COMISIÓN
EUROPEA

Bruselas, 6.4.2016
COM(2016) 205 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad

1. INTRODUCCIÓN

Europa es una sociedad móvil. Millones de ciudadanos de la UE y nacionales de terceros países cruzan cada día las fronteras interiores y exteriores. En 2015, más de 50 millones de nacionales de terceros países visitaron la UE, lo que representa más de 200 millones de cruces de las fronteras exteriores del espacio Schengen.

Más allá de estos flujos de viajeros regulares, tan solo en 2015, el conflicto en Siria y otras crisis desencadenaron 1,8 millones de cruces irregulares de las fronteras exteriores de Europa. Los ciudadanos de la UE esperan que los controles de personas en las fronteras exteriores sean eficaces, a fin de permitir una gestión eficaz de la migración y contribuir a la seguridad interior. Los ataques terroristas perpetrados en París en 2015 y en Bruselas en marzo de 2016 han demostrado amargamente la continua amenaza que existe para la seguridad interior de Europa.

Ambos elementos apuntan a la necesidad de aunar y reforzar los marcos de la UE en materia de gestión de fronteras, migración y cooperación para la seguridad, y las herramientas de información, de manera exhaustiva. La gestión de las fronteras, las funciones policiales y el control de la migración están interconectados de forma dinámica. Consta que ciudadanos de la UE han cruzado la frontera exterior para viajar a zonas de conflicto con fines terroristas y suponen un riesgo a su retorno. Existen pruebas de que los terroristas han utilizado rutas de migración irregular para entrar en la UE y seguidamente se han desplazado dentro del espacio Schengen sin ser detectados.

Las Agendas Europeas de Seguridad y Migración han fijado la dirección para el desarrollo y la aplicación de la política de la UE destinada a abordar los retos paralelos de la gestión de la migración y la lucha contra el terrorismo y la delincuencia organizada. La presente Comunicación se basa en las sinergias entre dichas Agendas y está concebida como un punto de partida para un debate sobre la forma en que los sistemas de información existentes y futuros podrían reforzar tanto la gestión de las fronteras exteriores como la seguridad interior de la UE. Complementa la propuesta de diciembre de 2015 sobre la creación de una Guardia Europea de Fronteras y Costas y la mejora de la prevención de crisis y la intervención en las fronteras exteriores.

Existen varios sistemas de información a escala de la UE que proporcionan a la guardias de fronteras y agentes de policía información pertinente sobre las personas, pero la arquitectura de gestión de datos de la UE no es perfecta. La presente Comunicación expone algunas de las opciones posibles para maximizar los beneficios de los sistemas de información existentes y, en caso necesario, desarrollar acciones nuevas y complementarias para abordar las carencias. Destaca asimismo la necesidad de mejorar la interoperabilidad de los sistemas de información como objetivo a largo plazo, como también establecieron el Consejo Europeo y el Consejo[1], y presenta ideas sobre la manera en que pueden desarrollarse los sistemas de información en el futuro para garantizar que la guardias de fronteras, las autoridades aduaneras, los agentes de policía y las autoridades judiciales tengan a su disposición la información necesaria.

Cualquier iniciativa futura debería elaborarse sobre la base de los principios de legislar mejor, con consulta pública y evaluación de impacto, en particular por lo que respecta a

[1] Conclusiones de la reunión del Consejo Europeo de 17 y 18 de diciembre de 2015; Declaración conjunta de los Ministros de Justicia y Asuntos de Interior y representantes de las instituciones de la UE sobre los atentados terroristas perpetrados el 22 de marzo de 2016 en Bruselas (24 de marzo de 2016); Conclusiones del Consejo de la Unión Europea y de los Estados miembros reunidos en el seno del Consejo, sobre lucha contra el terrorismo (20 de noviembre de 2015).

los derechos fundamentales, concretamente el derecho a la protección de los datos personales.

2. DESAFÍOS QUE DEBEN ABORDARSE

La ausencia de fronteras interiores en el espacio Schengen exige una gestión sólida y fiable de la circulación de personas por las fronteras exteriores. Esta es una condición previa para garantizar un alto nivel de seguridad interior y la libre circulación de personas dentro de este espacio. Al mismo tiempo, la ausencia de fronteras interiores significa que las autoridades policiales de los Estados miembros también tienen acceso a los datos sobre personas. Existen varios sistemas de información y bases de datos a escala de la UE que proporcionan a la guardia de fronteras, la policía y otras autoridades información pertinente sobre las personas, de acuerdo con sus respectivos objetivos[2].

Sin embargo, existen deficiencias relativas a los sistemas de información que obstaculizan la labor de estas autoridades nacionales. Por tanto, la Agenda Europea de Seguridad destacaba el intercambio de información como una de las prioridades clave. Las principales deficiencias son: a) funcionalidades de los sistemas de información existentes por debajo del nivel óptimo; b) deficiencias en la arquitectura de gestión de datos de la UE; c) un panorama complejo de sistemas de información gestionados de manera diferente; y d) una estructura fragmentada de gestión de datos para el control de las fronteras y la seguridad.

Los sistemas de información existentes en la UE para la gestión de las fronteras y la seguridad interior cubren un amplio abanico de funcionalidades. No obstante, sigue habiendo **carencias en las funcionalidades de los sistemas existentes**. Al examinar los procedimientos de control en las fronteras aplicables a distintas categorías de viajeros, se pone de manifiesto que existen deficiencias en algunos de estos procesos y entre los respectivos sistemas de información utilizados en los controles fronterizos. Asimismo, es preciso optimizar el rendimiento de las herramientas existentes para las fuerzas de seguridad. Esto exige estudiar medidas para mejorar los sistemas de información actuales (sección 5).

Por otra parte, existen **lagunas en la arquitectura de gestión de datos de la UE**. Sigue habiendo cuestiones pendientes en cuanto a los controles fronterizos de categorías específicas de viajeros, como los nacionales de terceros países titulares de un visado de larga duración. Asimismo, hay un vacío de información antes de la llegada a las fronteras por lo que se refiere a los nacionales de terceros países que están exentos de la obligación de visado. Debe considerarse si es preciso abordar dichas lagunas desarrollando sistemas de información adicionales cuando sea necesario (sección 6).

La guardia de fronteras y en particular los agentes de policía se enfrentan a un **panorama complejo de sistemas de información gestionados de forma diferente** a escala de la UE. Esta complejidad ocasiona dificultades prácticas, en particular en cuanto a qué bases de datos deberían comprobarse en una situación determinada. Además, no todos los Estados miembros están conectados a todos los sistemas existentes[3]. La complejidad

[2] Véase la sección 4 para una descripción general de los sistemas de información para las fronteras y la seguridad, y el anexo 2 para un inventario más detallado.

[3] Con sujeción a las disposiciones específicas del Protocolo n.º 22 por lo que respecta a Dinamarca, y los Protocolos n.º 21 y 36 por lo que respecta al Reino Unido e Irlanda, y las respectivas Actas de Adhesión.

actual de acceder a los sistemas de información a nivel de la UE podría reducirse mediante el establecimiento de una interfaz única de búsqueda a escala nacional que respete los diferentes fines del acceso (sección 7.1).

La actual arquitectura de gestión de datos de la UE para el control de las fronteras y la seguridad se caracteriza por la **fragmentación**. Esto se debe a los diferentes contextos institucionales, jurídicos y políticos en los que se han desarrollado estos sistemas. La información se almacena por separado en diferentes sistemas que rara vez están interconectados. No hay coherencia entre las bases de datos y existen divergencias de acceso a los datos por parte de las autoridades pertinentes. Esto puede llevar a ángulos muertos, en particular para las autoridades policiales, ya que puede ser muy difícil reconocer conexiones entre fragmentos de datos. En consecuencia, es necesario y urgente avanzar hacia soluciones integradas para mejorar el acceso a los datos con fines de gestión de las fronteras y seguridad, respetando plenamente los derechos fundamentales. Para ello, es preciso iniciar un proceso hacia la interoperabilidad de los sistemas de información existentes (sección 7).

3. DERECHOS FUNDAMENTALES

El pleno respeto de los derechos fundamentales y las normas de protección de datos es una condición previa esencial para abordar cualquiera de estos desafíos.

El respeto de los derechos fundamentales exige tecnología y sistemas de información bien diseñados y utilizados correctamente. La tecnología y los sistemas de información pueden ayudar a los poderes públicos a proteger los derechos fundamentales de los ciudadanos. La tecnología biométrica puede reducir el riesgo de confusión de identidades, de discriminación y de control policial con sesgo racista. También puede contribuir a hacer frente a los riesgos de protección para los niños tales como los niños desaparecidos o víctimas de la trata, si va acompañada de salvaguardias de los derechos fundamentales y de medidas de protección. Este sistema puede reducir el riesgo de interpelaciones o detenciones injustas. Puede contribuir también a incrementar la seguridad de los ciudadanos que residen en el espacio Schengen, ya que con ello se contribuiría a la lucha contra el terrorismo y los delitos graves.

La existencia de sistemas de información a gran escala también implica riesgos potenciales para la intimidad, que deben preverse y abordarse convenientemente. La recopilación y el uso de datos personales en estos sistemas tiene repercusiones en el derecho a la intimidad y la protección de los datos personales, consagrados en la Carta de los Derechos Fundamentales de la Unión Europea. Todos los sistemas deben ajustarse a los principios de protección de datos y a los requisitos de necesidad, proporcionalidad, limitación de la finalidad y calidad de los datos. Es preciso establecer salvaguardias para garantizar los derechos de los interesados en relación con la protección de su vida privada y sus datos personales. Los datos solo deberán conservarse durante el tiempo que sea necesario para la finalidad para la que fueron recogidos. Deben preverse mecanismos que garanticen una gestión del riesgo adecuada y una protección efectiva de los derechos de los interesados.

