestructuras de comunicación y sus especificaciones técnicas, y su evolución en lo relativo a la infraestructura central y la infraestructura de comunicación segura, que será adoptado por el Consejo de Administración, previo dictamen favorable de la Comisión. La agencia eu-LISA realizará también cualquier adaptación necesaria del SES, [el SEIAV], el SIS o el VIS que se derive del establecimiento de la interoperabilidad y que disponga el presente Reglamento.

   La agencia eu-LISA desarrollará e implementará los componentes de interoperabilidad lo antes posible después de la entrada en vigor del presente Reglamento y la adopción por la Comisión de las medidas previstas en el artículo 8, apartado 2, el artículo 9, apartado 7, el artículo 28, apartados 5 y 6, el artículo 37, apartado 4, el artículo 38, apartado 4, el artículo 39, apartado 5, y el artículo 44, apartado 5.

   El desarrollo consistirá en la elaboración y aplicación de las especificaciones técnicas, los ensayos y la coordinación global del proyecto.

4. Durante la fase de diseño y desarrollo, se establecerá un comité de gestión del programa compuesto por un máximo de diez miembros. El comité estará compuesto por siete miembros designados por el Consejo de Administración de eu-LISA de entre sus miembros o sus suplentes, el presidente del grupo consultivo de interoperabilidad a que se refiere el artículo 65, un miembro representante de eu-LISA nombrado por su director ejecutivo y un miembro nombrado por la Comisión. Los miembros nombrados por el Consejo de Administración de eu-LISA solo podrán ser elegidos de entre los Estados miembros que estén plenamente obligados con arreglo a la legislación de la Unión por los instrumentos legislativos reguladores del desarrollo, establecimiento, funcionamiento y uso de todos los sistemas informáticos de gran magnitud gestionados por eu-LISA y que vayan a participar en los componentes de interoperabilidad.

5. El comité de gestión del programa se reunirá periódicamente y al menos tres veces por trimestre. Garantizará la gestión adecuada de la fase de diseño y desarrollo de los componentes de interoperabilidad.

El comité de gestión del programa presentará mensualmente al Consejo de Administración informes por escrito sobre los progresos del proyecto. El comité de gestión del programa no tendrá competencias para adoptar decisiones ni mandato alguno de representación de los miembros del Consejo de Administración de eu-LISA.

6. El Consejo de Administración de eu-LISA establecerá el reglamento interno del comité de gestión del programa, que incluirá, en particular, normas relativas a:

a) la presidencia;

b) los lugares de reunión;

c) la preparación de las reuniones;

d) la admisión de expertos a las reuniones;

e) planes de comunicación que garanticen una información completa a los miembros del Consejo de Administración no participantes.

La presidencia la ostentará un Estado miembro que esté plenamente obligado con arreglo a la legislación de la Unión por los instrumentos legislativos reguladores del desarrollo, establecimiento, funcionamiento y uso de todos los sistemas informáticos de gran magnitud gestionados por eu-LISA.

Todos los gastos de viaje y dietas de los miembros del comité de gestión del programa serán abonados por la agencia, y el artículo 10 del Reglamento Interno de eu-LISA se aplicará *mutatis mutandis*. La agencia eu-LISA realizará las labores de secretaría del comité de gestión del programa.

El grupo consultivo de interoperabilidad a que se refiere el artículo 65 se reunirá periódicamente hasta que los componentes de interoperabilidad entren en funcionamiento. Presentará un informe al comité de gestión del programa después de cada una de sus reuniones. Asimismo, aportará los conocimientos técnicos para llevar a cabo las tareas del comité de gestión del programa y realizará un seguimiento del estado de preparación de los Estados miembros.

Artículo 53
Responsabilidades de eu-LISA tras la entrada en funcionamiento

1. Tras la entrada en funcionamiento de cada componente de interoperabilidad, eu-LISA será responsable de la gestión técnica de la infraestructura central y las interfaces uniformes nacionales. En cooperación con los Estados miembros, garantizará en todo momento la mejor tecnología disponible sobre la base de un análisis coste-beneficio. La agencia eu-LISA también será responsable de la gestión técnica de la infraestructura de comunicación a que se refieren los artículos 6, 12, 17, 25 y 39.

La gestión técnica de los componentes de interoperabilidad consistirá en todas las tareas necesarias para mantenerlos en funcionamiento durante las veinticuatro horas del día, siete días a la semana, de conformidad con el presente Reglamento y, en particular, en el trabajo de mantenimiento y los desarrollos técnicos necesarios para garantizar que los componentes funcionen con una calidad técnica de un nivel

satisfactorio, en particular en lo que se refiere al tiempo de respuesta para la consulta de las infraestructuras centrales, de acuerdo con las características técnicas.

2. Sin perjuicio de lo dispuesto en el artículo 17 del Estatuto de los funcionarios de la Unión Europea, eu-LISA aplicará las normas adecuadas sobre secreto profesional u otras obligaciones de confidencialidad equivalentes a todos los miembros de su personal que deban trabajar con los datos almacenados en los componentes de interoperabilidad. Esta obligación seguirá siendo aplicable después de que dichos miembros del personal hayan cesado en el cargo o el empleo, o tras la terminación de sus actividades.

3. La agencia eu-LISA desarrollará y mantendrá un mecanismo y procedimientos para realizar controles de calidad de los datos almacenados en el servicio de correspondencia biométrica compartido y el registro común de datos de identidad de conformidad con el artículo 37.

4. La agencia eu-LISA desempeñará las funciones relacionadas con la formación sobre la utilización técnica de los componentes de interoperabilidad.

Artículo 54
Responsabilidades de los Estados miembros

1. Cada Estado miembro será responsable de:

   a) la conexión con la infraestructura de comunicación del portal europeo de búsqueda (PEB) y el registro común de datos de identidad (RCDI);

   b) la integración de los sistemas e infraestructuras nacionales existentes con el PEB, el servicio de correspondencia biométrica compartido, el RCDI y el detector de identidades múltiples;

   c) la organización, la gestión, el funcionamiento y el mantenimiento de su infraestructura nacional existente y su conexión con los componentes de interoperabilidad;

   d) la gestión y las condiciones de acceso del personal debidamente autorizado y, a través del personal debidamente facultado, de las autoridades nacionales competentes al PEB, el RCDI y el detector de identidades múltiples, de conformidad con el presente Reglamento, y el establecimiento y la actualización periódica de la lista de dicho personal y sus perfiles;

   e) la adopción de las medidas legislativas a que se refiere el artículo 20, apartado 3, para acceder al RCDI a efectos de identificación;

   f) la verificación manual de identidades diferentes a que se refiere el artículo 29;

   g) la aplicación de los requisitos de calidad de los datos en los sistemas de información de la UE y en los componentes de interoperabilidad;

   h) la corrección de las deficiencias detectadas en el informe de valoración de la Comisión sobre la calidad de los datos a que se refiere el artículo 37, apartado 5.

2. Cada Estado miembro conectará a sus autoridades designadas mencionadas en el artículo 4, apartado 24, con el RCDI.

Artículo 55
Responsabilidades de la unidad central SEIAV

La unidad central SEIAV será responsable de:

a) la verificación manual de identidades diferentes contemplada en el artículo 29;

b) la detección de identidades múltiples entre los datos almacenados en el VIS, Eurodac y el SIS contemplada en el artículo 59.

CAPÍTULO IX
Modificaciones de otros instrumentos de la Unión

Artículo 55 bis
Modificaciones del Reglamento (UE) 2016/399

El Reglamento (UE) 2016/399 se modifica como sigue:

En el artículo 8 del Reglamento (UE) 2016/399, se añade el apartado 4 *bis* siguiente:

«4 *bis*. Si a la entrada o a la salida, la consulta de las bases de datos pertinentes, incluido el detector de identidades múltiples, a través del portal europeo de búsqueda al que se refieren respectivamente [el artículo 4, punto 36, y el artículo 4, punto 33, del Reglamento 2018/XX sobre interoperabilidad], resulta en un vínculo amarillo o detecta un vínculo rojo, la persona objeto de la inspección será remitida a la inspección de segunda línea.

El guardia de fronteras en segunda línea consultará el detector de identidades múltiples, junto con el registro común de datos de identidad a que se refiere [el artículo 4, punto 35, del Reglamento 2018/XX sobre interoperabilidad], el Sistema de Información de Schengen o ambos, para evaluar las diferencias en las identidades vinculadas y llevará a cabo cualquier verificación adicional necesaria para adoptar una decisión sobre el carácter y el color del vínculo, así como una decisión sobre la entrada o la denegación de entrada de la persona de que se trate.

De conformidad con el [artículo 59, apartado 1, del Reglamento 2018/XX], el presente apartado será de aplicación únicamente a partir de la entrada en funcionamiento del detector de identidades múltiples.».

Artículo 55 ter
Modificaciones del Reglamento (UE) 2017/2226

El Reglamento (UE) 2017/2226 se modifica como sigue:

1) En el artículo 1, se añade el apartado siguiente:

«1 *bis*. Mediante el almacenamiento de identidades, documentos de viaje y datos biométricos en el registro común de datos de identidad (RCDI) creado por el [artículo 17 del Reglamento 2018/XX sobre interoperabilidad], el SES contribuye a facilitar la identificación correcta de las personas registradas en el SES y a ayudar a ella, en las condiciones y para los objetivos finales a que se refiere el [artículo 20] de dicho Reglamento.».

2) En el artículo 3, apartado 1, se añade el punto 21 *bis* siguiente:

«"RCDI": el registro común de datos de identidad, tal como se define en el [artículo 4, punto 35, del Reglamento 2018/XX sobre interoperabilidad];».

3) El texto del artículo 3, apartado 1, punto 22, se sustituye por el siguiente:

«22) "datos del SES": todos los datos almacenados en el sistema central del SES y en el RCDI, de conformidad con los artículos 14 y 16 a 20.».

4) En el artículo 3, apartado 1, se añade un nuevo punto 22 *bis*:

«22 *bis*) "datos de identidad": los datos a que se refiere el artículo 16, apartado 1, letra a);».

5) En el artículo 6, apartado 1, se añade la letra siguiente:

«j) garantizar la identificación correcta de las personas.».

6) En el artículo 7, apartado 1, la letra a) se sustituye por el texto siguiente:

«a) un registro común de datos de identidad (RCDI), tal como se define en el [artículo 17, punto 2, letra a), del Reglamento 2018/XX sobre interoperabilidad];

a *bis*) un sistema central (sistema central del SES);».

7) En el artículo 7, apartado 1, la letra f) se sustituye por el texto siguiente:

«f) una infraestructura de comunicación segura entre el sistema central del SES y las infraestructuras centrales del portal europeo de búsqueda creado por [el artículo 6 del Reglamento 2018/XX sobre interoperabilidad], el servicio de correspondencia biométrica compartido creado por [el artículo 12 del Reglamento 2018/XX sobre interoperabilidad], el registro común de datos de identidad creado por [el artículo 17 del Reglamento 2018/XX sobre interoperabilidad] y el detector de identidades múltiples creado por [el artículo 25 del Reglamento 2018/XX sobre interoperabilidad].».

8) En el artículo 7, se añade el apartado siguiente:

«1 *bis*. El RCDI contendrá los datos a que se refieren el artículo 16, apartado 1, letras a) a d), y el artículo 17, apartado 1, letras a) a c), y los restantes datos del SES se almacenarán en el sistema central SES.».

9) En el artículo 9, se añade el apartado siguiente:

«3. El acceso para consultar los datos del SES almacenados en el RCDI estará reservado exclusivamente al personal debidamente autorizado de las autoridades nacionales de cada Estado miembro y al personal debidamente autorizado de los organismos de la UE que sean competentes para los fines establecidos en [el artículo 20 y el artículo 21 del Reglamento 2018/XX sobre interoperabilidad]. Dicho acceso se limitará a la medida necesaria para la realización de las tareas de esas autoridades nacionales y organismos de la UE con arreglo a dichos fines, y será proporcionado a los objetivos perseguidos.».

10) En el artículo 21, apartado 1, las palabras «el sistema central del SES» se sustituyen, en los dos casos en que aparecen, por las palabras «el sistema central del SES o el RCDI».

11) En el artículo 21, apartado 2, las palabras «tanto en el sistema central del SES como en la INU» se sustituyen por las palabras «tanto en el sistema central del SES y en el RCDI, por una parte, como en la INU, por otra».

12) En el artículo 21, apartado 2, las palabras «se introducirán en el sistema central del SES» se sustituyen por las palabras «se introducirán en el sistema central del SES y en el RCDI».

13) En el artículo 32, se añade el apartado 1 *bis* siguiente:

«1 *bis*. En los casos en que las autoridades designadas hayan iniciado una consulta al RCDI de conformidad con [el artículo 22 del Reglamento 2018/XX sobre interoperabilidad], podrán acceder al SES para consultarlo cuando la respuesta recibida a que se refiere el [el artículo 22, apartado 3, del Reglamento 2018/XX sobre interoperabilidad] ponga de manifiesto que los datos están almacenados en el SES.».

14) En el artículo 32, el apartado 2 se sustituye por el texto siguiente:

«2. Se autorizará el acceso al SES como herramienta para identificar a un sospechoso, autor o víctima desconocidos de un delito de terrorismo u otro delito grave únicamente cuando se haya iniciado una consulta al RCDI de conformidad con [el artículo 22 del Reglamento 2018/XX sobre interoperabilidad] y se cumplan todas las condiciones enumeradas en el apartado 1 y el apartado 1 bis.

No obstante, esta condición adicional no resultará de aplicación en caso de urgencia, cuando sea necesario impedir un peligro inminente para la vida de alguna persona asociado a la comisión de un delito de terrorismo u otro delito grave. Tales motivos fundados se incluirán en la solicitud electrónica o presentada por escrito que envíe la unidad operativa de la autoridad designada al punto de acceso central.».

15) En el artículo 32, se suprime el apartado 4.

16) En el artículo 33, se añade el apartado 1 *bis* siguiente:

«1 bis. En los casos en que Europol haya iniciado una consulta al RCDI de conformidad con [el artículo 22 del Reglamento 2018/XX sobre interoperabilidad], podrá acceder al SES para consultarlo cuando la respuesta recibida a que se refiere [el artículo 22, apartado 3, del Reglamento 2018/XX sobre interoperabilidad] ponga de manifiesto que los datos están almacenados en el SES.».

17) En el artículo 33, el apartado 3 se sustituye por el texto siguiente:

«Se aplicarán en consecuencia las condiciones establecidas en el artículo 32, apartados 3 y 5.».

18) En el artículo 34, apartados 1 y 2, las palabras «en el sistema central del SES» se sustituyen por las palabras «en el RCDI y en el sistema central del SES, respectivamente,».

19) En el artículo 34, apartado 5, las palabras «del sistema central del SES» se sustituyen por las palabras «del sistema central del SES y del RCDI».