En diciembre de 2015, los colegisladores alcanzaron un acuerdo político sobre la reforma de la protección de datos. Una vez adoptado, el nuevo Reglamento general de protección de datos y la Directiva sobre protección de datos por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de

infracciones penales o de ejecución de sanciones penales[4] serán aplicables en 2018 y proporcionarán un marco armonizado para el tratamiento de los datos personales.

La limitación de la finalidad es un principio clave de la protección de datos consagrado en la Carta de los Derechos Fundamentales. Debido a los diferentes contextos políticos, institucionales y jurídicos en que se desarrollaron los sistemas de información a escala de la UE, el principio de limitación de la finalidad se estableció mediante una estructura compartimentada de gestión de la información[5]. Esta es una de las razones de la fragmentación actual en la arquitectura de la UE de gestión de datos para el control fronterizo y la seguridad interior. Con el nuevo marco general para la protección de datos personales en la UE en vigor y unos cambios significativos en la tecnología y la seguridad informática, el principio de limitación de la finalidad puede aplicarse más fácilmente por lo que respecta al nivel de acceso y la utilización de los datos almacenados, de plena conformidad con la Carta de los Derechos Fundamentales y con la reciente jurisprudencia del Tribunal de Justicia Europeo. Garantías como la compartimentación de los datos dentro de un sistema y normas específicas de acceso y utilización para cada categoría de datos y de usuarios, garantizarán la necesaria limitación de la finalidad en las soluciones integradas de gestión de datos. Esto abre una vía hacia la interoperabilidad de los sistemas de información que va acompañada de las necesarias normas estrictas en materia de acceso y uso sin afectar a la actual limitación de la finalidad.

La «protección de los datos desde el diseño» y la «protección de los datos por defecto» son ahora principios de la normativa europea de protección de datos. Al desarrollar nuevos instrumentos basados en el uso de tecnología de la información, la Comisión tratará de seguir este enfoque. Esto supone integrar la protección de datos personales en la base tecnológica del instrumento propuesto, limitando el tratamiento de datos a lo que sea necesario para el objetivo propuesto y concediendo el acceso a los datos sólo a las entidades con «necesidad de conocer»[6].

Los requisitos de la Carta de los Derechos Fundamentales, y en particular los nuevos instrumentos de reforma de la protección de datos servirán de guía a la Comisión a la hora de abordar las actuales lagunas y deficiencias en la arquitectura de la UE de gestión de datos para el control de las fronteras y la seguridad. Con ello se garantizará que el desarrollo futuro de sistemas de información en estos ámbitos se haga en consonancia con las normas más exigentes en materia de protección de datos, y que estos sistemas respetarán y contribuirán a los derechos fundamentales garantizados por la Carta de los Derechos Fundamentales.

---

4 Véase http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

5 COM(2010) 385 final.

6 Para una amplia descripción de la «protección de la intimidad desde el diseño» véase el Dictamen del SEPD acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, Supervisor Europeo de Protección de Datos, 18.3.2010.

4. DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA LAS FRONTERAS Y LA SEGURIDAD[7]

Los sistemas de información existentes en la UE para la gestión de las fronteras y la seguridad interior tienen cada uno sus propios objetivos, finalidades, bases jurídicas[8], grupos de usuarios y contexto institucional. Juntos constituyen un complejo modelo de bases de datos pertinentes.

Los tres principales **sistemas de información centralizados** desarrollados por la UE son: i) el Sistema de Información de Schengen (SIS) con un amplio espectro de descripciones de personas y objetos; ii) el Sistema de Información de Visados (VIS) con datos sobre visados para estancias de corta duración; y iii) el sistema EURODAC, con datos relativos a impresiones dactilares de solicitantes de asilo y nacionales de terceros países que han cruzado las fronteras exteriores de forma irregular. Estos tres sistemas son complementarios y, con la excepción del SIS, están principalmente destinados a los nacionales de terceros países. Los sistemas también apoyan a las autoridades nacionales en la lucha contra la delincuencia y el terrorismo[9]. Esto se aplica en particular al SIS como instrumento de intercambio de información más utilizado en la actualidad. El intercambio de información de estos sistemas se realiza en una infraestructura de comunicación específica segura denominada sTesta[10].

Además de estos sistemas existentes, la Comisión propone crear un cuarto sistema centralizado de gestión de las fronteras, el **Sistema de Entradas y Salidas** (SES)[11], que se espera entre en funcionamiento en 2020, dirigido asimismo a los nacionales de terceros países.

---

7 En el anexo 2 figura un inventario de los sistemas de información existentes para la gestión de las fronteras y los servicios policiales.

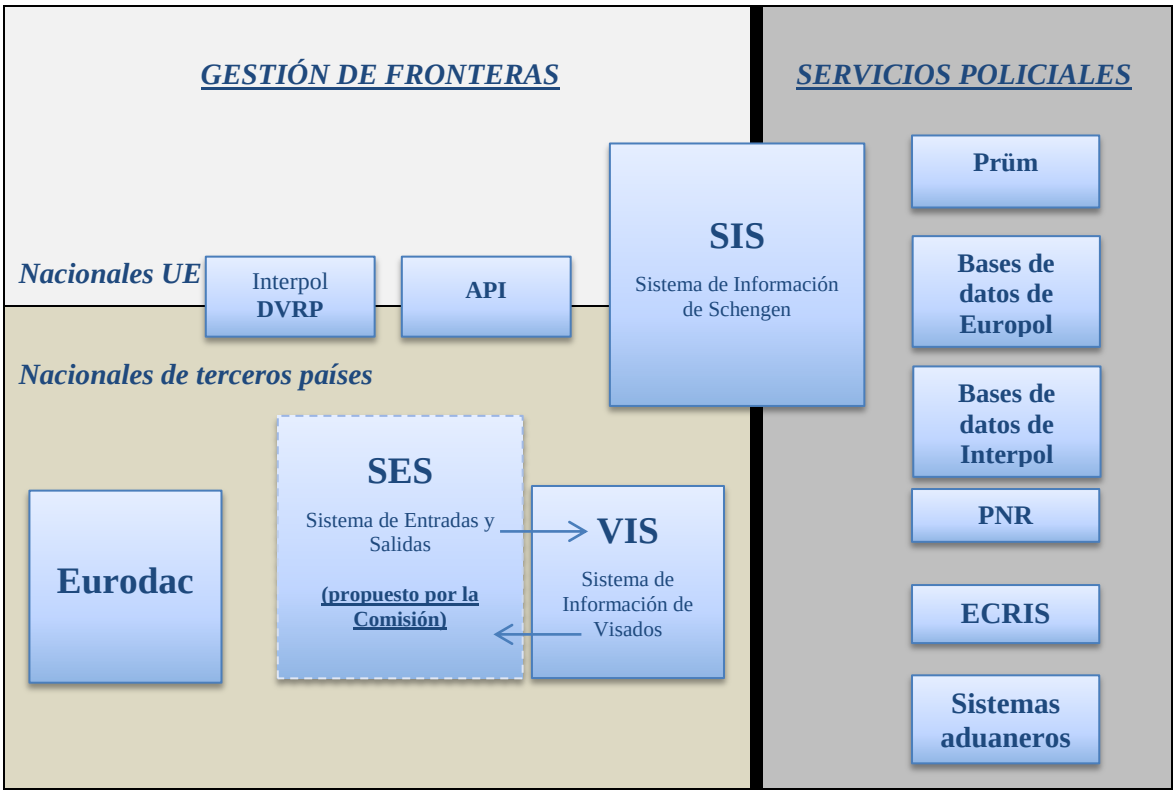
8 Con sujeción a las disposiciones específicas del Protocolo n.º 22 por lo que respecta a Dinamarca, y de los Protocolos n.º 21 y 36 por lo que respecta al Reino Unido y a Irlanda.

9 El acceso de las autoridades policiales al VIS y a EURODAC puede ejercerse en condiciones limitadas debido al hecho de que los servicios policiales son un objetivo accesorio de dichos sistemas. En relación con VIS, los Estados miembros tienen que designar una autoridad responsable de controlar el acceso de las autoridades policiales, y la policía deberá aportar pruebas de que su acceso es necesario para las investigaciones penales. En relación con EURODAC, la autoridad encargada de la investigación debe buscar en el SAID nacional, el VIS y Prüm antes de que se le conceda acceso a EURODAC.

10 Pronto será sustituido por TESTA-NG.

11 COM(2016)194 final.

Figura 1 *Sinopsis esquemática de los principales sistemas de información para la gestión de fronteras y los servicios policiales:*



Otros instrumentos existentes para la gestión de fronteras son la base de datos de Interpol sobre documentos de viaje robados y perdidos (DVRP) y el sistema de información anticipada sobre los pasajeros (API), que recopila información sobre los pasajeros antes de los vuelos con destino a la UE. Estos instrumentos son pertinentes para los ciudadanos de la UE y los nacionales de terceros países.

Específicamente con fines policiales, de investigación penal y cooperación judicial, la UE ha desarrollado **instrumentos descentralizados para el intercambio de información**, a saber: i) el marco de Prüm para intercambiar ADN, impresiones dactilares y datos de matriculación de vehículos; y ii) el Sistema Europeo de Información de Antecedentes Penales (ECRIS) para el intercambio de información sobre antecedentes penales nacionales. ECRIS permite el intercambio de información, a través de una red segura, sobre las condenas anteriores pronunciadas contra una persona determinada por los órganos jurisdiccionales penales en la Unión Europea. Las solicitudes se basan principalmente en información de identificación alfanumérica, aunque es posible el intercambio de datos biométricos.