20) En el artículo 35, el apartado 7 se sustituye por el texto siguiente:

«El sistema central del SES y el RCDI informarán inmediatamente a todos los Estados miembros de la supresión de datos del SES o el RCDI y, cuando proceda, de la lista de las personas a que se refiere el artículo 12, apartado 3.».

21) En el artículo 36, las palabras «del sistema central del SES» se sustituyen por las palabras «del sistema central del SES y el RCDI».

22) En el artículo 37, apartado 1, las palabras «desarrollo del sistema central del SES» se sustituyen por las palabras «desarrollo del sistema central del SES y el RCDI».

23) En el artículo 37, apartado 3, párrafo primero, las palabras «sistema central del SES» se sustituyen, la primera y la tercera vez que aparecen, por las palabras «sistema central del SES y el RCDI».

24) En el artículo 46, apartado 1, se añade la letra f) siguiente:

«f) cuando proceda, una referencia a la utilización del portal europeo de búsqueda para consultar el SES, según se contempla en [el artículo 7, apartado 2, del Reglamento n.º 2018/XX sobre interoperabilidad].».

25) En el artículo 63, el apartado 2 se sustituye por el texto siguiente:

«2. A los efectos del apartado 1 del presente artículo, eu-LISA almacenará los datos a los que se refiere el apartado 1 en el repositorio central para la presentación de informes y estadísticas a que se refiere [el artículo 39 del Reglamento 2018/XX sobre interoperabilidad].».

26) En el artículo 63, apartado 4, se añade el párrafo segundo siguiente:

«Las estadísticas cotidianas se almacenarán en el repositorio central para la presentación de informes y estadísticas.».

Artículo 55 quater
Modificaciones de la Decisión 2004/512/CE del Consejo

La Decisión 2004/512/CE del Consejo por la que se establece el Sistema de Información de Visados (VIS) se modifica como sigue:

En el artículo 1, el apartado 2 se modifica del siguiente modo:

«2. El Sistema de Información de Visados se basará en una arquitectura centralizada y consistirá en:

a) un registro común de datos de identidad, tal como se define en el [artículo 17, punto 2, letra a), del Reglamento 2018/XX sobre interoperabilidad];

b) un sistema central de información, denominado en lo sucesivo "Sistema Central de Información de Visados" (CS-VIS);

c) una interfaz en cada Estado miembro, denominada en lo sucesivo "interfaz nacional" (NI-VIS) que proporcionará la conexión a la autoridad nacional central pertinente del respectivo Estado miembro;

d) la infraestructura de comunicación entre el Sistema Central de Información de Visados y las interfaces nacionales;

e) un canal seguro de comunicación entre el sistema central del SES y el CS-VIS;

f) una infraestructura de comunicación segura entre el sistema central del SES y las infraestructuras centrales del portal europeo de búsqueda creado por [el artículo 6 del Reglamento 2018/XX sobre interoperabilidad], el servicio de correspondencia biométrica compartido creado por [el artículo 12 del Reglamento 2018/XX sobre interoperabilidad], el registro común de datos de identidad y el detector de identidades múltiples (DIM) creado por [el artículo 25 del Reglamento 2018/XX sobre interoperabilidad].».

Artículo 55 quinquies
Modificaciones del Reglamento (CE) n.º 767/2008

1) En el artículo 1, se añade el apartado siguiente:

«2. Mediante el almacenamiento de identidades, documentos de viaje y datos biométricos en el registro común de identidades (RCDI) creado por el [artículo 17 del Reglamento 2018/XX sobre interoperabilidad], el VIS contribuye a facilitar la

identificación correcta de las personas registradas en el VIS y a ayudar a ella, en las condiciones y para los objetivos finales establecidos en el apartado 1 del presente artículo.».

2) En el artículo 4, se añaden los puntos siguientes:

«12) "datos del VIS", todos los datos almacenados en el VIS central y en el RCDI, de conformidad con los artículos 9 a 14.

13) "datos de identidad", los datos a que se refiere el artículo 9, apartado 4, letras a) a a *bis*);

14) "datos dactiloscópicos", los datos relativos a las cinco impresiones dactilares de los dedos índice, corazón, anular, meñique y pulgar de la mano derecha, en caso de que existan, y de la mano izquierda;

15) "imagen facial", las imágenes digitales del rostro;

16) "datos biométricos", los datos dactiloscópicos y la imagen facial.».

3) En el artículo 5, se añade el apartado siguiente:

«1 *bis*. El RCDI contendrá los datos a que se refieren el artículo 9, apartado 4, letras a) a c *bis*); el artículo 9, apartado 5, y el artículo 9, apartado 6, y el resto de los datos del VIS se almacenarán en el VIS central.».

4) En el artículo 6, el apartado 2 se modifica del siguiente modo:

«2. El acceso al VIS para consultar los datos estará reservado exclusivamente al personal debidamente autorizado de las autoridades nacionales de cada Estado miembro que sean competentes para los fines establecidos en los artículos 15 a 22 y al personal debidamente autorizado de las autoridades de cada Estado miembro y de los organismos de la UE que sean competentes para los fines establecidos en [el artículo 20 y el artículo 21 del Reglamento 2018/XX sobre interoperabilidad], en la medida en que los datos sean necesarios para realizar sus tareas con arreglo a dichos fines y proporcionados con respecto a los objetivos perseguidos.».

5) En el artículo 9, punto 4, las letras a) a c) se modifican como sigue:

«a) apellido(s); nombre(s) (nombres de pila); fecha de nacimiento; nacionalidad o nacionalidades; sexo;

a *bis*) apellido(s) de nacimiento [apellido(s) anterior(es)]; fecha y país de nacimiento; nacionalidad de nacimiento;

b) tipo y número del documento o documentos de viaje y código de tres letras del país expedidor del documento o documentos de viaje;

c) fecha de expiración de la validez del documento o documentos de viaje;

c *bis*) autoridad que haya expedido el documento de viaje y fecha de expedición de este;».

6) En el artículo 9, el punto 5 se sustituye por el texto siguiente:

«una imagen facial tal como se define en el artículo 4, punto 15;».

7) En el artículo 29, apartado 2, letra a), las palabras «VIS central» se sustituyen por las palabras «VIS central o el RCDI» en los dos casos en que aparecen.

Artículo 55 sexies
Modificaciones de la Decisión 2008/633/JAI del Consejo

1) En el artículo 5, se añade el apartado 1 *bis* siguiente:

«1 *bis*. En los casos en que las autoridades designadas hayan iniciado una consulta al VIS de conformidad con [el artículo 22 del Reglamento 2018/XX sobre interoperabilidad], podrán acceder al VIS para consultarlo cuando la respuesta recibida a que se refiere el apartado 3 [del artículo 22 del Reglamento 2018/XX sobre interoperabilidad] ponga de manifiesto que los datos están almacenados en el VIS.».

2) En el artículo 7, se añade el apartado 1 *bis* siguiente:

«1 *bis*. En los casos en que Europol haya iniciado una consulta al VIS de conformidad con [el artículo 22 del Reglamento 2018/XX sobre interoperabilidad], podrá acceder al VIS para consultarlo cuando la respuesta recibida a que se refiere el apartado 3 [del artículo 22 del Reglamento 2018/XX sobre interoperabilidad] ponga de manifiesto que los datos están almacenados en el VIS.».

CAPÍTULO X
Disposiciones finales

Artículo 56
Presentación de informes y estadísticas

1. El personal debidamente autorizado de las autoridades competentes de los Estados miembros, la Comisión y eu-LISA tendrá acceso a la consulta de los datos siguientes en relación con el portal europeo de búsqueda (PEB), únicamente a efectos de la presentación de informes y estadísticas y sin que ello le otorgue competencias para la identificación individual:

   a) número de consultas por usuario del perfil del PEB;

   b) número de consultas de cada base de datos de Interpol.

2. El personal debidamente autorizado de las autoridades competentes de los Estados miembros, la Comisión y eu-LISA tendrá acceso a la consulta de los datos siguientes en relación con el registro común de datos de identidad, únicamente a efectos de la presentación de informes y estadísticas y sin que ello le otorgue competencias para la identificación individual:

   a) número de consultas a los efectos de los artículos 20, 21 y 22;

   b) nacionalidad, sexo y año de nacimiento de la persona;

   c) tipo de documento de viaje y código de tres letras del país de expedición;

   d) número de búsquedas realizadas con y sin datos biométricos.

3. El personal debidamente autorizado de las autoridades competentes de los Estados miembros, la Comisión y eu-LISA tendrá acceso a la consulta de los datos siguientes en relación con el detector de identidades múltiples, únicamente a efectos de la presentación de informes y estadísticas y sin que ello le otorgue competencias para la identificación individual:

   a) nacionalidad, sexo y año de nacimiento de la persona;

   b) tipo de documento de viaje y código de tres letras del país de expedición;

c) número de búsquedas realizadas con y sin datos biométricos;

d) número de cada tipo de vínculo.

4. El personal debidamente autorizado de la Agencia Europea de la Guardia de Fronteras y Costas, establecida por el Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo[76], tendrá acceso a la consulta de los datos a que se refieren los apartados 1, 2 y 3 con el fin de llevar a cabo los análisis de riesgos y la evaluación de la vulnerabilidad a que se hace referencia en los artículos 11 y 13 de dicho Reglamento.

5. A los efectos del apartado 1 del presente artículo, eu-LISA almacenará los datos a los que se refiere el apartado 1 del presente artículo en el repositorio central para la presentación de informes y estadísticas a que se refiere el capítulo VII del presente Reglamento. Los datos contenidos en el registro no harán posible la identificación de los individuos, pero permitirán a las autoridades enumeradas en el apartado 1 del presente artículo la elaboración de informes y estadísticas personalizados para mejorar la eficiencia de los controles fronterizos, para ayudar a las autoridades a tramitar las solicitudes de visado y para respaldar la elaboración de políticas basadas en pruebas en el ámbito de la migración y la seguridad en la Unión.

Artículo 57
Periodo transitorio para la utilización del portal europeo de búsqueda

Durante un periodo de dos años a partir de la fecha en que el PEB entre en funcionamiento, no serán de aplicación las obligaciones a que se refiere el artículo 7, apartados 2 y 4, y la utilización del PEB será facultativa.

Artículo 58
Periodo transitorio aplicable a las disposiciones sobre el acceso al registro común de datos de identidad con fines policiales

El artículo 22, el artículo 55 *ter*, puntos 13, 14, 15 y 16, y el artículo 55 *sexies* serán de aplicación a partir de la fecha de entrada en funcionamiento a que se refiere el artículo 62, apartado 1.

Artículo 59
Periodo transitorio para el detector de identidades múltiples

1. Durante un periodo de un año tras la notificación por parte de eu-LISA de la realización del ensayo al que se hace referencia en el artículo 62, apartado 1, letra b), relativo al detector de identidades múltiples (DIM) y antes de la entrada en funcionamiento del DIM, la unidad central SEIAV a que se refiere el [artículo 33, letra a), del Reglamento (UE) 2016/1624] se encargará de efectuar una detección de identidades múltiples entre los datos almacenados en el VIS, Eurodac y el SIS. Las detecciones de identidades múltiples se llevarán a cabo utilizando solamente datos biométricos, de conformidad con el artículo 27, apartado 2, del presente Reglamento.

[76] Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2016, sobre la Guardia Europea de Fronteras y Costas, por el que se modifica el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo y por el que se derogan el Reglamento (CE) n.º 863/2007 del Parlamento Europeo y del Consejo, el Reglamento (CE) n.º 2007/2004 del Consejo y la Decisión 2005/267/CE del Consejo (DO L 251 de 16.9.2016, p. 1).

2. Cuando la consulta dé lugar a una o varias respuestas positivas y los datos de identidad de los expedientes vinculados sean idénticos o similares, se creará un vínculo blanco de conformidad con el artículo 33.

Cuando la consulta dé lugar a una o varias respuestas positivas y los datos de identidad de los expedientes vinculados no puedan considerarse similares, se creará un vínculo amarillo de conformidad con el artículo 30 y será de aplicación el procedimiento a que se refiere el artículo 29.

Cuando se registren varias respuestas positivas, se creará un vínculo a cada uno de los datos que hayan dado lugar a una respuesta positiva.

3. Cuando se cree un vínculo amarillo, el DIM concederá a la unidad central SEIAV acceso a los datos de identidad presentes en los distintos sistemas de información.

4. Cuando se cree un vínculo a una descripción en el SIS, distinta de una descripción de denegación de entrada o una descripción relativa a un documento de viaje declarado perdido, robado o invalidado de conformidad con el artículo 24 del Reglamento sobre el SIS en el ámbito de los controles fronterizos y el artículo 38 del Reglamento sobre el SIS en el ámbito de la cooperación policial y judicial, respectivamente, el DIM concederá a la oficina SIRENE del Estado miembro que haya creado la descripción acceso a los datos de identidad presentes en los distintos sistemas de información.

5. La unidad central SEIAV o la oficina SIRENE del Estado miembro que haya creado la descripción tendrán acceso a los datos contenidos en el expediente de confirmación de identidad, evaluarán las diferentes identidades y actualizarán el vínculo con arreglo a los artículos 31, 32 y 33 y lo añadirán al expediente de confirmación de identidad.

6. La agencia eu-LISA prestará asistencia, cuando sea necesario, a la unidad central SEIAV en la detección de identidades múltiples a que se refiere el presente artículo.

Artículo 60
Costes

1. Los costes en que se incurra en relación con la creación y funcionamiento del PEB, el servicio de correspondencia biométrica compartido, el registro común de datos de identidad (RCDI) y el DIM correrán a cargo del presupuesto general de la Unión.

2. Los costes en que se incurra en relación con la integración de las infraestructuras nacionales existentes y su conexión a las interfaces nacionales uniformes, así como en relación con el alojamiento de las interfaces nacionales uniformes, correrán a cargo del presupuesto general de la Unión.

Quedan excluidos los costes siguientes:

a) la oficina de gestión del proyecto de los Estados miembros (reuniones, misiones, despachos);

b) el alojamiento de los sistemas informáticos nacionales (espacio, ejecución, electricidad, refrigeración);

c) el funcionamiento de los sistemas informáticos nacionales (operadores y contratos de apoyo);

d) el diseño, el desarrollo, la implementación, la explotación y el mantenimiento de las redes de comunicación nacionales.

3. Los costes en que incurran las autoridades designadas a que se refiere el artículo 4, apartado 24, correrán a cargo de cada Estado miembro y de Europol, respectivamente. Los costes generados por la conexión de las autoridades designadas al RCDI correrán a cargo de cada Estado miembro y Europol, respectivamente.

Artículo 61
Notificaciones

1. Los Estados miembros notificarán a eu-LISA las autoridades a que se refieren los artículos 7, 20, 21 y 26 que podrán utilizar el PEB, el RCDI y el DIM o tener acceso a ellos, respectivamente.