Europol apoya el intercambio de información entre las autoridades policiales nacionales como eje de información criminal de la UE. El sistema de información de Europol (SIE) proporciona una base de datos centralizada de información penal para que los Estados miembros almacenen y consulten datos relativos a la delincuencia grave y el terrorismo. Los puntos de contacto de Europol proporcionan ficheros de trabajo de análisis sobre temas concretos con información sobre las operaciones en curso en los Estados miembros. La Aplicación de la Red de Intercambio Seguro de Información (SIENA) de Europol permite a los Estados miembros intercambiar información de manera rápida, segura y fácil entre sí, con Europol, o con terceros que hayan celebrado un acuerdo de cooperación con Europol. Al mismo tiempo, SIENA presta gran atención a la interoperabilidad con otros sistemas en Europol, por ejemplo para intercambiar

directamente información con los puntos de contacto, y ofrece la posibilidad de alimentar las bases de datos de Europol con información intercambiada entre Estados miembros. Los Estados miembros deben por tanto utilizar SIENA como primer canal para el intercambio de informaciones policiales en la UE.

Un conjunto suplementario de sistemas de tratamiento de datos personales que se desarrollará en los Estados miembros es el **registro de nombres de los pasajeros** (PNR)[12]. Los datos PNR consisten en información sobre reservas facilitada en el momento de la reserva y la facturación.

Por último, las **autoridades aduaneras** son también una parte crucial de la cooperación entre organismos en las fronteras exteriores. Cuentan con diferentes sistemas[13] y bases de datos que contienen información sobre movimientos de mercancías, identificación de operadores económicos e información relacionada con riesgos que pueden utilizarse para reforzar la seguridad interior. Estos sistemas tienen también su propia infraestructura segura, restringida y controlada (Red Común de Comunicación), que ha demostrado su viabilidad. Es preciso seguir explorando las sinergias y la convergencia entre los sistemas de información y sus correspondientes infraestructuras para la gestión de las fronteras de la UE y las operaciones aduaneras.

5. MEJORA DE LOS SISTEMAS DE INFORMACIÓN EXISTENTES

Los sistemas de información existentes en la UE para la gestión de las fronteras y la seguridad interior cubren un amplio abanico de funcionalidades. Sin embargo, todavía existen **deficiencias** en los sistemas que deben abordarse a fin de optimizar su rendimiento.

Sistema de Información de Schengen (SIS)

Los controles fronterizos con arreglo al **Sistema de Información de Schengen** (SIS) se realizan actualmente sobre la base de consultas alfanuméricas (es decir, nombre y fecha de nacimiento). Las impresiones dactilares solo pueden utilizarse para comprobar y confirmar la identidad de una persona que ya haya sido identificada por su nombre. Esta laguna de seguridad permite a las personas objeto de una descripción utilizar documentos fraudulentos para escapar de una correspondencia exacta en el SIS.

Esta deficiencia crítica se abordará añadiendo al SIS una función de búsqueda de impresiones dactilares mediante un **Sistema Automático de Identificación Dactilar (SAID)**, tal y como se prevé en el marco jurídico vigente[14]. El SAID debería estar operativo a mediados de 2017[15]. Una vez desarrollado, el SAID será accesible por

[12] Véase la sección 6.2.

[13] Los sistemas de información aduanera incluyen todos los sistemas creados en virtud del Código Aduanero Comunitario (Reglamento 2913/92) y el futuro código aduanero de la Unión (Reglamento 952/2013), la Decisión relativa a un entorno sin soporte papel en las aduanas y el comercio (Decisión 70/2008/CE) y el Sistema de Información Aduanero establecido en el marco del Convenio SIA de 1995. Su objetivo es ayudar en la lucha contra delitos en materia aduanera facilitando la cooperación entre las autoridades aduaneras europeas.

[14] Artículo 22, letra c), del Reglamento (CE) n.º 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) y 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 381 de 28.12.2006, p. 4 y DO L 205 de 7.8.2007, p. 63).

[15] En marzo de 2016, la Comisión presentó un informe al Parlamento Europeo y al Consejo sobre la disponibilidad y grado de preparación de la tecnología para identificar a una persona sobre la base de

Europol y servirá de complemento a los sistemas de Europol para las investigaciones penales y de lucha contra el terrorismo, así como para los intercambios de impresiones dactilares realizadas en el marco de Prüm. La Comisión y eu-LISA estudiarán el potencial de ese mayor uso del futuro SAID.

Sobre la base de la evaluación continua y de un estudio técnico, la Comisión está evaluando **otras posibles funciones del SIS** con vistas a presentar propuestas para revisar la base jurídica del SIS. Entre los aspectos considerados figuran los siguientes:

- la creación de descripciones del SIS relativas a migrantes irregulares sujetos a una decisión de retorno;
- el uso de imágenes faciales para la identificación biométrica, además de las impresiones dactilares;
- la transmisión automatizada de información sobre una respuesta positiva a raíz de una comprobación;
- el almacenamiento de información sobre una respuesta positiva a descripciones de controles discretos y específicos en el sistema central del SIS;
- la creación de una nueva categoría de descripciones sobre «personas desconocidas buscadas» para las que puedan existir datos forenses en las bases de datos nacionales (por ejemplo, una impresión latente dejada en la escena de un crimen)[16].

La Comisión seguirá apoyando con financiación de la UE la aplicación de proyectos que permitan la realización de consultas simultáneas en el SIS y en las bases de datos de Interpol sobre documentos de viaje robados y perdidos (DVRP) y armas de fuego (iARMS), vehículos y personas buscadas que complementan a los sistemas de información de la UE[17].

Base de datos de documentos de viaje robados y perdidos (DVRP) de Interpol

Para una gestión eficaz de las fronteras es de vital importancia que los documentos de viaje de todos los nacionales de terceros países y ciudadanos de la UE se contrasten con la **base de datos DVRP**. Las autoridades policiales también deberían utilizar la base de datos DVRP para búsquedas en el espacio Schengen. Tras los atentados terroristas perpetrados en París el 13 de noviembre de 2015, el Consejo hizo un llamamiento para establecer conexiones electrónicas con las bases de datos de Interpol pertinentes en todos los pasos fronterizos exteriores y un control automático de los documentos de viaje para marzo de 2016[18]. Todos los Estados miembros deben establecer las conexiones electrónicas e instalar sistemas que permitan la actualización automática de datos sobre documentos de viaje robados o perdidos en la base de datos DVRP.

Información anticipada sobre los pasajeros (API)

En línea con las mejores prácticas existentes, los Estados miembros también deben aumentar el valor añadido de la **información anticipada sobre los pasajeros** (API),

---

las impresiones dactilares almacenadas en el Sistema de Información de Schengen de segunda generación (SIS II).

[16] La creación de esta nueva descripción se evaluará a fin de garantizar la complementariedad y evitar solapamientos con el actual marco de Prüm para la búsqueda de impresiones dactilares en las diferentes bases de datos nacionales de los Estados miembros de la UE.

[17] Algunas herramientas de búsqueda de información desarrolladas por Interpol, tales como la base de datos fija en red de Interpol (BFRI) y la base de datos móvil en red de Interpol (BMRI), tienen por objeto facilitar búsquedas simultáneas en los sistemas de Interpol y en el SIS.

[18] Conclusiones del Consejo de la UE y de los Estados miembros reunidos en el Consejo sobre la lucha contra el terrorismo, 20 de noviembre de 2015.

estableciendo controles cruzados automatizados de estos datos con el SIS y la base de datos DVRP de Interpol. La Comisión evaluará la necesidad de revisar la base jurídica para el tratamiento de los datos API a fin de garantizar una aplicación más amplia, y de incluir la obligación de que los Estados miembros soliciten y utilicen datos API para todos los vuelos entrantes y salientes. Esto es especialmente importante en el contexto de la aplicación de la futura Directiva sobre el registro de nombres de los pasajeros, dado que el uso combinado de los datos API y PNR reforzarán la eficacia de los datos PNR en la lucha contra el terrorismo y la delincuencia grave[19].

Sistema de Información de Visados (VIS)

La Comisión también está realizando una evaluación global del **Sistema de Información de Visados** (VIS), que está previsto finalice en 2016. La evaluación examina, entre otras cosas, cómo se utiliza el VIS para los controles en las fronteras exteriores y en el territorio de los Estados miembros, y la manera en que contribuye a la lucha contra el fraude de identidad y visados. Sobre esta base, la Comisión examinará las posibilidades de mejorar las funcionalidades del VIS, en particular:

- mejorando la calidad de las imágenes faciales para permitir la comparación de los datos biométricos;
- utilizando los datos biométricos de los solicitantes de visado para la búsqueda en el futuro Sistema Automático de Identificación Dactilar que se desarrollará para el SIS;
- reduciendo el límite de edad para la toma de impresiones dactilares de los niños de edades comprendidas entre los 6 y los 12 años, al tiempo que se prevén sólidas salvaguardias de los derechos fundamentales y medidas de protección[20];
- facilitando el control de la base de datos DVRP de Interpol en el contexto de las solicitudes de visado.

En lo que respecta a las posibilidades que ofrece el marco jurídico vigente para acceder a los datos del VIS con **fines policiales**, los Estados miembros aplican estas posibilidades de forma desigual. En este contexto, algunos Estados miembros han notificado problemas prácticos en los procedimientos de acceso al VIS por las autoridades policiales. Asimismo, el establecimiento del acceso a EURODAC con fines policiales sigue estando muy limitado. La Comisión estudiará si es necesario revisar el marco jurídico para el acceso de las autoridades policiales al VIS y a EURODAC.