   La lista consolidada de dichas autoridades se publicará en el *Diario Oficial de la Unión Europea* en un plazo de tres meses a partir de la fecha en que cada componente de interoperabilidad entre en funcionamiento, de conformidad con el artículo 62. Cuando se modifique dicha lista, eu-LISA publicará una lista consolidada actualizada una vez al año.

2. La agencia eu-LISA notificará a la Comisión la realización satisfactoria del ensayo mencionado en el artículo 62, apartado 1, letra b).

3. La agencia eu-LISA notificará a la Comisión la realización satisfactoria de la medida transitoria establecida en el artículo 59.

4. La Comisión pondrá a disposición de los Estados miembros y del público, mediante un sitio web público constantemente actualizado, la información notificada de conformidad con el apartado 1.

Artículo 62
Entrada en funcionamiento

1. La Comisión decidirá la fecha a partir de la que cada componente de interoperabilidad debe entrar en funcionamiento, una vez que se cumplan las condiciones siguientes:

   a) que se hayan adoptado las medidas a que se refieren el artículo 8, apartado 2; el artículo 9, apartado 7; el artículo 28, apartados 5 y 6; el artículo 37, apartado 4; el artículo 38, apartado 4; el artículo 39, apartado 5; y el artículo 44, apartado 5;

   b) que eu-LISA haya declarado la realización satisfactoria de un ensayo global del componente de interoperabilidad pertinente, que eu-LISA debe llevar a cabo en cooperación con los Estados miembros;

   c) que eu-LISA haya validado las disposiciones legales y técnicas necesarias para recoger y transmitir los datos a que se refieren el artículo 8, apartado 1; el artículo 13; el artículo 19; el artículo 34 y el artículo 39 y las haya notificado a la Comisión;

   d) que los Estados miembros hayan efectuado las notificaciones a que se refiere el artículo 61, apartado 1, a la Comisión;

   e) en el caso del detector de identidades múltiples, que la unidad central SEIAV haya efectuado las notificaciones a que se refiere el artículo 61, apartado 3, a la Comisión.

2. La Comisión informará al Parlamento Europeo y al Consejo de los resultados del ensayo realizado de conformidad con el apartado 1, letra b).

3. La decisión de la Comisión contemplada en el apartado 1 se publicará en el *Diario Oficial de la Unión Europea*.

4. Los Estados miembros y Europol comenzarán a utilizar los componentes de interoperabilidad a partir de la fecha determinada por la Comisión de conformidad con el apartado 1.

Artículo 63
Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar los actos delegados mencionados en el artículo 8, apartado 2, y el artículo 9, apartado 7, se otorgan a la Comisión por un periodo de tiempo indefinido a partir de [*la fecha de entrada en vigor del presente Reglamento*].

3. La delegación de poderes mencionada en el artículo 8, apartado 2, y el artículo 9, apartado 7, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La Decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La Decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 8, apartado 2, y el artículo 9, apartado 7, entrarán en vigor únicamente si, en un plazo de [dos meses] desde su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará [dos meses] a iniciativa del Parlamento Europeo o del Consejo.

Artículo 64
Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 65
Grupo consultivo

La agencia eu-LISA creará un grupo consultivo que proporcionará conocimientos técnicos relacionados con la interoperabilidad, en particular en el contexto de la preparación de su programa de trabajo anual y de su informe de actividad anual. Durante la fase de diseño y desarrollo de los instrumentos de interoperabilidad, se aplicará el artículo 52, apartados 4 a 6.

Artículo 66
Formación

La agencia eu-LISA desempeñará las funciones relacionadas con la formación sobre el uso técnico de los componentes de interoperabilidad, de conformidad con el Reglamento (UE) n.º 1077/2011.

Artículo 67
Manual práctico

La Comisión, en estrecha cooperación con los Estados miembros, eu-LISA y otras agencias pertinentes, publicará un manual práctico de aplicación y gestión de los componentes de interoperabilidad. El manual práctico proporcionará orientaciones técnicas y operativas, recomendaciones y mejores prácticas. La Comisión adoptará el manual práctico en forma de recomendación.

Artículo 68
Supervisión y valoración

1. La agencia eu-LISA se asegurará de que se establezcan procedimientos para llevar a cabo la supervisión del desarrollo de los componentes de interoperabilidad a la luz de los objetivos en materia de planificación y costes, y de su funcionamiento a la luz de los objetivos en materia de resultados técnicos, rentabilidad, seguridad y calidad del servicio.

2. A más tardar [*seis meses después de la entrada en vigor del presente Reglamento* — la Oficina de Publicaciones insertará la fecha real], y posteriormente cada seis meses durante la fase de desarrollo de los componentes de interoperabilidad, eu-LISA presentará un informe al Parlamento Europeo y al Consejo sobre el estado de desarrollo de la interoperabilidad. Una vez finalizado el desarrollo, se presentará un informe al Parlamento Europeo y al Consejo en el que se explique con detalle cómo se han conseguido los objetivos, en particular en lo relativo a la planificación y los costes, y se justifique toda divergencia.

3. A efectos de mantenimiento técnico, eu-LISA tendrá acceso a la información necesaria relacionada con las operaciones de tratamiento de datos realizadas en los componentes de interoperabilidad.

4. Cuatro años después de la entrada en funcionamiento de cada componente de interoperabilidad y, posteriormente, cada cuatro años, eu-LISA presentará al Parlamento Europeo, al Consejo y a la Comisión un informe sobre el funcionamiento técnico de los componentes de interoperabilidad, incluida su seguridad.

5. Además, un año después de cada informe de eu-LISA, la Comisión realizará una valoración global de los componentes, que incluirá:

a) una evaluación de la aplicación del presente Reglamento;

b) un examen de los resultados alcanzados en comparación con los objetivos y de la repercusión sobre los derechos fundamentales;

c) una evaluación de la vigencia de los motivos que fundamentan los componentes de interoperabilidad;

d) una evaluación de la seguridad de los componentes de interoperabilidad;

e) una evaluación de las posibles consecuencias, incluida cualquier repercusión desproporcionada, en el flujo de tráfico en los pasos fronterizos y de aquellas consecuencias que tengan incidencia en el presupuesto de la Unión.

Las valoraciones incluirán todas las recomendaciones necesarias. La Comisión remitirá el informe de valoración al Parlamento Europeo, al Consejo, al Supervisor Europeo de Protección de Datos y a la Agencia de los Derechos Fundamentales de la Unión Europea, establecida por el Reglamento (CE) n.º 168/2007 del Consejo[77].

6. Los Estados miembros y Europol proporcionarán a eu-LISA y a la Comisión la información necesaria para elaborar los informes a que se refieren los apartados 4 y 5. Esta información no deberá nunca poner en riesgo los métodos de trabajo ni incluir datos que revelen fuentes, miembros del personal o investigaciones de las autoridades designadas.

7. La agencia eu-LISA facilitará a la Comisión la información necesaria para realizar las valoraciones a que se refiere el apartado 5.

8. Con pleno respeto de las disposiciones de la legislación nacional en materia de publicación de información sensible, cada Estado miembro y Europol prepararán informes anuales sobre la eficacia del acceso a los datos almacenados en el registro común de datos de identidad a efectos con fines policiales, que comprenderán información y estadísticas sobre:

a) la finalidad exacta de la consulta, incluido el tipo del delito de terrorismo u otro delito grave;

b) los motivos razonables alegados para la sospecha fundada de que el sospechoso, el autor o la víctima están cubiertos por el [Reglamento SES], el Reglamento VIS o el [Reglamento SEIAV];

c) el número de solicitudes de acceso al registro común de datos de identidad con fines policiales;

d) el número y tipo de casos que hayan resultado en una identificación positiva;

e) la necesidad y el recurso al caso de urgencia excepcional, incluyendo aquellos casos en los que la urgencia no fue aceptada por la verificación efectuada a posteriori por el punto de acceso central.

Los informes anuales de los Estados miembros y de Europol se remitirán a la Comisión antes del 30 de junio del año siguiente.

[77] Reglamento (CE) n.º 168/2007 del Consejo, de 15 de febrero de 2007, por el que se crea una Agencia de los Derechos Fundamentales de la Unión Europea (DO L 53 de 22.2.2007, p. 1).

Artículo 69
Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en los Estados miembros de conformidad con los Tratados.

Hecho en Estrasburgo, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA

1.3. Naturaleza de la propuesta/iniciativa

1.4. Objetivo(s)

1.5. Justificación de la propuesta/iniciativa

1.6. Duración e incidencia financiera

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema de gestión y de control

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

3.2.2. Incidencia estimada en los créditos de operaciones

3.2.3. Incidencia estimada en los créditos de carácter administrativo

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE relativos a la gestión de la seguridad, las fronteras y la migración.

1.2. Ámbito(s) político(s) afectado(s)

Asuntos de Interior (Título 18).

1.3. Naturaleza de la propuesta/iniciativa

X La propuesta/iniciativa se refiere a **una acción nueva**

☐ La propuesta/iniciativa se refiere a **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[78]

☐ La propuesta/iniciativa se refiere a **la prolongación de una acción existente**

☐ La propuesta/iniciativa se refiere a **una acción reorientada hacia una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivos estratégicos plurianuales de la Comisión contemplados por la propuesta/iniciativa

Gestión de las fronteras: salvar vidas y proteger las fronteras exteriores

Los componentes de interoperabilidad brindan la oportunidad de hacer un mejor uso de la información contenida en los sistemas de la UE existentes para la gestión de la seguridad, las fronteras y la migración. Estas medidas evitan, principalmente, que una misma persona se registre en diferentes sistemas con diferentes identidades. En la actualidad, la identificación única de una persona es posible dentro de un determinado sistema, pero no entre los distintos sistemas. Esta deficiencia puede dar lugar a decisiones erróneas de las autoridades o, por el contrario, ser utilizada por viajeros de mala fe para ocultar su identidad real.

Mejor intercambio de información

Las medidas propuestas también prevén un acceso racionalizado, aunque limitado, de los cuerpos policiales a estos datos. Pero, a diferencia de lo que ocurre hoy día, se establece un único conjunto de condiciones en lugar de condiciones diferentes para acceder a cada base de datos.

1.4.2. Objetivo(s) específico(s) y objetivo específico n.º[ ]

La creación de los componentes de interoperabilidad tiene los objetivos generales siguientes:

a) mejorar la gestión de las fronteras exteriores;

b) contribuir a la prevención y la lucha contra la migración irregular y

[78] Tal como se contempla en el artículo 54, apartado 2, letra a) o b), del Reglamento Financiero.

c) contribuir a un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, incluido el mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros.

Los objetivos que persigue la garantía de la interoperabilidad de los servicios se alcanzarán:

a) garantizando la identificación correcta de las personas;

b) contribuyendo a la lucha contra la usurpación de identidad;

c) mejorando y armonizando los requisitos de calidad de los datos de los respectivos sistemas de información de la UE;

d) facilitando la implementación operativa y técnica por los Estados miembros de los sistemas de información existentes y futuros de la Unión;

e) reforzando, simplificando y uniformando las condiciones de protección y seguridad de los datos que rigen en los respectivos sistemas de información de la UE;

f) simplificando y uniformando las condiciones de acceso de los cuerpos policiales al VIS, el SES, el SEIAV y Eurodac;

g) apoyando los fines del SES, el SEIAV, el VIS, Eurodac, el SIS y el sistema ECRIS-TCN.

Actividad(es) GPA/PPA afectada(s)

Capítulo de seguridad y defensa de las libertades: seguridad interior

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios/la población destinataria.

Los objetivos generales de esta iniciativa se derivan de dos objetivos basados en el Tratado:

1. Mejorar la gestión de las fronteras exteriores del espacio Schengen, sobre la base de la Agenda Europea de Migración y las comunicaciones posteriores, incluida la Comunicación sobre la protección y el refuerzo del espacio Schengen.

2. Contribuir a la seguridad interior de la Unión Europea, sobre la base de la Agenda Europea de Seguridad y el trabajo de la Comisión en pro de una Unión de la Seguridad genuina y efectiva.

Los objetivos específicos de la presente iniciativa de interoperabilidad son:

1. garantizar que los usuarios finales, en particular los guardias de fronteras, la policía, los funcionarios de inmigración y las autoridades judiciales tengan un acceso rápido, ininterrumpido, sistemático y controlado a la información que necesitan para desempeñar sus tareas;

2. aportar una solución para detectar las identidades múltiples vinculadas al mismo conjunto de datos biométricos, con la doble finalidad de garantizar la correcta identificación de las personas de buena fe y de luchar contra la usurpación de identidad;

3. facilitar los controles de identidad de los nacionales de terceros países, en el territorio de un Estado miembro, por las autoridades policiales y

4. facilitar y racionalizar el acceso de los cuerpos policiales a los sistemas de información no policiales a escala de la UE, cuando sea necesario con fines de prevención, investigación, detección o enjuiciamiento de los delitos graves y de terrorismo.

Para cumplir el objetivo específico n.º 1, se creará el portal europeo de búsqueda (PEB).

Para cumplir el objetivo específico n.º 2, se creará el detector de identidades múltiples (DIM), con el apoyo de un registro común de datos de identidad (RCDI) y el servicio de correspondencia biométrica compartido (SCB compartido).

Para cumplir el objetivo específico n.º 3, se permitirá el acceso al RCDI a agentes autorizados a efectos de identificación.

Para cumplir el objetivo n.º 4, el RCDI contendrá una funcionalidad de aviso de respuesta positiva que permitirá un planteamiento en dos fases del acceso de los cuerpos policiales a los sistemas de gestión de fronteras.

Además de estos cuatro componentes de interoperabilidad, se respaldará la consecución de los objetivos descritos en la sección 1.4.2 mediante el establecimiento y la gobernanza del formato universal de mensajes (UMF), como norma de la UE para el desarrollo de los sistemas de información en el ámbito de la justicia y de los asuntos de interior, y la creación de un repositorio común para la presentación de informes y estadísticas (RCIE).

1.4.4. Indicadores de los resultados e incidencia

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

Cada una de las medidas propuestas requiere el desarrollo, seguido del mantenimiento y funcionamiento, de un componente.

Durante el desarrollo

Cada componente se desarrollará una vez que se cumplan los requisitos previos, es decir, que la propuesta legislativa sea adoptada por los colegisladores y se reúnan las condiciones técnicas previas necesarias, ya que algunos componentes solo podrán construirse cuando se disponga de otros.

Objetivo específico: aptitud para entrar en funcionamiento en la fecha prevista

A finales de 2017, la propuesta se envía a los colegisladores para su adopción. Se supone que el proceso de adopción concluirá en 2018, por analogía con el tiempo que se necesitó para la adopción de otras propuestas.