EURODAC

Según lo establecido en la Comunicación Hacia una reforma del Sistema Europeo Común de Asilo y una mejora de las vías legales a Europa[21], la Comisión presentará una propuesta de reforma de **EURODAC** para mejorar sus funcionalidades en lo que respecta a la migración irregular y el retorno. Esto permitirá abordar una laguna existente en relación con la capacidad para rastrear los movimientos secundarios de los inmigrantes irregulares entre Estados miembros. Por otra parte, la propuesta buscará mejorar la eficacia de los procedimientos de retorno y readmisión aportando medios para identificar y redocumentar a los migrantes irregulares a efectos de retorno. En este contexto, la propuesta también cubrirá el intercambio con terceros países de información contenida en

[19] Véase la sección 6.2 sobre la propuesta de Directiva relativa al registro de nombres de los pasajeros.

[20] Indicado como técnicamente factible en el estudio de JRC *Fingerprint recognition for children* (Reconocimiento de impresiones dactilares de niños), EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013.

[21] COM(2016)197 final.

EURODAC, teniendo en cuenta las salvaguardias necesarias en cuanto a protección de datos.

Europol

La UE ha concedido a **Europol** acceso a las principales bases de datos centrales, pero la Agencia aún no ha utilizado plenamente esta oportunidad. Europol tiene derecho de acceso y búsqueda directa en los datos introducidos en el SIS a efectos de detención, a efectos de controles discretos y específicos y a efectos de la incautación de objetos. Hasta la fecha, Europol solo ha realizado un número relativamente limitado de búsquedas en el SIS. El acceso al VIS para consulta es legalmente posible para Europol desde septiembre de 2013. Desde julio de 2015, la base jurídica de EURODAC permite el acceso de Europol. La Agencia debe acelerar los trabajos en curso para establecer la conexión al VIS y a EURODAC. De manera más general, la Comisión evaluará si es necesario facilitar el acceso a los sistemas de información de otras agencias de la UE en el ámbito de los asuntos de interior, especialmente por lo que se refiere al futuro de la Guardia Europea de Fronteras y Costas.

Marco de Prüm

El **marco de Prüm** funciona actualmente por debajo de su potencial. Ello se debe a que no todos los Estados miembros han cumplido sus obligaciones legales en términos de integración de la red en sus propios sistemas. Los Estados miembros han recibido un apoyo financiero y técnico considerable para su aplicación, y deberían aplicar ya plenamente el marco de Prüm. La Comisión está utilizando los poderes que se le han conferido para garantizar el pleno cumplimiento de las obligaciones legales de los Estados miembros, e inició un diálogo estructurado (EU Pilot) con los Estados miembros afectados en enero de 2016. En caso de que las respuestas de los Estados miembros no sean satisfactorias, la Comisión no dudará en incoar procedimientos de infracción.

Sistema Europeo de Información de Antecedentes Penales (ECRIS)

El Sistema Europeo de Información de Antecedentes Penales **ECRIS** permite el intercambio de información sobre las condenas de nacionales de terceros países y apátridas, pero no existe ningún procedimiento para hacerlo eficazmente. En enero de 2016, la Comisión adoptó una propuesta legislativa para subsanar esta laguna[22]. En este contexto, la Comisión propuso permitir que las autoridades nacionales puedan buscar a nacionales de terceros países mediante sus impresiones dactilares a efectos de una identificación más segura. El Parlamento Europeo y el Consejo deben adoptar el texto legislativo en 2016.

Cuestiones horizontales

Un motivo de preocupación general en relación con los sistemas de información es el **nivel de aplicación** por parte de los Estados miembros. La aplicación desigual del marco de Prüm y la falta de conexiones electrónicas con la base de datos DVRP son ejemplos destacados de esto. Para mejorar el nivel de aplicación en lo que respecta a los sistemas de información, la Comisión seguirá de cerca la actuación de cada Estado miembro[23]. El seguimiento no solo examinará si los Estados miembros cumplen sus obligaciones legales en el ámbito de los sistemas de información, sino también la manera en que utilizan los instrumentos existentes y si se ajustan a las mejores prácticas. La Comisión recurrirá a diversas fuentes para controlar y promover el nivel de aplicación, en particular

[22] COM(2016) 7 final de 19.1.2016.

[23] Con sujeción a las disposiciones específicas del Protocolo n.º 22 por lo que respecta a Dinamarca, y los Protocolos n.º 21 y 36 por lo que respecta al Reino Unido e Irlanda.

a las notificaciones de los Estados miembros y a las visitas realizadas en el marco del mecanismo de evaluación y seguimiento de Schengen.

Otra preocupación general en relación con los sistemas de información es la **calidad de los datos introducidos**. Si los Estados miembros no respetan los requisitos mínimos de calidad, la fiabilidad y el valor de los datos almacenados quedan muy limitados, y el riesgo de correspondencias erróneas y falta de respuestas positivas socava el valor de los sistemas. Con el fin de mejorar la calidad de los datos introducidos, eu-LISA elaborará una **capacidad central de control de la calidad de los datos** para todos los sistemas en el ámbito de sus competencias.

La mayoría de los sistemas de información en el ámbito de los controles fronterizos y la seguridad manejan datos procedentes de documentos de identidad y de viaje. Para reforzar las fronteras y la seguridad, además de unos sistemas que funcionen correctamente, los documentos de viaje y de identidad deben autenticarse con facilidad y seguridad. Con este fin, la Comisión presentará una serie de medidas para mejorar la gestión de la identidad y la **seguridad de los documentos** de forma electrónica e intensificar la lucha contra el fraude documental. Los niveles interoperables de identificación segura que pueden alcanzarse gracias al Reglamento eIDAS[24] podrían proporcionar un medio posible para lograrlo.

Acciones destinadas a mejorar los sistemas de información existentes

Sistema de Información de Schengen (SIS)

- La Comisión y eu-LISA desarrollarán y aplicarán un Sistema Automático de Identificación Dactilar (SAID) en el SIS como muy tarde a mediados de 2017.
- La Comisión presentará propuestas antes de finales de 2016 para revisar la base jurídica del SIS, con el fin de mejorar su funcionalidad.
- Los Estados miembros maximizarán su utilización del SIS, tanto mediante la introducción de toda la información pertinente como consultando el sistema cuando sea necesario.

Base de datos de documentos de viaje robados y perdidos de Interpol (DVRP)

- Los Estados miembros establecerán conexiones electrónicas con los instrumentos de Interpol en todos sus pasos fronterizos exteriores.
- Los Estados miembros respetarán su obligación de introducir y consultar datos sobre documentos de viaje perdidos o robados en el SIS y en la base de datos DVRP al mismo tiempo.

Información anticipada sobre los pasajeros (API)

- Los Estados miembros automatizarán el uso de los datos API para las comprobaciones en el SIS y en la base de datos de documentos de viaje robados y perdidos de Interpol (DVRP), en línea con las mejores prácticas existentes.
- Comisión valorará la necesidad de revisar la base jurídica para el tratamiento de los datos API.

[24] Reglamento (UE) n.° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Sistema de Información de Visados (VIS)

- La Comisión estudiará nuevas mejoras del VIS antes de finales de 2016.

EURODAC

- La Comisión presentará una propuesta para revisar la base jurídica de EURODAC para mejorar sus funcionalidades en lo que respecta a la migración irregular y el retorno.

Europol

- Europol deberá hacer pleno uso de sus derechos de acceso al SIS, VIS y EURODAC, para fines de consulta.
- Los servicios de la Comisión y Europol estudiarán y promoverán sinergias entre el sistema de información de Europol (SIE) y otros sistemas, en particular el SIS.
- La Comisión y eu-LISA examinarán si el Sistema Automático de Identificación Dactilar (SAID) que se desarrollará para el SIS puede complementar los sistemas de Europol a efectos de las investigaciones penales y de la lucha contra el terrorismo.

Marco de Prüm

- Los Estados miembros deberán aplicar y utilizar plenamente el marco de Prüm.
- En caso necesario, la Comisión incoará procedimientos de infracción contra los Estados miembros que no se hayan conectado al marco de Prüm.
- La Comisión y eu-LISA examinarán si el Sistema Automático de Identificación Dactilar (SAID) que se desarrollará para el SIS puede complementar los intercambios de datos sobre impresiones dactilares efectuados en el marco de Prüm.

Sistema Europeo de Información de Antecedentes Penales (ECRIS)

- El Parlamento Europeo y el Consejo deberán adoptar en 2016 la propuesta legislativa que permita a las autoridades nacionales consultar el sistema ECRIS para buscar a nacionales de terceros países por sus impresiones dactilares.

Cuestiones horizontales

- La Comisión deberá **vigilar y promover el nivel de aplicación** en relación con los sistemas de información.
- eu-LISA deberá desarrollar una **capacidad central de control de la calidad de los datos** para todos los sistemas en el ámbito de sus competencias.
- La Comisión deberá presentar medidas para mejorar la **gestión de la identidad y la seguridad de los documentos** de forma electrónica e intensificar la lucha contra el fraude documental.
- La Comisión deberá explorar las sinergias y la convergencia entre los sistemas de información y sus correspondientes infraestructuras para la gestión de las fronteras de la UE y las **operaciones aduaneras**.

6. DESARROLLO DE SISTEMAS DE INFORMACIÓN ADICIONALES Y SOLUCIÓN DE DEFICIENCIAS

Si bien los sistemas de información existentes cubren un abanico muy amplio de los datos exigidos en el marco de la gestión de las fronteras y los servicios policiales, también hay importantes lagunas. Algunas de estas han sido abordadas por la Comisión con propuestas legislativas, en particular las propuestas para un Sistema de Entradas y Salidas y para un sistema de la UE de registro de nombres de los pasajeros (PNR). Para

otras deficiencias, es necesario realizar una evaluación minuciosa para determinar si se precisan herramientas de la UE adicionales.