Con arreglo a este supuesto, el inicio del periodo de desarrollo se fija al comienzo de 2019 (= T0) con el fin de disponer de un punto de referencia a partir del cual se calculen los plazos, en lugar de fechas absolutas. Si la adopción por los colegisladores tuviera lugar en una fecha posterior, todo el calendario se modificaría en consecuencia. Por otra parte, el SCB compartido tiene que estar disponible para que puedan desarrollarse el RCDI y el DIM. Los plazos de desarrollo se indican en el cuadro siguiente:

	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
	Adopción de la propuesta legislativa		**Enero de 2021 SES SCB disponibles**						
Gestión de programas									
RCIE									
PEB (portal europeo de búsqueda)									
SCB compartido									
Migración de Eurodac, SIS, ECRIS									
RCDI (registro común de datos de identidad)									
Incorporación de Eurodac y ECRIS al RCDI									
DIM (detector de identidades múltiples)									
Validación manual de									

vínculos			

(El bloque amarillo se refiere a una tarea específica de Eurodac).

— Repositorio común para la presentación de informes y estadísticas (RCIE): fecha de entrega: T0 + 12 meses (2019-2020).

— Portal europeo de búsqueda (PEB): fecha de entrega: T0 + 36 meses (2019-2021).

— El servicio de correspondencia biométrica compartido (SCB compartido) se crea en primer lugar para entregar el Sistema de Entradas y Salidas (SES). Cuando se alcance esta fase, las aplicaciones que utilicen el SCB compartido deberán actualizarse y los datos contenidos en el sistema automático de identificación dactilar (SAID) del SIS, el SAID de Eurodac y ECRIS-TCN deberán exportarse al SCB compartido. La fecha límite de entrega es el final de 2023.

— El registro común de datos de identidad (RCDI) se creará durante la implementación del SES. Cuando el SES esté finalizado, los datos de Eurodac y ECRIS se incorporarán al RCDI. La fecha límite de entrega es el final de 2022 (disponibilidad del SCB compartido + 12 meses).

El detector de identidades múltiples (DIM) se creará cuando el RCDI entre en funcionamiento. La fecha de entrega es el final de 2022 (disponibilidad del SCB compartido + 24 meses), pero hay que contar con un periodo en el que habrá que movilizar muchos recursos para validar los vínculos entre identidades propuestos por el DIM. Cada enlace examinado deberá validarse manualmente. Esta tarea se llevará a cabo hasta el final de 2023.

El periodo de funcionamiento comenzará una vez concluido el periodo de desarrollo antes mencionado.

Funcionamiento

Los indicadores correspondientes a cada uno de los objetivos específicos mencionados en el punto 1.4.3 son los siguientes:

Objetivo específico n.º 1: Acceso rápido, ininterrumpido y sistemático a fuentes de datos autorizadas

- Número de casos de uso ejecutados (= número de consultas que pueden tramitarse a través del PEB) por periodo de tiempo.

- Número de consultas tramitadas por el PEB en comparación con el número total de búsquedas (a través del PEB y de los sistemas directamente) por periodo de tiempo.

Objetivo específico n.º 2: Detector de identidades múltiples

- Número de identidades vinculadas al mismo conjunto de datos biométricos comparado con el número de identidades con información biográfica por periodo de tiempo.

- Número de casos detectados de usurpación de identidad en comparación con el número de datos de identidad vinculados y el número total de datos de identidad por periodo de tiempo.

Objetivo específico n.º 3: Facilitar la identificación de los nacionales de terceros países

- Número de controles de identificación realizados en comparación con el número total de transacciones por periodo de tiempo.

Objetivo específico n.º 4: Simplificar el acceso a las fuentes de datos autorizadas a efectos policiales

— Número de accesos en la «fase 1» (= control de presencia de datos) a efectos policiales por periodo de tiempo.

- Número de accesos en la «fase 2» (= consulta efectiva de los datos procedentes de los sistemas de la UE dentro del ámbito de aplicación) a efectos policiales por periodo de tiempo.

5. Objetivo transversal adicional: Mejora de la calidad de los datos y uso de los datos para una mejor elaboración de las políticas

- Presentación de informes periódicos de control de calidad de los datos.

- Número de solicitudes *ad hoc* de información estadística por periodo de tiempo.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo

Como queda demostrado en la evaluación de impacto que acompaña a la presente propuesta legislativa, los respectivos componentes propuestos son necesarios para lograr la interoperabilidad:

• Para cumplir el objetivo de ofrecer a los usuarios autorizados un acceso rápido, ininterrumpido, sistemático y controlado a los sistemas de información pertinentes, debe crearse un portal europeo de búsqueda (PEB), basado en un SCB compartido, que permita consultar todas las bases de datos.

• Para cumplir el objetivo de facilitar los controles de identidad de los nacionales de terceros países, en el territorio de un Estado miembro, por los agentes autorizados, debe crearse un registro común de datos de identidad (RCDI) que contenga el conjunto mínimo de datos de identificación y se base en el mismo SCB compartido.

• Para cumplir el objetivo de detectar identidades múltiples vinculadas al mismo conjunto de datos biométricos, con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y de luchar contra la usurpación de identidad, debe crearse un detector de identidades múltiples (DIM) que contenga los vínculos entre las identidades múltiples en los distintos sistemas.

• Para cumplir el objetivo de facilitar y racionalizar el acceso de los cuerpos policiales a los sistemas de información no policiales, con el fin de prevenir, investigar, detectar o enjuiciar los delitos graves y de terrorismo, debe crearse una funcionalidad de «aviso de correspondencia» en el registro común de datos de identidad (RCDI).

Dado que todos los objetivos deben cumplirse, la solución completa es la combinación de PEB, RCDI (con aviso de correspondencia) y DIM, todos ellos basados en el SCB compartido.

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como, por ejemplo, coordinación, seguridad jurídica, mayor eficacia o las complementariedades). A los efectos de este punto, se entenderá por «valor añadido

de la intervención de la Unión» el valor resultante de una intervención de la Unión que se sume al valor que se hubiera generado de haber actuado los Estados miembros de forma aislada.

Es necesario actuar a escala europea, ya que los sistemas que se propone hacer interoperables son utilizados por numerosos Estados miembros: todos los Estados miembros (en el caso de Eurodac) o todos los Estados miembros que forman parte del espacio Schengen (SES, VIS, SEIAV y SIS). Por definición, simplemente no se puede actuar a otra escala.

El principal valor añadido previsto es acabar con los casos de usurpación de identidad, establecer el mapa de los casos en que una persona ha hecho uso de identidades diferentes al entrar en la UE y evitar que personas de buena fe sean confundidas con personas de mala fe que tengan el mismo nombre. Un valor añadido adicional es que la interoperabilidad propuesta permite una implementación y un mantenimiento más fáciles de los sistemas informáticos de gran magnitud de la UE. Para los servicios policiales, las medidas propuestas deben dar lugar a un acceso más frecuente y provechoso a datos concretos en los sistemas informáticos de gran magnitud de la UE. A nivel operativo, la calidad de los datos solo puede mantenerse y mejorarse si es objeto de seguimiento. Además, para la elaboración de políticas y la toma de decisiones, es necesario permitir la realización de consultas *ad hoc* de datos anonimizados.

Un análisis coste-beneficio forma parte de la evaluación de impacto, y si solo se tienen en cuenta los beneficios que pueden cuantificarse, cabe estimar razonablemente los beneficios esperados en unos 77,5 millones EUR anuales, principalmente para los Estados miembros. Estos beneficios consisten fundamentalmente en:

— coste reducido de los cambios en las aplicaciones nacionales cuando el sistema central esté en funcionamiento (estimado en 6 millones EUR anuales para los departamentos informáticos de los Estados miembros);

— ahorro de costes por tener un SCB compartido central en lugar de un SCB para cada sistema central que contenga datos biométricos (estimado en 1,5 millones EUR anuales y un ahorro único de 8 millones EUR para eu-LISA);

— ahorro del coste de identificación de identidades múltiples, en comparación con la situación en que se lograría el mismo resultado sin los medios propuestos. Esto representaría un ahorro de costes de al menos 50 millones EUR anuales para las administraciones de los Estados miembros en la gestión de las fronteras, la migración y el orden público;

— ahorro de costes de formación de un amplio grupo de usuarios finales, en comparación con la situación en que se requiere formación de forma recurrente, estimado en 20 millones EUR anuales para las administraciones de los Estados miembros en la gestión de las fronteras, la migración y el orden público.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La experiencia adquirida con el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II) y del Sistema de Información de Visados (VIS) ha permitido extraer las enseñanzas siguientes:

1. Como posible salvaguardia frente a los sobrecostes y los retrasos resultantes de los requisitos cambiantes, no debe desarrollarse ningún nuevo sistema de información en

el espacio de libertad, seguridad y justicia, especialmente si se trata de un sistema informático de gran magnitud, antes de que hayan sido definitivamente adoptados los instrumentos jurídicos subyacentes que establezcan su finalidad, alcance, funciones y especificaciones técnicas.

2. En el caso del SIS II y el VIS, el desarrollo nacional en los Estados miembros podía ser cofinanciado por el Fondo para las Fronteras Exteriores (FFE), aunque no era obligatorio. Por ese motivo, resultaba imposible tener una visión de conjunto del grado de avance en los Estados miembros que no habían contemplado las actividades correspondientes en su programación plurianual o cuya programación adolecía de falta de precisión. Por tanto, se propone ahora que la Comisión reembolse todos los gastos de integración sufragados por los Estados miembros con el fin de poder supervisar el avance de estos desarrollos.

3. Con vistas a facilitar la coordinación general de la implementación, todos los intercambios de mensajes propuestos entre los sistemas nacionales y centrales reutilizarán las redes existentes y la interfaz uniforme nacional.

1.5.4. Compatibilidad y posibles sinergias con otros instrumentos adecuados

Compatibilidad con el marco financiero plurianual vigente

El Reglamento FSI-Fronteras es el instrumento financiero en el que se ha incluido el presupuesto para la ejecución de la iniciativa de interoperabilidad.

Su artículo 5, letra b), dispone que se destinarán 791 millones EUR a un programa de desarrollo de sistemas informáticos basado en sistemas existentes o nuevos, en apoyo a la gestión de los flujos migratorios en las fronteras exteriores, a reserva de la adopción de los actos legislativos de la Unión pertinentes y con arreglo a las condiciones establecidas en el artículo 15. De esos 791 millones EUR, 480,2 millones EUR están reservados para el desarrollo del SES, 210 millones EUR para el SEIAV y 67,9 millones EUR para la revisión del SIS II. El resto (32,9 millones EUR) se reasignará utilizando los mecanismos FSI-F. La propuesta actual implica un gasto de 32,1 millones EUR con cargo al marco financiero plurianual vigente, que se cubre con el saldo presupuestario.

La propuesta actual implica una dotación presupuestaria total de 424,7 millones EUR (rúbrica 5) durante el periodo comprendido entre 2019 y 2027. El marco financiero plurianual (MFP) vigente solo abarca dos años, 2019 y 2020. Los costes se han calculado, no obstante, hasta 2027 inclusive, para dar una información sólida de las consecuencias financieras de la presente propuesta, sin perjuicio del próximo marco financiero plurianual.

El presupuesto solicitado para nueve años asciende a 424,7 millones EUR, desglosados en los siguientes elementos:

1) 136,3 millones EUR para que los Estados miembros realicen los cambios necesarios en sus sistemas nacionales con objeto de utilizar los componentes de interoperabilidad, la INU desarrollada por eu-LISA y la formación de una comunidad de usuarios finales esencial. No hay ningún impacto sobre el MFP vigente dado que la financiación se facilitará a partir de 2021.

2) 4,8 millones EUR para que la Agencia de la GEFC aloje un equipo de especialistas que, durante un año (2023), validará los vínculos entre identidades en el momento en que el DIM entre en funcionamiento. Las actividades del equipo pueden asociarse a la labor de desambiguación de identidades atribuida a la Agencia de la

GEFC en el marco de la propuesta relativa al SEIAV. No hay ningún impacto sobre el MFP vigente dado que la financiación se facilitará a partir de 2021.

3) 48,9 millones EUR para que Europol financie la mejora de sus sistemas informáticos en consonancia con el volumen de mensajes que deberán tratarse y los niveles de rendimiento más elevados requeridos. Los componentes de interoperabilidad serán utilizados por el SEIAV con el fin de consultar los datos de Europol. Sin embargo, la actual capacidad de tratamiento de información de Europol no es conforme con los grandes volúmenes (media de 100 000 consultas diarias) y el menor tiempo de respuesta. Está previsto un gasto de 9,1 millones EUR con cargo al MFP actual.

4) 2,0 millones EUR para que la CEPOL prepare e imparta la formación del personal operativo. Está previsto un gasto de 0,1 millones EUR en 2020.

5) 225,0 millones EUR para eu-LISA, que cubren el coste total de ejecución del programa de desarrollo de los cinco componentes de interoperabilidad (68,3 millones EUR), el coste de mantenimiento desde el momento en que los componentes se entreguen hasta 2027 (56,1 millones EUR), un presupuesto específico de 25,0 millones EUR para la migración de los datos de los sistemas existentes al SCB compartido y los costes adicionales de actualización de la INU, redes, formación y reuniones. Un presupuesto específico de 18,7 millones EUR cubre el coste de actualización y funcionamiento del ECRIS-TCN en modo de alta disponibilidad a partir de 2022. De la dotación total, está previsto gastar 23,0 millones EUR en el transcurso del actual MFP.

6) 7,7 millones EUR para que la DG HOME financie un aumento limitado de personal y los costes conexos durante el periodo de desarrollo de los diversos componentes, puesto que la Comisión también será responsable del comité que se ocupará del formato universal de mensajes (UMF). Este presupuesto, que se inscribe en la rúbrica 5, no será financiado con cargo al presupuesto del FSI. Para información, se ha comprometido el gasto de 2,0 millones EUR a lo largo del periodo 2019-2020.

Compatibilidad con iniciativas previas

Esta iniciativa es compatible con lo siguiente:

En abril de 2016, la Comisión presentó la **Comunicación *Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad*** con el fin de solventar una serie de deficiencias estructurales de los sistemas de información. Dio lugar a tres actuaciones:

En primer lugar, la Comisión tomó **medidas para reforzar y maximizar los beneficios de los sistemas de información existentes**. En diciembre de 2016, la Comisión adoptó propuestas para reforzar el actual Sistema de Información de Schengen (SIS). Entre tanto, a raíz de la propuesta de la Comisión de mayo de 2016, se aceleraron las negociaciones para la revisión de la base jurídica de Eurodac, la base de datos de impresiones dactilares relacionadas con las solicitudes de asilo de la UE. También está en preparación una propuesta de una nueva base jurídica para el Sistema de Información de Visados (VIS), que se presentará en el segundo trimestre de 2018.