1. Sistema de Entradas y Salidas

Paralelamente a la presente Comunicación, la Comisión ha presentado las propuestas legislativas revisadas para el establecimiento de un Sistema de Entradas y Salidas (SES). Tras la adopción por los colegisladores, corresponderá a eu-LISA desarrollar y aplicar el sistema, en colaboración con los Estados miembros de Schengen.

El SES sistema registrará el cruce de fronteras (entrada y salida) de todos los nacionales de terceros países que visitan el espacio Schengen para una estancia de corta duración (máximo de 90 días en cualquier período de 180 días), tanto de los viajeros sujetos a la obligación de visado como de los que están exentos de dicha obligación, o para estancias sobre la base del nuevo visado itinerante (hasta un año). Los objetivos del SES son: a) mejorar la gestión de las fronteras exteriores; b) reducir la migración irregular, abordando el fenómeno del rebasamiento de la estancia legal; y c) contribuir a la lucha contra el terrorismo y las formas graves de delincuencia, contribuyendo así a garantizar un alto nivel de seguridad interior.

El SES registrará la identidad de los nacionales de terceros países (datos alfanuméricos, cuatro impresiones dactilares e imagen facial), junto con detalles de sus documentos de viaje, y los vinculará a los registros electrónicos de entrada y salida. La actual práctica de sellado de los documentos de viaje quedará suprimida. El SES permitirá la gestión efectiva de las estancias de corta duración autorizadas, una mayor automatización en los controles fronterizos, y una mejor detección del fraude documental y de identidad. El registro central permitirá la detección de las personas en situación de permanencia ilegal y la identificación de las personas sin papeles en el espacio Schengen. El SES propuesto aborda, por tanto, una carencia importante en el contexto de los sistemas de información existentes.

2. Registros de nombres de los pasajeros

Los datos del registro de nombres de los pasajeros (PNR) consisten en información sobre la reserva con los datos de contacto, el trayecto completo y detalles sobre la reserva, observaciones especiales, información relativa al asiento y al equipaje, y medios de pago. Los datos PNR son útiles y necesarios para identificar a pasajeros de alto riesgo en el contexto de la lucha contra el terrorismo, el tráfico de drogas, la trata de seres humanos, la explotación sexual de niños y otras formas graves de delincuencia. La propuesta de Directiva sobre PNR garantizará una mejor cooperación entre los sistemas nacionales y reducirá las brechas de seguridad entre los Estados miembros. La propuesta de Directiva sobre PNR aborda, por tanto, una carencia importante en la disponibilidad de los datos, que se precisa para la lucha contra la delincuencia grave y el terrorismo. **La Directiva sobre PNR debe adoptarse y ponerse en práctica con carácter urgente.**

La futura Directiva prevé que los Estados miembros deben crear Unidades de Información sobre Pasajeros (UIP) para recibir datos PNR de las compañías aéreas. Ello no supondrá la creación de un sistema o una base de datos central, pero se beneficiará de un cierto grado de normalización de los procedimientos y soluciones técnicas. Esto facilitará el intercambio de datos PNR entre las Unidades de Información sobre Pasajeros, tal como se prevé en la propuesta de Directiva. Con este fin, la Comisión ayudará a los Estados miembros a analizar diferentes escenarios para la interconectividad entre las UIP, con vistas a ofrecer soluciones y procedimientos normalizados. Una vez adoptada la Directiva, la Comisión acelerará los trabajos sobre los protocolos comunes y los formatos de datos admitidos para la transferencia de datos PNR por las compañías

aéreas a las UIP. La Comisión elaborará un proyecto de acto de ejecución en el plazo de tres meses tras la adopción de la Directiva.

3. Falta de información previa a la llegada de nacionales de terceros países no sujetos a la obligación de visado

Si bien la identidad, los contactos y la información de los titulares de los visados están registrados en el VIS, la única información sobre las personas exentas de la obligación de visado procede de su documento de viaje. Para los pasajeros que llegan por vía aérea o marítima esto podrá completarse antes de la llegada mediante los datos API. Con arreglo a la propuesta de Directiva sobre PNR, los datos PNR de estos pasajeros también se recopilarán si llegan a la UE por vía aérea. Para las personas que entran en la UE a través de las fronteras terrestres, no se dispone de información previa a su llegada a la frontera exterior de la UE.

Mientras que las autoridades policiales pueden obtener del VIS información sobre los titulares de visados si es necesario para la lucha contra la delincuencia grave y el terrorismo, no se dispone de datos comparables sobre las personas exentas de la obligación de visado. Esta falta de información es especialmente relevante para la gestión de las fronteras terrestres de la UE, en una situación en la que un número considerable de viajeros no sujetos a la obligación de visado llegan en coche, autobús o tren. Varios países vecinos de la UE ya están exentos de la obligación de visado, y los diálogos sobre la liberalización de visados entre la UE y otros países vecinos están avanzando. Ello conllevará probablemente un considerable aumento del número de viajeros no sujetos a la obligación de visado en un futuro próximo.

La Comisión examinará si es necesario, factible y proporcional crear un nuevo instrumento de la UE para responder a esta cuestión. Una opción que puede considerarse es un **Sistema de autorización e información sobre viajes de la UE** (SAIV), en el que los viajeros exentos de la obligación de visado registrarían la información pertinente sobre su viaje previsto. El tratamiento automático de esta información podría ayudar a los agentes de la guardia de fronteras en su evaluación de los visitantes que llegan de un tercer país para una estancia de corta duración. Países como Estados Unidos, Canadá y Australia ya han puesto en marcha sistemas similares, incluso para los ciudadanos de la UE.

Los sistemas de autorización de viaje se basan en solicitudes en línea en las que el solicitante presenta datos sobre su identidad, datos de contacto, objeto del viaje, itinerario, etc. antes de la salida. Una vez obtenida la autorización, los procedimientos en la frontera a la llegada son más rápidos y fluidos. Más allá de los beneficios para la seguridad y la gestión fronteriza, y de su posible relevancia en el contexto de la reciprocidad en materia de visados, un sistema como el SAIV podría servir también como instrumento de facilitación de los viajes.

4. Sistema Europeo de Índice de Ficheros Policiales (EPRIS)

Como se indica en la Agenda Europea de Seguridad, la disponibilidad en tiempo real de los datos policiales existentes en los Estados miembros será objeto de futuros trabajos sobre intercambio de información. La Comisión evaluará la necesidad, la viabilidad técnica y la proporcionalidad de un Sistema Europeo de Índice de Ficheros Policiales (EPRIS) para facilitar el acceso transfronterizo a la información contenida en las bases de datos policiales nacionales. En este contexto, la Comisión apoya con financiación de la UE la puesta en marcha de un proyecto piloto por un grupo de cinco Estados miembros para establecer mecanismos que permitan realizar búsquedas transfronterizas

automatizadas en los índices nacionales mediante un sistema de respuesta positiva o negativa[25]. La Comisión tendrá en cuenta en su evaluación los resultados del proyecto.

Acciones para desarrollar sistemas de información adicional y para subsanar las lagunas en materia de información

Sistema de Entradas y Salidas (SES)

- El Parlamento Europeo y el Consejo deberán tratar las propuestas legislativas sobre el SES con carácter prioritario, con el fin de adoptar las propuestas como muy tarde a finales de 2016.

Registros de nombres de los pasajeros (PNR)

- El Parlamento Europeo y el Consejo deberán adoptar la Directiva PNR como muy tarde en abril de 2016.
- Una vez adoptada, los Estados miembros deberán aplicar la Directiva PNR con carácter de urgencia.
- La Comisión deberá apoyar el intercambio de datos entre las Unidades de Información sobre Pasajeros a través de procedimientos y soluciones normalizadas.
- La Comisión deberá elaborar un proyecto de Decisión de ejecución relativa a protocolos comunes y formatos de datos admitidos para la transferencia de datos PNR por las compañías aéreas a las UIP en el plazo de tres meses después de la adopción de la Directiva PNR.

Falta de información previa a la llegada de nacionales de terceros países no sujetos a la obligación de visado

- La Comisión deberá evaluar en 2016 la necesidad, la viabilidad técnica y la proporcionalidad de crear un nuevo instrumento de la UE, como un Sistema de autorización e información sobre viajes de la UE.

Sistema Europeo de Índice de Ficheros Policiales (EPRIS)

- La Comisión deberá evaluar en 2016 la necesidad, la viabilidad técnica y la proporcionalidad de establecer un EPRIS.

7. HACIA LA INTEROPERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN

La interoperabilidad es la capacidad de los sistemas de información para intercambiar datos y permitir la puesta en común de la información. Pueden distinguirse **cuatro dimensiones de interoperabilidad**, que plantean cada una cuestiones jurídicas[26], técnicas y operativas, en particular en materia de protección de datos:

- una interfaz única de búsqueda para consultar varios sistemas de información simultáneamente y obtener resultados combinados en una sola pantalla;

[25] El proyecto piloto sobre proceso de intercambio de datos automatizado (PIDA) tiene por objetivo crear un sistema técnico que permita, mediante un índice, ver si existen expedientes policiales sobre una persona o una investigación policial penal en uno o varios Estados miembros. La respuesta automatizada a una consulta en el índice revelaría únicamente si se dispone o no de datos; sería una respuesta positiva o negativa. Otros datos personales deberían solicitarse en una segunda fase, en caso de una respuesta positiva, a través de los canales habituales de cooperación policial.

[26] Con sujeción a las disposiciones específicas del Protocolo n.º 22 por lo que respecta a Dinamarca, y los Protocolos n.º 21 y 36 por lo que respecta al Reino Unido e Irlanda.

- la interconectividad de los sistemas de información cuando los datos registrados en un sistema sean consultados automáticamente por otro sistema;
- el establecimiento de un servicio de correspondencia biométrica compartido que soporte a varios sistemas de información;
- un depósito común de datos para distintos sistemas de información (módulo central).

Con el fin de iniciar un proceso hacia la interoperabilidad de los sistemas de información a escala de la UE, la Comisión creará un **grupo de expertos sobre sistemas de información e interoperabilidad** a nivel de altos funcionarios con las agencias de la UE, expertos nacionales y distintos actores institucionales. El grupo de expertos estará encargado de abordar los aspectos jurídicos, técnicos y operativos de las diferentes opciones para lograr la interoperabilidad de los sistemas de información, incluida la necesidad, la viabilidad técnica y la proporcionalidad de todas las opciones disponibles y sus implicaciones para la protección de datos. También deberá abordar las actuales deficiencias y lagunas de conocimiento causadas por la complejidad y la fragmentación de los sistemas de información a escala europea. El grupo de expertos adoptará una perspectiva amplia y global en materia de gestión de las fronteras y actuación policial, teniendo en cuenta asimismo las funciones, responsabilidades y sistemas de las autoridades aduaneras a este respecto. El método de trabajo del grupo tendrá por objeto la sinergia de todas las experiencias pertinentes, que en el pasado estaban demasiado a menudo compartimentadas.

El objetivo de este proceso es ofrecer una visión estratégica general de la arquitectura de la UE de gestión de datos para el control fronterizo y la seguridad, así como aportar soluciones para su aplicación.

Este proceso de consulta **se guiará por los siguientes objetivos**:

- Los sistemas de información deben ser complementarios. Deben evitarse los solapamientos y las superposiciones existentes deben eliminarse. Las lagunas se abordarán de manera apropiada.
- Deberá adoptarse un enfoque modular, haciendo pleno uso de la tecnología y sobre la base de los principios de protección de la privacidad desde el diseño.
- Deberá garantizarse el pleno respeto de todos los derechos fundamentales de los ciudadanos de la UE y los nacionales de terceros países desde el comienzo, en consonancia con la Carta de los Derechos Fundamentales.
- Cuando sea necesario y factible, los sistemas de información deberán estar interconectados y ser interoperables. Deberán facilitarse las búsquedas simultáneas en los sistemas, para garantizar que toda la información pertinente esté a disposición de los agentes de la guardia de fronteras o los agentes de policía cuando y donde sea necesario para la ejecución de sus tareas respectivas, sin modificar los derechos de acceso existentes.

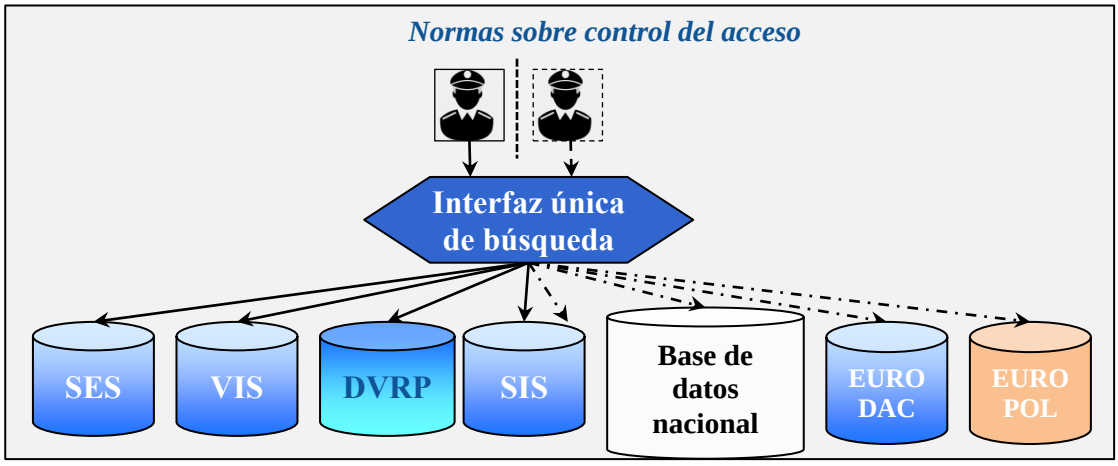
1. Interfaz única de búsqueda

La primera dimensión de la interoperabilidad es la **capacidad,** para la guardia de fronteras o los agentes de policía, **de buscar en varios sistemas de información simultáneamente, y obtener resultados combinados en una única pantalla**, con pleno respeto de sus derechos de acceso, en consonancia con los respectivos objetivos. Ello requiere plataformas con una interfaz única de búsqueda que puedan consultar los sistemas de información simultáneamente con una sola consulta. Por ejemplo, al leer el chip de un documento de viaje o utilizando datos biométricos, esta plataforma podría consultar varias bases de datos diferentes al mismo tiempo. El enfoque del método de búsqueda único se aplica a todas las autoridades que necesiten acceder a los datos y

utilizarlos (es decir, guardias de fronteras, autoridades policiales y servicios de asilo) en consonancia con la limitación de la finalidad y unas normas estrictas sobre control del acceso. También pueden utilizarse con equipos móviles. El establecimiento de una interfaz única de búsqueda permite reducir la complejidad de los sistemas de información a nivel europeo, ya que permite a los agentes de la guardia de fronteras y a los agentes de policía consultar varios sistemas de información simultáneamente a través de un único procedimiento, y de conformidad con sus derechos de acceso.

Varios Estados miembros ya han instalado dichas plataformas con una interfaz única de búsqueda. Sobre esta base de esta buena práctica existente, la Comisión, junto con eu-LISA, colaborarán para establecer una solución estándar para una interfaz única de búsqueda. Los Estados miembros deberán utilizar la financiación de la UE al amparo de su programa nacional del Fondo de Seguridad Interior para financiar la instalación de esta funcionalidad. La Comisión seguirá de cerca el modo en que los Estados miembros hagan uso de la funcionalidad de una interfaz única de búsqueda a nivel nacional.

Gráfico 2 *Interfaz única de búsqueda*



Buscar en sistemas nacionales o centralizados múltiples (según se muestra en el gráfico) es más sencillo que buscar en sistemas descentralizados. La Comisión y eu-LISA estudiarán si también se puede utilizarse una interfaz única de búsqueda para realizar búsquedas simultáneas de una vez en sistemas descentralizados como Prüm y ECRIS. La Comisión y eu-LISA realizarán este análisis junto con el grupo de expertos sobre sistemas de información e interoperabilidad, sin modificar los derechos de acceso existentes.

2. Interconectividad de los sistemas de información

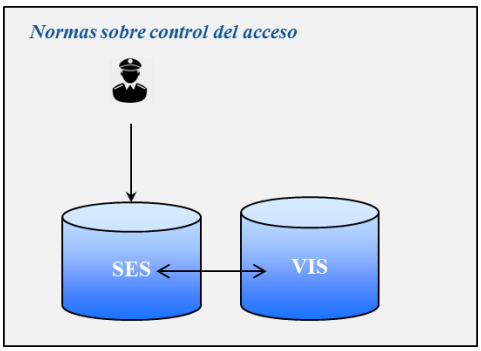
Una segunda dimensión de la interoperabilidad es la interconectividad de los sistemas de información. Esto significa que los distintos sistemas o bases de datos son capaces de «hablar entre sí» desde el punto de vista técnico. **Los datos registrados en un sistema pueden ser consultados automáticamente por otro sistema a nivel central.** Ello exige la compatibilidad técnica entre los sistemas y que los elementos de los datos almacenados en dichos sistemas (por ejemplo, impresiones dactilares) sean interoperativos. La interconectividad permite reducir la cantidad de datos que circulan por las redes de comunicación y que transitan a través de los sistemas nacionales.

La interconectividad requiere unas salvaguardias adecuadas en cuanto a la protección de datos y unas normas estrictas sobre el control del acceso. El acuerdo político alcanzado por los colegisladores en diciembre de 2015 sobre la reforma de la protección de datos

establecerá un marco moderno en materia de protección de datos en toda la UE que incluirá estas salvaguardias. Es importante que los colegisladores adopten sin demora el Reglamento general de protección de datos y la Directiva sobre protección de datos.

El concepto de interconectividad está incardinado en el futuro SES. Este sistema será capaz de comunicarse directamente con el VIS a nivel central y viceversa. Se trata de un paso importante para afrontar la fragmentación actual en la arquitectura de gestión de datos de la UE para el control fronterizo y la seguridad, así como los problemas conexos. El cotejo automatizado eximirá a los Estados miembros de la necesidad de consultar el VIS en los controles fronterizos, reducirá los requisitos de mantenimiento y mejorará el rendimiento del sistema.

Gráfico 3 *Interconectividad de los sistemas: el ejemplo del SES/VIS*



Como paso siguiente, la Comisión y eu-LISA analizarán si la interconectividad a nivel central entre el futuro SES y el VIS puede ampliarse al SIS, y si puede establecerse la interconectividad entre EURODAC y el SIS. La Comisión y eu-LISA efectuarán este análisis junto con el grupo de expertos sobre sistemas de información e interoperabilidad.

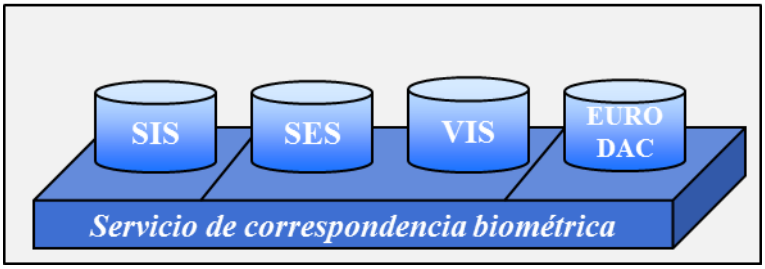
3. Servicio compartido de correspondencia biométrica

Una tercera dimensión de la interoperabilidad se halla en el ámbito de los identificadores biométricos. Por ejemplo, cuando se toman las impresiones dactilares en el consulado de un Estado miembro con equipos específicos, es sumamente importante que estas impresiones puedan cotejarse a través de VIS en un puesto fronterizo de otro Estado miembro, utilizando equipos de otro tipo. El mismo requisito se aplica a las consultas de impresiones dactilares en otros sistemas: las muestras biométricas deben cumplir unos requisitos mínimos de formato y calidad para lograr este tipo de interoperabilidad sin dificultad.