En segundo lugar, la Comisión propuso **sistemas de información adicionales para colmar las lagunas detectadas** en la arquitectura de gestión de datos de la UE. Las negociaciones sobre la propuesta de la Comisión, de abril de 2016, para establecer un

Sistema de Entradas y Salidas (SES)[79] con el objeto de mejorar los procedimientos de control fronterizo de los nacionales de terceros países que viajen a la UE, concluyeron en julio de 2017, cuando los colegisladores llegaron a un acuerdo político, confirmado por el Parlamento Europeo en octubre de 2017 y adoptado formalmente por el Consejo en noviembre de 2017. En noviembre de 2016, la Comisión presentó también una propuesta para el establecimiento de un Sistema Europeo de Información y Autorización de Viajes (SEIAV)[80]. El objetivo de esta propuesta consiste en reforzar los controles de seguridad de los viajeros exentos de la obligación de visado al permitir controles anticipados de migración irregular y seguridad. Se encuentra actualmente en fase de negociación por los colegisladores. En junio de 2017, también se propuso el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)[81] para solucionar la disparidad detectada en el intercambio de información entre los Estados miembros sobre las condenas de nacionales de terceros países.

En tercer lugar, la Comisión trabajó para lograr **la interoperabilidad de los sistemas de información**, centrándose en las cuatro opciones presentadas en la Comunicación de abril de 2016[82] con vistas a asegurar la interoperabilidad. Tres de las cuatro opciones son precisamente el PEB, el RCDI y el SCB compartido. Quedó de manifiesto posteriormente que era preciso establecer una distinción entre el RCDI como base de datos de identidad y un nuevo componente que detecte las identidades múltiples vinculadas a un mismo identificador biométrico (DIM). Por lo tanto, los cuatro componentes son: el PEB, el RCDI, el DIM y el SCB compartido.

Sinergia

Por sinergia se entiende aquí el beneficio obtenido por la reutilización de las soluciones existentes y el ahorro de nuevas inversiones.

Existe una gran sinergia entre estas iniciativas y el desarrollo del SES y el SEIAV.

Para el funcionamiento del SES, se creará un expediente individual de todos los nacionales de terceros países que entren en el espacio Schengen para una estancia de corta duración. A tal efecto, el actual sistema de correspondencias biométricas utilizado para el VIS, que contiene las plantillas de las impresiones dactilares de todos los viajeros a los que se exige visado, se ampliará para incluir también los datos biométricos de los viajeros exentos de visado. El SCB compartido es, por lo tanto, conceptualmente una generalización ulterior del sistema de correspondencias biométricas que se va a desarrollar como parte del SES. Las plantillas biométricas contenidas en el sistema de correspondencias biométricas del SIS y de Eurodac serán, por tanto, migradas (este es el término técnico cuando los datos se trasladan de un sistema a otro) al SCB compartido. Según los datos de los proveedores, el almacenamiento en bases de datos independientes cuesta una media de 1 EUR por conjunto de datos biométricos (potencialmente, existen 200 millones de conjuntos de datos en total), mientras que el coste medio se reduce a 0,35 EUR por conjunto de datos biométricos si se crea un SCB compartido. El coste más elevado del material informático necesario para tratar un gran volumen de datos compensa parcialmente estos beneficios, pero se calcula que al final el coste de un SCB compartido será un

79 COM(2016) 194 de 6 de abril de 2016.
80 COM(2016) 731 de 16 de noviembre de 2016.
81 COM(2017) 344 de 29 de junio de 2017.
82 COM(2016) 205 de 6 de abril de 2016.

30 % inferior al coste de almacenar los mismos datos en múltiples sistemas de menores dimensiones que el SCB compartido.

Para el funcionamiento del SEIAV, se necesita un componente para consultar un conjunto de sistemas de la UE. Podrá utilizarse el PEB o desarrollarse un componente específico como parte de la propuesta del PEB. La propuesta de interoperabilidad permite desarrollar un componente, en lugar de dos.

Se logra asimismo una sinergia mediante la reutilización de la misma interfaz nacional uniforme (INU) que se utilice para el SES y el SEIAV. La INU habrá de actualizarse, pero seguirá utilizándose.

1.6. Duración e incidencia financiera

☐ Propuesta/iniciativa de **duración limitada**

- ☐ Propuesta/iniciativa en vigor desde [el] [DD.MM]AAAA hasta [el] [DD.MM]AAAA
- ☐ Incidencia financiera desde AAAA hasta AAAA

☒ Propuesta/iniciativa de **duración ilimitada**

- Periodo de desarrollo de 2019 a 2023 inclusive, seguido del pleno funcionamiento.
- Duración de la incidencia financiera estimada de 2019 a 2027.

1.7. Modo(s) de gestión previstos[83]

☒**Gestión directa** a cargo de la Comisión

- X por sus servicios, incluido su personal en las Delegaciones de la Unión;
- ☐ por las agencias ejecutivas.

☒ **Gestión compartida** con los Estados miembros

☒ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

- ☐ terceros países o los organismos que estos hayan designado;
- ☐ organizaciones internacionales y sus agencias (especifíquense);
- ☐ el BEI y el Fondo Europeo de Inversiones;
- ☒ los organismos a que se hace referencia en los artículos 208 y 209 del Reglamento Financiero;
- ☐ organismos de Derecho público;
- ☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que presenten garantías financieras suficientes;
- ☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;

[83] Las explicaciones sobre los modos de gestión y las referencias al Reglamento financiero pueden consultarse en el sitio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la PESC, de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

– *Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.*

Observaciones

Bloques	Fase de desarrollo	Fase de funcionamiento	Modo de gestión	Actor
Desarrollo y mantenimiento (de los componentes de interoperabilidad de los sistemas centrales, formación en el sistema)	X	X	Indirecta	eu-LISA Europol CEPOL
Migración de datos (migración de las plantillas biométricas al SCB compartido), costes de la red, actualización de la INU, reuniones y formación	X	X	Indirecta	eu-LISA
Validación de vínculos al crear el DIM	X	—	Indirecta	GEFC
Adaptación de la INU, integración de los sistemas nacionales y formación de los usuarios finales	X	X	Compartida (o directa) (1)	COM + Estados miembros

1) No hay importes para la fase de funcionamiento incluida en este instrumento.

La fase de desarrollo se inicia en 2019 y se extiende hasta la entrega de cada componente, entre 2019 y 2023 (véase la sección 1.4.4).

1. Gestión directa por la DG HOME: durante la fase de desarrollo, en caso necesario, la Comisión también podrá ejecutar directamente medidas, que podrían incluir, en particular, la ayuda financiera de la Unión a las actividades en forma de subvenciones (también a las autoridades nacionales de los Estados miembros), los contratos públicos o el reembolso de los gastos realizados por los expertos externos.

2. Gestión compartida: durante la fase de desarrollo, los Estados miembros tendrán que adaptar sus sistemas nacionales a fin de acceder al PEB, en vez de a los sistemas individuales (mensajes salientes de los Estados miembros), y adecuarse a los cambios en las respuestas a sus solicitudes de búsqueda (mensajes entrantes en los Estados miembros). Se actualizará también la INU actual del SES y el SEIAV.

3. Gestión indirecta: eu-LISA se encargará del desarrollo de todos los aspectos informáticos del proyecto, es decir, los componentes de interoperabilidad, la actualización de la interfaz nacional uniforme (INU) de cada Estado miembro, la actualización de la infraestructura de comunicación entre los sistemas centrales y las interfaces nacionales uniformes, la migración de las plantillas biométricas de los actuales sistemas de correspondencia de datos biométricos del SIS y Eurodac al SCB compartido y la limpieza de datos correspondiente.

Durante la fase de funcionamiento, eu-LISA desempeñará todas las actividades técnicas relacionadas con el mantenimiento de los componentes.

La Agencia de la Guardia Europea de Fronteras y Costas (GEFC) incorporará un equipo adicional dedicado a la validación de los vínculos una vez que el DIM entre en funcionamiento. Se trata de una tarea de duración limitada.

Europol se ocupará del desarrollo y el mantenimiento de sus sistemas para garantizar la interoperabilidad con el PEB y el SEIAV.

CEPOL preparará y suministrará la formación a los servicios operativos con un enfoque de formación de formadores.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones.

Normas de seguimiento e información para el desarrollo y el mantenimiento de otros sistemas:

1. La agencia eu-LISA se asegurará de que se establezcan procedimientos para supervisar el desarrollo de los componentes de interoperabilidad a la luz de los objetivos en materia de planificación y costes, y su funcionamiento a la luz de los objetivos en materia de resultados técnicos, rentabilidad, seguridad y calidad del servicio.

2. En el plazo de seis meses desde la entrada en vigor del presente Reglamento y posteriormente cada seis meses durante la fase de desarrollo de los componentes, eu-LISA presentará un informe al Parlamento Europeo y al Consejo sobre el estado de desarrollo de cada componente. Una vez finalizado el desarrollo, presentará un informe al Parlamento Europeo y al Consejo en el que se explique con detalle cómo se han alcanzado los objetivos, en particular en materia de planificación y costes, y se justifique toda divergencia.

3. A efectos del mantenimiento técnico, eu-LISA tendrá acceso a la información necesaria relacionada con las operaciones de tratamiento de datos que se realicen en los componentes.

4. Cuatro años después del inicio del funcionamiento del último componente implementado y posteriormente cada cuatro años, eu-LISA presentará al Parlamento Europeo, al Consejo y a la Comisión un informe sobre el funcionamiento técnico de los componentes.

5. Cada cinco años desde el inicio del funcionamiento del último componente implementado y posteriormente cada cuatro años, la Comisión elaborará una valoración global y formulará las recomendaciones necesarias. Esta evaluación global incluirá: los resultados obtenidos por los componentes en relación con los objetivos de la interoperabilidad, la facilidad de mantenimiento, el rendimiento y las implicaciones financieras, así como el impacto en los derechos fundamentales.

La Comisión remitirá el informe de evaluación al Parlamento Europeo y al Consejo.

6. Los Estados miembros y Europol suministrarán a eu-LISA y a la Comisión la información necesaria para elaborar los informes a que se refieren los apartados 4 y 5 con arreglo a los indicadores cuantitativos previamente definidos por la Comisión o eu-LISA. Esta información no deberá nunca poner en peligro los métodos de trabajo ni incluir datos que revelen fuentes, la identidad de miembros del personal o investigaciones de las autoridades designadas.

7. eu-LISA proporcionará a la Comisión la información necesaria para elaborar las evaluaciones globales a que se refiere el apartado 5.

8. Sin perjuicio de las disposiciones de la legislación nacional en materia de publicación de información sensible, cada Estado miembro y Europol prepararán informes anuales sobre la eficacia del acceso a los sistemas de la UE a efectos policiales, que incluirán información y estadísticas sobre:

- la finalidad exacta de la consulta, incluido el tipo de delito de terrorismo u otro delito grave;

- los motivos razonables alegados para la sospecha fundada de que el sospechoso, el autor o la víctima están cubiertos por el presente Reglamento;

- el número de solicitudes de acceso a los componentes con fines policiales;

- el número y tipo de casos que hayan arrojado identificaciones positivas;

- la necesidad y la utilización del recurso excepcional de urgencia, incluyendo aquellos casos en los que la urgencia no fue aceptada por la verificación efectuada *a posteriori* por el punto de acceso central.

Los informes anuales de Europol y de los Estados miembros se remitirán a la Comisión antes del 30 de junio del año siguiente.

2.2. Sistema de gestión y control

2.2.1. Riesgo(s) definido(s)

Los riesgos son los relacionados con el desarrollo informático de los cinco componentes por un contratista externo gestionado por eu-LISA. Son los típicos riesgos de los proyectos:

1. el riesgo de no completar el proyecto en el plazo previsto;

2. el riesgo de no completar el proyecto dentro de los límites del presupuesto;

3. el riesgo de no entregar la totalidad del proyecto.

El primer riesgo es el más importante porque todo retraso genera un incremento de los costes, dado que los costes tienen relación con el plazo: costes de personal, costes de las licencias anuales, etc.

Esos riesgos pueden mitigarse mediante técnicas de gestión del proyecto, incluidos los imprevistos en los proyectos de desarrollo y una dotación de personal suficiente para poder absorber los picos de trabajo. La estimación del esfuerzo se suele calcular suponiendo una carga de trabajo igual a lo largo del tiempo, mientras que la realidad de los proyectos es la desigualdad de la carga de trabajo, que es absorbida por un aumento de las asignaciones de recursos.

Existen varios riesgos relacionados con el uso de un contratista externo para esta labor de desarrollo:

1, en particular, el riesgo de que el contratista no asigne suficientes recursos al proyecto o diseñe y desarrolle un sistema que no sea de vanguardia;

2. el riesgo de que el contratista no respete plenamente las técnicas y los métodos administrativos para gestionar proyectos informáticos de gran magnitud, como forma de reducir los costes;

3. por último, no puede excluirse totalmente el riesgo de que el contratista se vea enfrentado a dificultades financieras por motivos ajenos a este proyecto.

Estos riesgos se mitigan mediante la adjudicación de contratos sobre la base de criterios de calidad sólidos, la comprobación de las referencias de los contratistas y el mantenimiento de una sólida relación con ellos. Finalmente, como último recurso, pueden incluirse, y aplicarse cuando sea necesario, cláusulas de penalización y de rescisión rigurosas.

2.2.2. Información relativa al sistema de control interno establecido

eu-LISA está considerada como un centro de excelencia en el campo del desarrollo y la gestión de sistemas informáticos de gran magnitud. Ejecutará las actividades relacionadas con el desarrollo y el funcionamiento de los distintos componentes de interoperabilidad, incluido el mantenimiento de la interfaz uniforme nacional en los Estados miembros.

Durante la fase de desarrollo, todas las actividades serán ejecutadas por eu-LISA, lo que incluye el desarrollo de todos los elementos del proyecto. Los costes relacionados con la integración de los sistemas en los Estados miembros durante la fase de desarrollo serán gestionados por la Comisión mediante gestión compartida o subvenciones.

Durante la fase de funcionamiento, eu-LISA será responsable de la gestión técnica y financiera de los componentes utilizados a nivel central, en particular de la adjudicación y la gestión de los contratos. La Comisión gestionará la financiación a los Estados miembros de los gastos de las unidades nacionales a través del FSI-Fronteras (programas nacionales).

A fin de evitar retrasos a nivel nacional, debe preverse una gobernanza eficiente entre todos los interesados antes del inicio de la fase de desarrollo. La Comisión presupone que se definirá una arquitectura interoperable al inicio del proyecto para aplicarla a los proyectos SES y SEIAV, dado que estos proyectos ofrecen y utilizan el SCB compartido, el registro común de datos de identidad y el portal europeo de búsqueda. Un miembro del equipo de gestión del proyecto de interoperabilidad debe formar parte de la estructura de gobierno de los proyectos SES y SEIAV.

2.2.3. Estimación de los costes y beneficios de los controles y evaluación del nivel de riesgo de error esperado

No se ha proporcionado ninguna estimación, puesto que el control y la reducción de los riesgos es una tarea propia de la estructura de gobierno del proyecto.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas.