Al nivel del sistema, la interoperabilidad de los identificadores biométricos permite utilizar un servicio compartido de correspondencia biométrica para varios sistemas de información, respetando las normas de protección de los datos personales mediante la compartimentación de los datos, con normas de control del acceso distintas para cada categoría de datos[27]. Tales servicios compartidos generan importantes beneficios financieros, operativos y de mantenimiento.

[27] Comparable a compartir un servidor de archivos físico con una multitud de usuarios, cada uno de los cuales dispone de derechos de acceso específicos solo a ciertas carpetas.

Gráfico 4 *Servicio compartido de correspondencia biométrica*



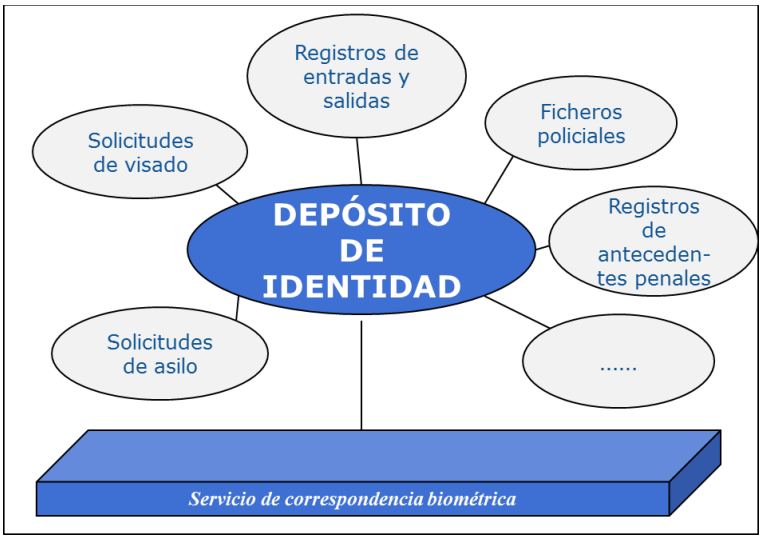
La Comisión y eu-LISA analizarán si es necesario y técnicamente viable crear un servicio compartido de correspondencia biométrica para todos los sistemas de información pertinentes. La Comisión y eu-LISA efectuarán este análisis junto con el grupo de expertos sobre sistemas de información e interoperabilidad.

4. Depósito común de datos

El enfoque más ambicioso a largo plazo de la interoperabilidad sería un **depósito común de datos a nivel de la UE para los distintos sistemas de información**. El depósito común constituiría un módulo central con los datos básicos (alfanuméricos y biométricos), mientras que otros elementos de datos y características específicas de los distintos sistemas de información (por ejemplo, datos sobre visados) se almacenarían en módulos específicos. El módulo central y los módulos específicos estarían conectados entre sí para vincular los respectivos conjuntos de datos. Esto crearía una **gestión de la identidad modular e integrada para las fronteras y la seguridad**. El cumplimiento de las normas de protección de datos tendría que garantizarse, por ejemplo, compartimentando los datos, con normas sobre control del acceso distintas para cada categoría de datos.

La creación de un depósito común de datos resolvería la fragmentación actual de la arquitectura de la UE de gestión de datos para el control de las fronteras y la seguridad. Esta fragmentación es contraria al principio de minimización de datos, ya que da lugar a que los mismos datos se almacenen varias veces. En caso necesario, el depósito común permitiría el reconocimiento de las conexiones y proporcionaría una visión global mediante la combinación de elementos específicos de los datos almacenados en los diferentes sistemas de información. Por tanto, resolvería las actuales deficiencias de conocimiento y arrojaría luz sobre los puntos ciegos para la guardia de fronteras y los agentes de policía.

Gráfico 5 *Depósito común de datos*



La opción de crear un depósito común de datos a nivel de la UE plantea importantes cuestiones de definición de la finalidad, la necesidad, la viabilidad técnica y la proporcionalidad del tratamiento de los datos en cuestión. Requeriría una revisión completa del marco jurídico que establece los diferentes sistemas de información y sería un objetivo que solo podría lograrse a largo plazo. El grupo de expertos sobre sistemas de información e interoperabilidad abordará las cuestiones jurídicas, técnicas y operativas vinculadas a un depósito común de datos, así como las cuestiones relativas a la protección de datos.

Para las cuatro dimensiones de la interoperabilidad mencionadas anteriormente (interfaz única de búsqueda, interconectividad de los sistemas, servicio compartido de correspondencia biométrica y depósito común de datos), es necesario que los datos almacenados en los distintos sistemas de información o módulos sean compatibles. Para conseguirlo, es importante avanzar en el ámbito del **Formato Uniforme de Mensajes** (FUM) con el fin de crear una norma común para todos los sistemas de información pertinentes[28].

Medidas para lograr la interoperabilidad de los sistemas de información

- La Comisión deberá establecer un **grupo de expertos sobre sistemas de información e interoperabilidad** con las agencias de la UE, los Estados miembros y las partes interesadas pertinentes para analizar los aspectos jurídicos, técnicos y operativos de la mejora de la interoperabilidad de los sistemas de información, incluida la necesidad, la viabilidad técnica y la proporcionalidad de todas las opciones disponibles y sus implicaciones para la protección de datos.

[28] La Comisión ha apoyado el desarrollo del FUM en la Comunicación de 2012 sobre el Modelo Europeo para el Intercambio de Información (EIXM), y actualmente está financiando el tercer proyecto piloto del FUM, con el objetivo de crear una norma común para todas las bases de datos pertinentes que pueda utilizarse a escala nacional (Estados miembros), a escala de la UE (sistemas centrales y Agencias) y a escala internacional (Interpol).

Interfaz única de búsqueda

- La Comisión y eu-LISA apoyarán a los Estados miembros en la instalación de una interfaz única de búsqueda para consultar los sistemas centrales.
- La Comisión y eu-LISA estudiarán, junto con el grupo de expertos, si la interfaz única de búsqueda puede utilizarse para realizar búsquedas simultáneas de una sola vez en todos los sistemas pertinentes sin modificar los actuales derechos de acceso.

Interconectividad de los sistemas de información

- La Comisión y eu-LISA analizarán, junto con el grupo de expertos, si puede ampliarse la interconectividad entre los sistemas de información centralizados, más allá de la interconectividad ya propuesta entre el Sistema de Entradas y Salidas y el Sistema de Información de Visados.

Servicio de correspondencia biométrica

- La Comisión y eu-LISA analizarán, junto con el grupo de expertos, la necesidad y la viabilidad técnica de establecer un servicio compartido de correspondencia biométrica para todos los sistemas de información pertinentes.

Depósito común de datos (módulo central)

- La Comisión y eu-LISA estudiarán, junto con el grupo de expertos, las implicaciones jurídicas, técnicas, operativas y financieras del desarrollo a más largo plazo de un depósito común de datos.
- La Comisión y eu-LISA participarán en los trabajos en curso sobre un Formato Uniforme de Mensajes para todos los sistemas de información pertinentes.

8. CONCLUSIÓN

La presente Comunicación abre un debate sobre la manera en que los sistemas de información de la UE pueden reforzar la seguridad interior y la gestión de las fronteras, sobre la base de las importantes sinergias entre las Agendas europeas sobre Seguridad y Migración. Diversos sistemas de información ya proporcionan a la guardia de fronteras y a la policía información pertinente, pero estos sistemas no son perfectos. La UE se enfrenta al desafío de crear una arquitectura de gestión de datos más sólida e inteligente, respetando plenamente los derechos fundamentales, en particular la protección de los datos personales y el principio de limitación de la finalidad.

En los casos en que existen lagunas en la arquitectura de la UE de gestión de datos, estas deben abordarse. Junto con esta Comunicación, la Comisión ha presentado una propuesta relativa a un Sistema de Entradas y Salidas que debería adoptarse con carácter de urgencia. La Directiva relativa al registro de nombres de los pasajeros también debería adoptarse en las próximas semanas. La propuesta sobre la Guardia Europea de Fronteras y Costas debería adoptarse antes del verano. Paralelamente, la Comisión seguirá trabajando en el refuerzo y, en caso necesario, la modernización de los sistemas existentes, por ejemplo desarrollando una funcionalidad de Sistema Automático de Identificación Dactilar para el Sistema de Información de Schengen.

Los Estados miembros deben hacer pleno uso de los sistemas de información existentes y establecer las conexiones técnicas necesarias con todos los sistemas de información y bases de datos, en consonancia con sus obligaciones jurídicas. Las deficiencias existentes, en particular en el marco de Prüm, deben solventarse sin demora. Si bien la presente Comunicación abre un debate e inicia un proceso para abordar sistemáticamente las lagunas y deficiencias, corresponde a los Estados miembros atender urgentemente a

las deficiencias persistentes en la alimentación de las bases de datos de la UE y el intercambio de información en toda la Unión.

A fin de mejorar estructuralmente la arquitectura de la UE de gestión de datos para el control de las fronteras y la seguridad, la presente Comunicación pone en marcha un proceso para lograr la interoperabilidad de los sistemas de información. La Comisión creará un grupo de expertos sobre sistemas de información e interoperabilidad para abordar las modalidades jurídicas, técnicas y operativas de las opciones para lograr la interoperabilidad de los sistemas de información y abordar las carencias y lagunas. A raíz de las conclusiones del grupo de expertos, la Comisión Europea presentará nuevas ideas concretas al Parlamento Europeo y al Consejo como base para un debate conjunto sobre el camino a seguir. Asimismo, la Comisión pedirá la aportación del Supervisor Europeo de Protección de Datos y de las autoridades nacionales de protección de datos, reunidas en el Grupo de Trabajo del artículo 29.