Las medidas previstas para luchar contra el fraude son las establecidas en el artículo 35 del Reglamento (UE) n.º 1077/2011, que dispone lo siguiente:

1. Con el fin de combatir el fraude, la corrupción y otras actividades ilegales, se aplicará el Reglamento (CE) n.º 1073/1999.

2. Las Agencias se adherirán al Acuerdo Interinstitucional relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF) y promulgarán sin demora las disposiciones adecuadas aplicables a todos sus empleados.

3. Las decisiones de financiación y los acuerdos e instrumentos de ejecución resultantes dispondrán de manera explícita que el Tribunal de Cuentas y la OLAF podrán efectuar, en caso necesario, controles *in situ* de los beneficiarios de la financiación de las Agencias, así como de los agentes responsables de su asignación.

De conformidad con esta disposición, el 28 de junio de 2012 se adoptó la Decisión del Consejo de Administración de la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia relativa a las condiciones y modalidades de las investigaciones internas en

materia de lucha contra el fraude, la corrupción y cualquier actividad ilegal que vaya en detrimento de los intereses de la Unión.

Será de aplicación la estrategia de prevención y detección del fraude de la DG HOME.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

EL IMPACTO ESTIMADO SOBRE EL GASTO Y LA DOTACIÓN DE PERSONAL PARA LOS AÑOS 2021 Y SIGUIENTES SE AÑADE A LA PRESENTE FICHA FINANCIERA LEGISLATIVA CON FINES ILUSTRATIVOS, SIN PERJUICIO DEL PRÓXIMO MARCO FINANCIERO PLURIANUAL

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectadas

- Líneas presupuestarias existentes

En el orden de las rúbricas y las líneas presupuestarias del marco financiero plurianual.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número [Rúbrica.....]	CD/CND[84]	de países de la AELC[85]	de países candidatos[86]	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
3	18.02.01.03 — «Fronteras inteligentes»	CD	NO	NO	SÍ	NO
3	18.02.03 — Agencia Europea de la Guardia de Fronteras y Costas	CD	NO	NO	SÍ	NO

84 CD = créditos disociados / CND = créditos no disociados.
85 AELC: Asociación Europea de Libre Comercio.
86 Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

	(Frontex)					
3	18.02.04 — EUROPOL	CD	NO	NO	NO	NO
3	18.02.05 — CEPOL	CND	NO	NO	NO	NO
3	18.02.07 — Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA)	CD	NO	NO	SÍ	NO

3.2. Incidencia estimada en los gastos

[Esta sección debe rellenarse mediante la **hoja de cálculo sobre datos presupuestarios de carácter administrativo** (segundo documento adjunto a la presente ficha financiera) y cargarse en DECIDE a efectos de consulta entre servicios.]

3.2.1. Resumen de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	3	Seguridad y ciudadanía

DG HOME			Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**Año 2028**	**TOTAL**
• Créditos de operaciones													
18.02.01.03 — «Fronteras inteligentes»	Compromisos	(1)	0	0	43,150	48,150	45,000	**0**	**0**	**0**	**0**	**0**	**136,300**
	Pagos	(2)	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Créditos de carácter administrativo financiados mediante la dotación de programas específicos[87]													
Número de línea presupuestaria		(3)											
Total de los créditos para la DG HOME	Compromisos	=1 + 1.a + 3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Pagos	=2 + 2.a + 3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Los gastos cubrirán:

– los costes de adaptación de la INU (interfaz uniforme nacional), cuyo desarrollo se financia de conformidad con la propuesta del SES, un importe presupuestado para los cambios en los sistemas de los Estados miembros a fin de tener en cuenta las modificaciones de los sistemas centrales y un importe presupuestado para la formación de los usuarios finales.

18.0203 — GEFC			Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
Título 1: Gastos de personal	Compromisos	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Pagos	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Título 2: Infraestructura y gastos de funcionamiento	Compromisos	(1 a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Pagos	(2 a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Título 3: Gastos operativos	Compromisos	(3 a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Pagos	(3 b)	0	0	0	0,183	2,200	0	0	0	0	2,383
Total de los créditos para EUROPOL	(total de los compromisos = total de los pagos)	= 1 + 1.a + 3.a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

[87] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

– El presupuesto de la GEFC cubre los gastos de un equipo dedicado a la validación de los vínculos generados por el DIM (detector de identidades múltiples) sobre el patrimonio de datos (alrededor de 14 millones de registros). El volumen de vínculos que deberán validarse manualmente se estima en unos 550 000. El equipo creado a tal fin se suma al equipo de la GEFC creado para el SEIAV porque están funcionalmente próximos y se evita así el coste de creación de un nuevo equipo.
Estos trabajos se llevarán a cabo en 2023. Los agentes contractuales se contratarán, por tanto, con 3 meses de antelación y su contrato finalizará 2 meses después del término de la actividad de migración. En principio, el resto de los recursos necesarios no se contratarán como agentes contractuales, sino como asesores. Esto explica los costes previstos en el Título 3 para el año 2023. En principio serán contratados con un mes de antelación. Más adelante se facilitarán otros detalles sobre la plantilla.

– El Título 1 incluye, por lo tanto, el coste de 20 empleados internos, y las disposiciones relativas al refuerzo de la gestión y al personal de apoyo.

– El Título 2 incluye los costes adicionales de alojamiento de los 10 empleados adicionales del contratista.

– El Título 3 incluye la tasa de los 10 empleados adicionales del contratista. No se incluyen otros tipos de costes.

18.0204 — Europol			Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
Título 1: Gastos de personal	Compromisos	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Pagos	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Título 2: Infraestructura y gastos de funcionamiento	Compromisos	(1 a)	0	0	0	0	0	0	0	0	0	0
	Pagos	(2 a)	0	0	0	0	0	0	0	0	0	0
Título 3: Gastos operativos	Compromisos	(3 a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Pagos	(3 b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
Total de los créditos para EUROPOL	(total de los compromisos = total de los pagos)	= 1 + 1.a + 3.a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Los gastos de Europol incluirán la mejora de las capacidades de los sistemas de tecnologías de la información de Europol para tratar el volumen de mensajes previsto y la mejora de su rendimiento (tiempo de respuesta).

Título 1: los gastos de personal cubren los costes relativos a la contratación de más informáticos para reforzar los sistemas de información de Europol por los motivos mencionados anteriormente. A continuación se ofrecen más detalles sobre el reparto de puestos entre agentes temporales y contractuales y sus perfiles.

El Título 3 incluye los costes de los equipos y programas necesarios para reforzar los sistemas de información de Europol. En la actualidad, los sistemas de tecnologías de la información de Europol prestan servicio a una comunidad limitada formada por Europol, los funcionarios de enlace de Europol y los investigadores de los Estados miembros que utilizan estos sistemas con fines de análisis y de investigación. Con la implementación de QUEST (la interfaz del sistema que permitirá que el PEB consulte los datos de Europol) a un nivel básico de protección (actualmente los sistemas de información de Europol están acreditados hasta el nivel RESTRINGIDO UE y CONFIDENCIAL UE), los sistemas de información de Europol serán accesibles por una comunidad policial autorizada mucho más amplia. Además de estas mejoras, el PEB también será utilizado por el SEIAV para consultar automáticamente los datos de Europol en la tramitación de las autorizaciones de viaje. Esto incrementará el volumen de consultas de datos de Europol desde las aproximadamente 107 000 consultas mensuales de la actualidad a más de 100 000 consultas diarias, y exigirá además una disponibilidad de los sistemas de información de Europol durante 24 horas al día, 7 días a la semana, y tiempos de respuesta muy cortos para cumplir los requisitos impuestos por el Reglamento SEIAV. La mayoría de los gastos se efectuarán en el periodo anterior a la entrada en funcionamiento de los componentes de interoperabilidad, pero algunos compromisos en curso son necesarios para garantizar un alto nivel de disponibilidad permanente de los sistemas de información de Europol. Además, Europol necesita, como usuario, algunos trabajos de desarrollo de los componentes de interoperabilidad.

18.0205 — CEPOL			Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
Título 1: Gastos de personal	Compromisos	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Pagos	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Título 2: Infraestructura y gastos de funcionamiento	Compromisos	(1 a)	0	0	0	0	0	0	0	0	0	0
	Pagos	(2 a)	0	0	0	0	0	0	0	0	0	0
Título 3: Gastos operativos	Compromisos	(3 a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Pagos	(3 b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840

Total de los créditos para CEPOL	(total de los compromisos = total de los pagos)	= 1 + 1.a + 3.a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

La formación coordinada centralmente a escala de la UE mejora la impartición coherente de cursos de formación a escala nacional y, en consecuencia, garantiza la correcta y lograda ejecución y utilización de los componentes de interoperabilidad. La CEPOL, como Agencia de la UE para la Formación Policial, se encuentra en una buena posición para ofrecer formación a nivel central de la UE. Estos gastos cubren la preparación de la «formación de formadores de los Estados miembros» requerida para utilizar los sistemas centrales una vez sean interoperables. Los costes incluyen un pequeño aumento de personal de la CEPOL para coordinar, administrar, organizar y actualizar los cursos, así como la prestación de una serie de sesiones de formación anuales y la preparación del curso en línea. Los detalles de estos costes se explican a continuación. El esfuerzo de formación se concentrará en los periodos inmediatamente anteriores a la puesta en marcha. Sigue siendo necesario realizar un esfuerzo continuo después de la entrada en funcionamiento, dado que los componentes interoperables son permanentes pero los formadores no serán siempre los mismos, según muestra la experiencia en la formación existente sobre el Sistema de Información de Schengen.

18.0207 — eu-LISA			Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
Título 1: Gastos de personal	Compromisos	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Pagos	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Título 2: Infraestructura y gastos de funcionamiento	Compromisos	(1 a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Pagos	(2 a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Título 3: Gastos operativos	Compromisos	(3 a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Pagos	(3 b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309

Total de los créditos para eu-LISA	(total de los compromisos = total de los pagos)	= 1 + 1.a + 3.a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Estos gastos cubrirán:

- El desarrollo y mantenimiento de los cuatro componentes de interoperabilidad [portal europeo de búsqueda (PEB), servicio de correspondencia biométrica compartido (SCB compartido), registro común de datos de identidad (RCDI) y detector de identidades múltiples (DIM)] incluidos en la propuesta legislativa, más el repositorio común para la presentación de informes y estadísticas (RCIE). eu-LISA actuará como representante del propietario del proyecto y utilizará su propio personal para la redacción de las especificaciones, la selección de contratistas, la dirección de los trabajos, la presentación de los resultados de una serie de ensayos y la aceptación del trabajo realizado.
- Los costes de la migración de datos de los sistemas existentes a los nuevos componentes. Sin embargo, eu-LISA no tiene una función directa en la carga de datos inicial del DIM (validación de vínculos) porque se trata de una acción sobre el contenido de los datos en sí. La migración de datos biométricos de los sistemas existentes se refiere al formato y el etiquetado de los datos, pero no a su contenido.
- Los gastos de actualización y explotación del ECRIS-TCN como un sistema de alta disponibilidad desde 2022. El ECRIS-TCN es el sistema central que contiene los registros de antecedentes penales de los nacionales de terceros países. Se prevé que el sistema esté disponible para 2020. Se espera que los componentes de interoperabilidad también den acceso a este sistema, que, por lo tanto, se convertiría también en un sistema de alta disponibilidad. Los gastos de funcionamiento incluyen el coste adicional para conseguir un alto nivel de disponibilidad. Habrá un importante gasto en desarrollo en 2021, seguido de un coste de mantenimiento y explotación en curso. Estos costes no se incluyen en la ficha financiera legislativa de la revisión del Reglamento constitutivo de eu-LISA[88], que solo incluye los presupuestos desde 2018 hasta 2020 y, por consiguiente, no se solapa con la presente solicitud presupuestaria.
- La pauta de los gastos es el resultado de la secuenciación del proyecto. Dado que los diversos componentes no son independientes entre sí, el periodo de desarrollo se extiende de 2019 a 2023. Sin embargo, a partir de 2020 se inicia el mantenimiento y el funcionamiento de los primeros componentes disponibles. Esto explica por qué los gastos empiezan lentamente, aumentan y luego disminuyen a un valor constante.

[88] COM 2017/0145 (COD) Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, y por el que se modifican el Reglamento (CE) n.º 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) n.º 1077/2011

– Los gastos en virtud del Título 1 (gastos de personal) siguen la secuenciación del proyecto: se necesita más personal para que el contratista entregue el proyecto (sus gastos figuran en el Título 3). Una vez entregado el proyecto, parte del equipo de desarrollo se asignará al trabajo de desarrollo y mantenimiento. Al mismo tiempo, aumenta el personal que utiliza los nuevos sistemas.

– Los gastos en virtud del Título 2 (infraestructura y gastos de funcionamiento) cubren el espacio de oficinas suplementario para alojar temporalmente a los equipos del contratista encargados de las labores de desarrollo, mantenimiento y funcionamiento. La pauta temporal del gasto sigue, por lo tanto, también la evolución de los niveles de personal. Los gastos de alojamiento de equipamientos adicionales ya se han incluido en el presupuesto de eu-LISA. Tampoco existen costes adicionales de alojamiento de personal de eu-LISA, pues ya se incluyen en los costes fijos de personal.

– Los gastos en virtud del Título 3 (gastos operativos) incluyen el coste para el contratista del desarrollo y el mantenimiento del sistema, así como la adquisición de equipos y programas informáticos específicos.
  Los costes del contratista se inician con los estudios para especificar los componentes y el desarrollo a partir de un componente (el RCIE). Durante el periodo 2020-2022, los gastos aumentarán a medida que se desarrolle un mayor número de componentes en paralelo. Los costes no disminuirán tras el pico porque las tareas de migración de datos son particularmente gravosas en este proyecto. Los costes del contratista disminuirán después, a medida que los componentes se entreguen y entren en funcionamiento, lo que exige una estructura estable de recursos.
  Al mismo tiempo que los gastos del Título 3, el gasto aumentará considerablemente en 2020 en comparación con el año anterior, debido a la inversión inicial en equipos y programas informáticos necesarios durante la fase de desarrollo. Los gastos del Título 3 (gastos operativos) tendrán un fuerte incremento en 2021 y 2022, porque se incurre en los costes de inversión en equipos y programas informáticos de los entornos informáticos operativos (producción y preproducción, tanto para la unidad central como para la unidad central de apoyo) el año anterior a la entrada en funcionamiento de los componentes de interoperabilidad (RCDI y DIM) con un nivel de exigencia alto en equipos y programas informáticos. Una vez en funcionamiento, los costes de equipos y programas informáticos son esencialmente los costes de mantenimiento.

– Se proporcionan detalles más adelante.

Rúbrica del marco financiero plurianual	**5**	«Gastos administrativos»

En millones EUR (al tercer decimal)

		Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
DG HOME											
• Recursos humanos Número de línea presupuestaria 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Otros costes administrativos (reuniones, etc.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
TOTAL PARA LA DG HOME	Créditos	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Total de los créditos para la RÚBRICA 5 del marco financiero plurianual	(total de los compromisos = total de los pagos)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

En millones EUR (al tercer decimal)

	Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	Año **2028**	**TOTAL**

Total de los créditos para las RÚBRICAS 1 a 5 del marco financiero plurianual	Compromisos	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Pagos	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Incidencia estimada en los créditos de operaciones

3.2.2.1. Incidencia estimada sobre los créditos de la Agencia GEFC

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

– X La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
Agencia GEFC	Tipo[89]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 1[90] Validación de vínculos																						
Personal contratado en calidad de expertos para validar vínculos	Costes del contratista		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383

[89] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[90] Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...»

Subtotal del objetivo específico n.º 1	**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2,383**

Estos gastos cubrirán:

— La contratación de suficiente personal suplementario (estimado en unos 10 expertos) al personal interno (estimado en unas 20 personas) que serán alojados por la GEFC con el fin de validar vínculos. Solo hay un mes de contratación antes de la fecha de inicio prevista para alcanzar la dotación de personal exigida.

— No existe ningún otro coste estimado del contratista. Los programas informáticos que se requieren forman parte de los costes de las licencias del SCB compartido. No existe una capacidad específica de tratamiento del equipo informático. Del alojamiento del personal del contratista se ocupa, en principio, la GEFC. Resulta, por tanto, que de conformidad con el Título 2 se añadirá el coste anual de 12 metros cuadrados de media por persona.

3.2.2.2. Incidencia estimada en los créditos de Europol

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

– X La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
Europol	Tipo[91]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 1[92] Desarrollo y mantenimiento de sistemas (Europol)																						
Entorno TI	Infraestructura					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
Entorno TI	Equipo informático					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144

[91] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[92] Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...»

Entorno TI	Programas informáticos				0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948
Trabajos de desarrollo	Contratista				0,360		0,360														0,720
Subtotal			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Estos gastos cubrirán la necesidad de reforzar los sistemas de información y la infraestructura de Europol para tener en cuenta el incremento de las consultas. Incluyen:

— La mejora de la seguridad y la infraestructura de red, el equipo informático (servidores, almacenamiento) y los programas informáticos (licencias). Como estas mejoras deben ultimarse antes de que el portal europeo de búsqueda y el SEIAV entren en funcionamiento en 2021, los costes se han distribuido a partes iguales entre 2020 y 2021. A partir de 2022, se ha tomado una tasa anual de mantenimiento del 20 % como base para calcular los costes de mantenimiento. Además, se ha tenido en cuenta el ciclo normal de cinco años para sustituir las infraestructuras y el material informático anticuados.

— Los costes del contratista para los trabajos de desarrollo de QUEST en el nivel básico de protección.

3.2.2.3. Incidencia estimada en los créditos de la CEPOL

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

– X La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
CEPOL	Tipo[93]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 1[94] Desarrollo e impartición de cursos de formación																						
Número de cursos residenciales	0,34 por curso		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Formación en línea	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052

[93] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[94] Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...»

Subtotal		**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

A fin de garantizar la aplicación y la utilización uniformes de las soluciones de interoperabilidad, la formación será organizada a nivel central de la UE por la CEPOL y a nivel de los Estados miembros. Los gastos de formación a nivel de la UE incluyen:

- Desarrollo de un plan de estudios común que deberán seguir los Estados miembros a la hora de impartir la formación a escala nacional;

-Actividades residenciales para formar a los formadores. En el plazo de dos años inmediatamente después de que las soluciones de interoperabilidad sean una realidad, se espera que la formación se dispense a mayor escala y posteriormente se mantenga en dos cursos de formación anuales en régimen residencial.

- Un curso en línea para complementar las actividades residenciales a nivel de la UE y en los Estados miembros.

3.2.2.4. Incidencia estimada en los créditos de eu-LISA

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

– X La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
eu-LISA	Tipo[95]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 1[96] Desarrollo de los componentes de interoperabilidad																						
Sistemas	Contratista			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Programas informáticos	Programas informáticos			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Equipo informático	Material informático			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133

[95] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[96] Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...»

Formación en informática	Formación y otros		0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340
Subtotal del objetivo específico n.º 1			**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Este objetivo incluye únicamente los costes de desarrollo de los cuatro componentes de interoperabilidad y el RCIE.

– Los costes del SCB compartido se han calculado partiendo del supuesto de que el SES, que se está finalizando, constituirá el sistema central de desarrollo. Por lo tanto, está previsto reutilizar las licencias de los programas informáticos biométricos (36 millones EUR) incluidas en el SES.

– En este presupuesto, el SCB compartido es tratado como una extensión del SCB del SES. Por lo tanto, la actual ficha financiera incluye el coste marginal de las licencias de los programas informáticos (6,8 millones EUR) para añadir los aproximadamente 20 millones de conjuntos de datos biométricos contenidos en el SAID del SIS (SAID es el sistema automático de identificación dactilar = el «SCB» del SIS), el SAID de Eurodac y el futuro ECRIS-TCN (Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países) al SCB desarrollado para el SES. Los costes de integración de los distintos sistemas (SIS, Eurodac y ECRIS-TCN) en el SCB compartido están incluidos en la presente ficha financiera.

– Como parte de los trabajos a lo largo de 2019 y 2020, eu-LISA deberá desarrollar una solución técnica precisa que no puede definirse en el momento de presentar la propuesta legislativa y evaluar el coste de aplicación de la solución técnica preferida. Para ello, podría ser necesario un cambio en la estimación de los costes aquí indicada.

– Todos los componentes se entregarán a finales de 2023, lo que explica que los costes del contratista se reduzcan prácticamente a cero en ese momento. Solo se mantiene un importe residual para la actualización periódica del RCIE.

– Durante el periodo comprendido entre 2019 y 2021, los gastos en programas informáticos aumentarán sustancialmente, al adquirirse las licencias de los programas informáticos para los distintos entornos necesarios para la producción, la preproducción y el ensayo, tanto en el sitio central como en el sitio de respaldo. Además, el precio de algunos componentes específicos e indispensables de los programas informáticos se ha calculado atendiendo al número de «objetos referenciados» (es decir, el volumen de datos). Como, en última instancia, la base de datos contendrá unos 220 millones de identidades, el precio de los programas informáticos es proporcional a este valor.

Indíquense los objetivos y los resultados **eu-LISA**			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
	Tipo[97]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 2 Mantenimiento y funcionamiento de los componentes de interoperabilidad																						
Sistemas operativos	Contratista			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Programas informáticos	Programas informáticos			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Equipo informático	Material informático			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
Formación en informática	Formación			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Subtotal del objetivo específico n.º 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

[97] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

– El mantenimiento comienza inmediatamente después de la entrega de algún componente. Por tanto, el presupuesto para el contratista de mantenimiento se incluye a partir del momento en que se entrega el PEB (en 2021). El presupuesto de mantenimiento aumentará a medida que se entreguen componentes hasta alcanzar un valor más o menos constante, que representa un porcentaje (entre el 15 y el 22 %) de la inversión inicial.

– El mantenimiento de equipos y programas informáticos comienza a partir del año de entrada en funcionamiento: la evolución de los costes es similar a la de costes del contratista.

Indíquense los objetivos y los resultados eu-LISA			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
	Tipo[98]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 3[99] Migración de datos																						
Datos SCB existentes migrados	Al SCB compartido			0		0		0		7,000		3,000		0		0		0		0		10,000
Datos EDAC existentes habilitados para la	Nuevo diseño y desarrollo de EDAC			0		0		7,500		7,500				0		0		0		0		15,000

[98] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[99] Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...»

Subtotal del objetivo específico n.º 3		**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– En el caso del proyecto SCB compartido, los datos deben migrarse de los demás motores biométricos al SCB compartido, puesto que este sistema común es más eficaz desde el punto de vista operativo y también ofrece una ventaja financiera en comparación con el mantenimiento de varios sistemas SCB más pequeños.

– La actual lógica funcional de Eurodac no está claramente separada del mecanismo de correspondencia de datos biométricos, como es el caso del SCB que funciona con el VIS. El funcionamiento interno de Eurodac y el mecanismo con el que los servicios funcionales recurren a los servicios de correspondencia biométrica subyacentes es una caja negra para el observador externo y se basa en una tecnología propia. No será posible migrar simplemente los datos a un SCB compartido y mantener el nivel funcional actual. Por tanto, la migración de los datos irá acompañada de costes considerables para cambiar los mecanismos de intercambio con la aplicación central de Eurodac.

Indíquense los objetivos y los resultados **eu-LISA**			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
	Tipo[100]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 4[101] Red																						
Conexiones de red	Configuración de la red			0		0		0		0,505										0		0,505

100 Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

101 Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...»

Tráfico en la red	Funcionamiento de la red		0		0						0,246		0,246		0,246		0,246		0,246		1,230
Subtotal del objetivo específico n.º 4			**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– Los componentes de interoperabilidad solo tendrán un efecto marginal en el tráfico en la red. En términos de datos, únicamente se crean vínculos entre los datos existentes, cuyo volumen es escaso. El coste incluido aquí es solo el aumento presupuestario marginal necesario, además de los presupuestos del SES y el SEIAV, para la configuración de la red y el tráfico.

Indíquense los objetivos y los resultados **eu-LISA**			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
	Tipo[102]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 5[103] Actualización de las INU																						
Actualización de las INU	Contratista			0		0		0		0,505		0,505								0		1,010
Subtotal del objetivo específico				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

102 Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

103 Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...»

n.º 5																				

– La propuesta del SES introdujo el concepto de interfaz nacional uniforme (INU), de cuyo desarrollo y mantenimiento se ocupará eu-LISA. El cuadro anterior incluye el presupuesto para la actualización de la INU integrando un tipo de intercambio de información suplementario. No hay ningún coste adicional al funcionamiento de la INU, que ya se había presupuestado con cargo a la propuesta del SES.

Indíquense los objetivos y los resultados **eu-LISA**			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
	Tipo[104]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 6: Reuniones y formación																						
Reuniones mensuales de evolución (desarrollo)	0,021 por reunión x 10 al año		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Reuniones trimestrales (funcionamiento)	0,021 x 4 al año		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756

[104] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

Grupos consultivos	0,021 x 4 por al año	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Formación EE.MM.	0,025 por formación	2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Subtotal del objetivo específico n.º 6		20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

– El subtotal 6 incluye los gastos de organización de reuniones por parte de la autoridad de gestión (en este caso, eu-LISA) para la gobernanza del proyecto. Se trata de los gastos en reuniones adicionales para la entrega de los componentes de interoperabilidad.

– El subtotal 6 incluye los costes de las reuniones de eu-LISA con el personal de los Estados miembros encargado del desarrollo, el mantenimiento y el funcionamiento de los componentes de interoperabilidad, así como la organización y la impartición de formación al personal informático de los Estados miembros.

– Durante la fase de desarrollo, el presupuesto incluye 10 reuniones de proyecto al año. Una vez preparada la entrada en funcionamiento (a partir de 2019), se organizarán cuatro reuniones anuales. A un nivel superior, se creará desde el inicio un grupo consultivo para aplicar las decisiones de ejecución de la Comisión. Se prevén cuatro reuniones anuales, como en el caso de los grupos consultivos existentes. Además, eu-LISA preparará e impartirá formación al personal informático de los Estados miembros sobre los aspectos técnicos de los componentes de interoperabilidad.

Indíquense los objetivos y los resultados **eu-LISA**			Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**

	Tipo[105]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 7[106] Alta disponibilidad del ECRIS-TCN																								
Sistema altamente disponible	Configuración del sistema			0		0		8,067														0		8,067
Funcionamiento altamente disponible	Mantenimiento y funcionamiento del sistema			0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Subtotal del objetivo específico n.º 4				**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– El objetivo n.º 7 es que el ECRIS-TCN pase de ser un sistema de disponibilidad «normal» a un sistema de alta disponibilidad. Esta mejora del ECRIS-TCN tendrá lugar en 2021, pues requiere esencialmente la adquisición de equipos informáticos adicionales. Dado que la finalización del ECRIS-TCN está prevista en 2020, resulta tentador hacer de él un sistema de alta disponibilidad desde el principio, integrado con los componentes de interoperabilidad. Sin embargo, como muchos de estos proyectos son dependientes entre sí, es prudente no partir de este supuesto y presupuestar medidas separadas. Este presupuesto es un presupuesto adicional a los costes de desarrollo, mantenimiento o funcionamiento del ECRIS-TCN en 2019 y 2020.

[105] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[106] Tal como se describe en el punto 1.4.2, «Objetivo(s) específico (s)...».

3.2.2.5. Incidencia estimada en los créditos de la DG HOME

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

– ☒ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados **DG HOME**			Año **2019**		Año **2020**		Año **2021**		Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
	Tipo[107]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO n.º 1: Integración de los sistemas nacionales (Estado miembro)																						
INU lista para su uso	Adaptación de la INU - desarrollo						30	3,150	30	3,150											30	6,300
Sistemas de los EE.MM. adaptados a la interoperabilidad	Costes de integración						30	40,000	30	40,000	30	40,000									30	120,000

[107] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

Formación de los usuarios finales	10 000 sesiones para usuarios finales en total @ 1 000 EUR por sesión							5 000	5,000	5 000	5,000									10 000	10,000
Subtotal del objetivo específico n.º 1							**43,150**		**48,150**		**45,000**										**136,300**

– El objetivo específico n.º 1 se refiere a los fondos puestos a disposición de los Estados miembros para beneficiarse de los sistemas centrales interoperables. La INU se adaptará cuando se ponga en marcha el PEB y cuando entre en funcionamiento el DIM. Cada Estado miembro tiene que hacer unos cambios relativamente moderados (estimados en 150 días/persona) para adaptarse a estos nuevos intercambios de mensajes mejorados con los sistemas centrales. Más importante es la modificación del contenido de los datos que introducirá la interoperabilidad y que está cubierta por los «costes de integración». Estos fondos financian los cambios del tipo de mensajes enviados al sistema central y para la tramitación de la respuesta recibida. Para estimar los costes de dichos cambios, se asigna a cada Estado miembro un presupuesto de 4 millones EUR. Este importe es el mismo que para el SES, ya que el trabajo necesario para adaptar la integración de los sistemas nacionales con la INU es comparable.

– Los usuarios finales deben recibir formación sobre los sistemas. Esta formación para un número muy grande de usuarios finales se financiará sobre la base de 1 000 EUR por sesión de 10 a 20 usuarios finales para las cerca de 10 000 sesiones que organizarán todos los Estados miembros en sus propias dependencias.

3.2.3. Incidencia estimada en los recursos humanos

3.2.3.1. Resumen de la Agencia GEFC

☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

X La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
Funcionarios (categoría AD)										
Funcionarios (categoría AST)	0									
Agentes contractuales	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Agentes temporales	0	0	0	0	0	0	0	0	0	0
Expertos nacionales en comisión de servicios										
TOTAL	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

El trabajo que se prevé que lleve a cabo este personal adicional de la GEFC es limitado en el tiempo (2023) y empezará, más concretamente, 24 meses después de la fecha en que esté disponible el motor biométrico del SES. Sin embargo, el personal deberá ser contratado previamente (se calcula una media de tres meses), lo que explica el coste en 2022. Al trabajo realizado le seguirán tareas de conclusión/finalización durante dos meses, lo que explica la dotación de personal en 2024.

La dotación de personal consiste en 20 personas necesarias para el trabajo que debe hacerse (más 10 personas aportadas por un contratista, que se reflejan en el título 3). También se supone que las tareas se llevarán a cabo durante horas de trabajo extraordinarias y no se limitarán a las horas normales. Se supone que se proporcionará personal de gestión y de apoyo en función de los recursos de la Agencia.

La dotación de personal se basa en el supuesto de que tendrán que evaluarse unas 550 000 impresiones dactilares, a un promedio de 5 a 10 minutos cada una (17 000 impresiones dactilares al año)[108].

Personal	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Personal para el tratamiento manual de vínculos y decisiones	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Título 1 - CA	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Título 1 - TA	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Total Título 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

3.2.3.2. Resumen de Europol

☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

X La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
Funcionarios (categoría AD)										
Funcionarios (categoría AST)	0									
Agentes contractuales	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Agentes temporales	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Expertos nacionales en comisión de servicios										
TOTAL	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Estos costes se calculan sobre la base de la dotación de personal siguiente:

Número de ETC	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**total**

[108] El personal en 2020 y años posteriores es indicativo y se deberá examinar si es adicional o no a la previsión de personal de la GEFC que figura en el documento COM(2015) 671.

para las TIC										
Agentes contractuales	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Agentes temporales	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Total personal (ETC)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Está previsto dotar a Europol con personal informático adicional para reforzar sus sistemas de información con el fin de dar respuesta al aumento del número de consultas del PEB y el SEIAV y, posteriormente, mantener los sistemas 24 horas al día, 7 días a la semana.

– Para la fase de ejecución del PEB (en 2020 y 2021) existe una necesidad adicional de expertos técnicos (arquitectos, ingenieros, desarrolladores, probadores). Será necesario un número reducido de expertos técnicos a partir de 2022, para la implementación del resto de los componentes de interoperabilidad y el mantenimiento de los sistemas.

– A partir del segundo semestre de 2021, deberá aplicarse un sistema de control informático 24horas al día, 7 días a la semana, para garantizar los niveles de servicio del PEB y el SEIAV. De ello se ocuparán 2 agentes contractuales, que trabajarán en 4 turnos 24horas al día, 7 días a la semana.

– En la medida de lo posible, los perfiles se han dividido entre agentes temporales y agentes contractuales. Nótese sin embargo que, debido a los elevados requisitos de seguridad, en diversos puestos solo es posible recurrir a agentes temporales. La solicitud de agentes temporales tendrá en cuenta los resultados de la conciliación del procedimiento presupuestario de 2018.

3.2.3.3. Resumen de la CEPOL

☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

☒ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año2019	Año2020	Año2021	Año2022	Año2023	Año2024	Año2025	Año2026	Año2027	**TOTAL**
Funcionarios (categoría AD)										
Funcionarios (categoría AST)										
Agentes contractuales			0,070	0,070						**0,140**

Agentes temporales		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Expertos nacionales en comisión de servicios										

TOTAL		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Será necesario más personal porque la formación de los formadores de los Estados miembros debe concebirse específicamente con vistas a utilizar los componentes de interoperabilidad en circunstancias operativas.

— El desarrollo de planes de estudios y módulos de formación debe iniciarse al menos 8 meses antes de que el sistema entre en funcionamiento. En los primeros dos años posteriores a la puesta en marcha, la formación es más intensa. Sin embargo, es necesario que se mantenga durante un periodo más largo para garantizar una ejecución coherente, según muestra la experiencia adquirida con el Sistema de Información de Schengen.

— El personal adicional es necesario para preparar, coordinar y ejecutar el plan de estudios, los cursos residenciales y el curso en línea. Estos cursos solo pueden impartirse como complemento del catálogo de formación existente de la CEPOL y, por lo tanto, es necesario personal adicional.

— Está previsto contar, a lo largo de todo el periodo de desarrollo y mantenimiento, con un agente temporal como administrador del curso, que estará asistido por un agente contractual en el periodo más intenso de la organización de formación.

3.2.3.4. Resumen de eu-LISA

☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

☒ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
Funcionarios (categoría AD)										
Funcionarios (categoría AST)										
Agentes contractuales	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570

Agentes temporales	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Expertos nacionales en comisión de servicios										

TOTAL	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

- Las necesidades de personal tienen en cuenta que los cuatro componentes y el RCIE constituyen una cartera de proyectos con dependencias (es decir, un programa). Para gestionar la dependencia entre proyectos, se creó un equipo de gestión del programa compuesto por los gestores de programas y proyectos y los perfiles (a menudo denominados arquitectos) que deben definir los elementos comunes entre ellos. La realización de los programas/proyectos requiere también perfiles de apoyo a los programas y proyectos.
- Las necesidades de personal por proyecto se han estimado por analogía con proyectos anteriores (Sistema de Información de Visados), distinguiendo entre la fase de conclusión del proyecto y la fase de funcionamiento.
- Los perfiles necesarios durante la fase de funcionamiento se contratan como agentes temporales. Los perfiles necesarios durante la ejecución de los programas/proyectos se contratan como agentes contractuales. Para garantizar la continuidad de las tareas y de los conocimientos de la Agencia, el número de puestos de trabajo se reparte casi al 50 % entre agentes temporales y agentes contractuales.
- Se parte del supuesto de que no se necesitará personal adicional para llevar a cabo el proyecto ECRIS-TCN de alta disponibilidad y que la dotación de personal del proyecto de eu-LISA consistirá en la reutilización del personal de los proyectos que se finalicen en ese periodo de tiempo.

Estas estimaciones se basan en los niveles de dotación de personal siguientes:

Agentes contractuales:

3.2.1. Resultados EU-LISA (igual a T1) en número de personas	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total (fórmula)
Agentes contractuales										-
Gestión de programas/proyectos	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
RCIE GP	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
DIM	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Oficinas de los programas/proyectos	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Garantía de calidad	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Gestión financiera y de contratos	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gestión financiera										*0,0*
Planificación y control presupuestario										*0,0*
Gestión de contratos y compras	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Expertos técnicos	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
RCIE	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
PEB	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
SCB compartido	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
RCDI	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
RCDI	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*

Pruebas	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
RCIE	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
PEB	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
SCB compartido	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
RCDI	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
DIM	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Supervisión del sistema	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Común (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Coordinación general	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Recursos humanos	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RR.HH.	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Subtotal agentes contractuales	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

Agentes temporales:

Agentes temporales										
Gestión del programa/proyecto	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Gestión de programas	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestión de proyectos	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Oficinas de los programas/proyectos	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
PEB	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
SCB compartido	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
RCDI	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
DIM	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Gestión financiera y de contratos	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Gestión financiera	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	7,0
Planificación y control presupuestario	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	9,0
Gestión de contratos y compras	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	18,0
Expertos técnicos	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
RCIE	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
PEB	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
SCB compartido	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
RCDI	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Seguridad	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
DIM	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Arquitectos	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Pruebas	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
RCIE	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
PEB	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
SCB compartido	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
RCDI	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*

DIM	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Supervisión del sistema	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RCIE	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
PEB	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
SCB compartido	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
RCDI	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
DIM	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Formación	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Formación	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Recursos humanos	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
RR.HH.	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Otros	*0,0*	*0,0*	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	5,0
Especialista en protección de datos	*0,0*	*0,0*	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*5,0*
Subtotal agentes temporales	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Total	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Incidencia estimada en los créditos de carácter administrativo

3.2.4.1. Resumen de la DG HOME

☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

X La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
RÚBRICA 5 del marco financiero plurianual										

Recursos humanos DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Otros gastos administrativos	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Subtotal para la RÚBRICA 5 del marco financiero plurianual	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Al margen de la RÚBRICA 5del marco financiero plurianual[109]	(no se utiliza)									
Recursos humanos										
Otros gastos de carácter administrativo										
Subtotal al margen de la RÚBRICA 5del marco financiero plurianual										

TOTAL	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

[109] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

3.2.4.2. Estimación de las necesidades en recursos humanos

☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

X La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

Estimación que debe expresarse en unidades de equivalente a jornada completa

	Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
• Empleos de plantilla (funcionarios y personal temporal)										
18 01 01 01 (Sede y Oficinas de Representación de la Comisión) DG HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (Delegaciones)										
XX 01 05 01 (Investigación indirecta)										
10 01 05 01 (Investigación directa)										
• Personal externo (en unidades de equivalente a jornada completa, EJC)[110]										
XX 01 02 02 (AC, AL, ENCS, INT y JED en las Delegaciones)										
XX 01 04 yy[111] — en la sede										
XX 01 04 yy[111] — en las delegaciones										
XX 01 05 02 (AC, ENCS, INT; investigación indirecta)										
10 01 05 02 (AC, ENCS, INT; investigación directa)										
Otras líneas presupuestarias (especifíquense)										
TOTAL	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 es el ámbito político o título presupuestario en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Supervisión y seguimiento de los proyectos. Tres funcionarios para el seguimiento. El personal asume las funciones de la Comisión en la ejecución del programa: comprobar la conformidad con la propuesta legislativa, abordar las cuestiones de conformidad, preparar los informes al Parlamento Europeo y al Consejo, evaluar los progresos de los Estados miembros. Habida cuenta de que el programa es una actividad adicional en comparación con la carga de trabajo actual, se necesita personal adicional. Este aumento de personal es limitado en términos de duración y solo cubre el periodo de desarrollo.

[110] AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal; JED = joven experto en delegación.

[111] Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

Gestión del UMF

La Comisión se encargará de gestionar la norma UMF de forma cotidiana. Se necesitan dos funcionarios a tal efecto: una persona como experto policial y otra persona con un buen conocimiento de los modelos operativos, así como sobre las TIC.

El formato universal de mensajes (UMF) establece una norma para el intercambio estructurado y transfronterizo de información entre sistemas de información, autoridades y organizaciones en el ámbito de la justicia y los asuntos de interior. El UMF define un vocabulario común y estructuras lógicas para la información comúnmente intercambiada con el objetivo de facilitar la interoperabilidad permitiendo la creación y la lectura del contenido del intercambio de forma congruente y equivalente desde el punto de vista semántico.

A fin de garantizar unas condiciones uniformes para la aplicación del formato universal de mensajes, se propone que se otorguen competencias de ejecución a la Comisión. Dichas competencias se ejercerán de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución de la Comisión.

3.2.5. Compatibilidad con el marco financiero plurianual vigente

– ☐ La propuesta/iniciativa es compatible con el marco financiero plurianual vigente.

– ☒ La propuesta/iniciativa implicará la reprogramación de la rúbrica correspondiente del marco financiero plurianual.

Explíquese la reprogramación requerida, precisando las líneas presupuestarias afectadas y los importes correspondientes.

El Reglamento FSI-Fronteras es el instrumento financiero en el que se ha incluido el presupuesto para la ejecución de la iniciativa de interoperabilidad.

Su artículo 5, letra b), dispone que se destinarán 791 millones EUR a un programa para el desarrollo de sistemas informáticos basados en los sistemas informáticos existentes o nuevos, en apoyo a la gestión de los flujos migratorios en las fronteras exteriores, a reserva de la adopción de los actos legislativos de la Unión pertinentes y con arreglo a las condiciones establecidas en el artículo 15. De esos 791 millones EUR, 480,2 millones EUR están reservados para el desarrollo del SES, 210 millones EUR para el SEIAV y 67,9 millones EUR para la revisión del SIS II. El resto (32,9 millones EUR) se reasignará utilizando los mecanismos FSI-F. **La propuesta actual requiere 32,1 millones EUR para el actual periodo del MFP, que se cubren con el saldo presupuestario.**

La conclusión del recuadro anterior sobre la cantidad necesaria de 32,1 millones EUR es el resultado del cálculo siguiente:

COMPROMISOS

3.2. Impacto estimado sobre el gasto DG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (horizontal)**
18 02 01 03 - Fronteras inteligentes (cubre el apoyo a los EE.MM.)	0,000	0,000	43,150	48,150	45,000	0,000	0,000	0,000	0,000	136,300
Total (1)	**0,000**	**0,000**	**43,150**	**48,150**	**45,000**	**0,000**	**0,000**	**0,000**	**0,000**	**136,300**

18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (fórmula)**
T1: Gastos de personal	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344

T2: Gastos en infraestructuras y operativos	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Gastos de explotación	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Total (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
	22,861							**202,181**		**225,041**

18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (fórmula)**
T1: Gastos de personal	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Gastos en infraestructuras y operativos	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
T3: Gastos de explotación	0,000	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Total (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
	9,072							39,788		48,860

18.02.05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (fórmula)**
T1: Gastos de personal	0,000	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Gastos en infraestructuras y operativos	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
T3: Gastos de explotación	0,000	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Total (4)	**0,000**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
	0,144							**1,906**		**2,050**

18.02.0 -3.2. Frontex - GEFC										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (fórmula)**

T1: Gastos de personal	0,000	0,000	0,0000	0,350	1,400	0,233	0,000	0,000	0,000	1,983
T2: Gastos en infraestructuras y operativos	0,000	0,000	0,0000	0,075	0,300	0,050	0,000	0,000	0,000	0,425
T3: Gastos de explotación	0,000	0,000	0,0000	0,183	2,200	0,000	0,000	0,000	0,000	2,383
Total (5)	**0,000**	**0,000**	**0,0000**	**0,608**	**3,900**	**0,283**	**0,000**	**0,000**	**0,000**	**4,792**
	0,000								**4,792**	**4,792**

TOTAL (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
	32,076								384,966	

3.2. DG HOME Rúbrica 5 «Gastos administrativos»										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Total (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTAL (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual.

3.2.6. Contribución de terceros

– La propuesta/iniciativa **no** prevé la cofinanciación por terceros.

3.3. Incidencia estimada en los ingresos

– ☐ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☒ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

– ☐ en los recursos propios

– ☒ en ingresos diversos

En millones EUR (al tercer decimal)

Línea presupuestaria de ingreso:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[112]								
		Año **2019**	Año **2020**	Año **2021**	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**
Artículo 6313 — Contribución de los países asociados a Schengen (CH, NO, LI, IS).....		pm	pm	pm	pm	pm	pm	pm	pm	pm

En el caso de los ingresos diversos «asignados», especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercutan.

18.0207

Especifíquese el método de cálculo de la incidencia en los ingresos.

El presupuesto incluirá una contribución de los países asociados a la ejecución, aplicación y desarrollo del acervo de Schengen y a las medidas relativas a Eurodac, según lo establecido en los respectivos acuerdos.

[112] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos tras la deducción del 25 % de los gastos de recaudación.