El objetivo debe ser desarrollar una estrategia común para hacer más eficaz y eficiente la gestión de datos en la UE, respetando plenamente los requisitos de protección de datos, a fin de proteger mejor sus fronteras exteriores y reforzar su seguridad interior, en beneficio de todos los ciudadanos.

ANEXO 1: ABREVIATURAS

API	Información anticipada sobre los pasajeros
SAID	Sistema Automático de Identificación Dactilar: sistema capaz de capturar, almacenar, comparar y comprobar las impresiones dactilares
SIA	Sistema de Información Aduanero
ECRIS	Sistema Europeo de Información de Antecedentes Penales
SES	Sistema de Entradas y Salidas (propuesto)
EIXM	Modelo Europeo para el Intercambio de Información
SIE	Sistema de información de Europol
EPRIS	Sistema Europeo de Índice de Ficheros Policiales
EURODAC	Sistema europeo para la comparación de las impresiones dactilares
EUROPOL	Oficina Europea de Policía
SAIV	(posible) Sistema de autorización e información sobre viajes de la UE
eu-LISA	Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia
BFRI	Base de datos fija en red de Interpol
FRONTEX	Agencia Europea para la Gestión de la Cooperación Operativa en las Fronteras Exteriores de los Estados Miembros de la Unión Europea
iARMS	Sistema de INTERPOL para la Gestión de los Registros y el Rastreo de Armas Ilícitas
INTERPOL	Organización Internacional de Policía Criminal
BMRI	Base de datos móvil en red de Interpol
UIP	Unidad de Información sobre Pasajeros: unidad que se creará en cada Estado miembro para recibir los datos del PNR de las compañías aéreas
PNR	Registro de nombres de los pasajeros
Prüm	Mecanismo de cooperación policial para intercambiar información sobre perfiles de ADN, impresiones dactilares y datos de matriculación de vehículos
SafeSeaNet	Plataforma europea para el intercambio de información marítima entre las autoridades marítimas de los Estados miembros
CFS	Código de fronteras Schengen
SIENA	Aplicación de la Red de Intercambio Seguro de Información
SIS	Sistema de Información de Schengen (a veces denominado de 2ª generación - SIS II)
DVRP	Base de datos de Interpol sobre documentos de viaje robados y perdidos
sTESTA	Servicios transeuropeos seguros de telemática entre administraciones [se actualizará a TESTA-NG (próxima generación)]
FUM	Formato Uniforme de Mensajes: formato de los mensajes que permite la compatibilidad entre los distintos sistemas de información
VIS	Sistema de Información de Visados

DMV	Datos de Matriculación de Vehículos

ANEXO 2: INVENTARIO DE LOS SISTEMAS DE INFORMACIÓN EXISTENTES PARA LA GESTIÓN DE LAS FRONTERAS Y LOS SERVICIOS POLICIALES

1. Sistema de Información de Schengen (SIS)

El SIS es la plataforma de intercambio de información sobre migración y servicios policiales más grande y más ampliamente utilizada. Se trata de un sistema centralizado, utilizado por 25 Estados miembros de la UE[29] y cuatro países asociados a Schengen[30], que contiene en la actualidad 63 millones de descripciones. Estas son introducidas y consultadas por las autoridades competentes, como la policía y los servicios de control fronterizo e inmigración. Incluye un registro de nacionales de terceros países a los que se prohíbe entrar o permanecer en el espacio Schengen, así como de nacionales de la UE y de terceros países que están buscados o desaparecidos (incluidos menores) y de objetos buscados (vehículos, armas de fuego, documentos de identidad, equipos industriales, etc.). La característica distintiva del SIS en comparación con otros instrumentos de intercambio de información es que su información se complementa con una instrucción para que los agentes que trabajan sobre el terreno tomen medidas concretas, como la detención o incautación.

Las comprobaciones en el SIS son obligatorias a efectos de la tramitación de visados para estancias de corta duración, para el control fronterizo de nacionales de terceros países y, de forma no sistemática[31], para los ciudadanos de la UE y otras personas que disfrutan del derecho a la libre circulación. Además, cada control policial en el territorio debe incluir un control automático en el SIS.

2. Sistema de Información de Visados (VIS)

El VIS es un sistema centralizado para el intercambio de datos entre los Estados miembros sobre visados para estancias de corta duración. Trata los datos y las decisiones relativas a las solicitudes de visados para estancias de corta duración para visitar o transitar por el espacio Schengen. Todos los consulados de los Estados Schengen (alrededor de 2 000) y todos sus pasos fronterizos exteriores (unos 1 800 en total) se han conectado al sistema.

El VIS contiene datos sobre las solicitudes de visado y las decisiones, así como sobre si los visados expedidos han sido anulados, revocados o ampliados. Actualmente contiene datos sobre 20 millones de solicitudes de visados, y en horas punta maneja más de 50 000 transacciones por hora. Cada solicitante de visado proporciona información biográfica detallada, una fotografía digital y diez impresiones dactilares. De esta forma, es un medio fiable para verificar la identidad de los solicitantes de visado, para evaluar los posibles casos de migración irregular y riegos para la seguridad, y para prevenir la búsqueda de visados de conveniencia.

En los pasos fronterizos o en el territorio de los Estados miembros, el VIS se utiliza para verificar la identidad de los titulares de visados, comparando sus impresiones dactilares con las impresiones dactilares almacenadas en dicho sistema. Este procedimiento garantiza que la persona que solicitó el visado es la misma que cruza la frontera. Una búsqueda de impresiones dactilares en el VIS también permite identificar a una persona

[29] Todos, excepto Irlanda, Chipre y Croacia.
[30] Islandia, Liechtenstein, Noruega y Suiza.
[31] Esta norma es susceptible de modificarse según lo previsto por la propuesta de la Comisión COM/2015/0670 sobre la modificación del Código de fronteras Schengen.

que haya solicitado un visado en los últimos cinco años y que pueda no llevar documentos de identidad.

3. EURODAC

EURODAC (European Dactyloscopy - sistema europeo para la comparación de impresiones dactilares) contiene las impresiones dactilares de los solicitantes de asilo y los nacionales de terceros países que cruzan ilegalmente las fronteras exteriores de Schengen. Su finalidad principal actualmente es determinar qué país de la UE es responsable de la tramitación de una solicitud de asilo, de acuerdo con el Reglamento de Dublín. Está disponible en los pasos fronterizos, pero a diferencia del SIS y del VIS, no es un sistema de gestión de fronteras.

Las impresiones dactilares de los migrantes irregulares que entran en la UE ilegalmente se toman en los pasos fronterizos y se almacenan en EURODAC para verificar la identidad de la persona en caso de una futura solicitud de asilo. Las autoridades de migración y la policía también pueden comparar las impresiones dactilares de los migrantes irregulares detectados en los Estados miembros de la UE con el fin de comprobar si han solicitado asilo en otro Estado miembro. Las autoridades policiales y Europol también tienen derecho a consultar EURODAC con el fin de prevenir, detectar o investigar un delito grave o un delito de terrorismo.

El registro de las impresiones dactilares de los solicitantes de asilo y los migrantes irregulares en un sistema centralizado permite la identificación y el seguimiento de sus movimientos secundarios[32] dentro de la UE, hasta que se presente una solicitud de protección internacional o se dicte una decisión de retorno (en el futuro, con la correspondiente descripción en el SIS). De manera más general, la identificación y el control de los migrantes irregulares son necesarios para garantizar la redocumentación por las autoridades en sus países de origen y facilitar así su retorno.

4. Documentos de viaje robados y perdidos (DVRP)

La base de datos de Interpol sobre documentos de viaje robados y perdidos (DVRP) es una base de datos central de pasaportes y otros documentos de viaje cuyo robo o pérdida hayan sido notificados a Interpol por las autoridades expedidoras. Incluye información sobre pasaportes en blanco robados. Los documentos de viaje declarados robados o perdidos a las autoridades de los países que participan en el SIS se registran tanto en la base de datos DVRP como en el SIS. La base de datos DVRP también incluye datos sobre documentos de viaje registrados por países que no participan en el SIS (Irlanda, Croacia, Chipre y terceros países).

Tal como se recoge en las Conclusiones del Consejo de 9 y 20 de noviembre de 2015, y en la Propuesta de la Comisión de 15 de diciembre de 2015 para la adopción de un Reglamento por el que se modifica el Código de fronteras Schengen[33], los documentos de viaje de todos los nacionales de terceros países y las personas que disfrutan del derecho de libre circulación deberán cotejarse con base de datos. Todos los puestos de control fronterizos deberán estar conectados a la base de datos sobre DVRP. Además de esto, las búsquedas policiales nacionales en la base de datos sobre DVRP generarían beneficios de seguridad adicionales.

---

[32] Por ejemplo, los refugiados que llegan a Grecia sin intención de presentar una solicitud de asilo en Grecia, sino de viajar a otros Estados miembros por tierra.

[33] COM(2015) 670 final Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (CE) n.º 562/2006 en lo relativo al refuerzo de los controles mediante la consulta de bases de datos pertinentes en las fronteras exteriores.

5. Información anticipada sobre los pasajeros (API)

El objetivo de la API es recopilar información sobre la identidad de una persona antes de que embarque en un vuelo con destino a la UE, así como identificar a los migrantes irregulares a su llegada. Los datos API comprenden la información contenida en un documento de viaje, y consisten en el nombre completo del pasajero, la fecha de nacimiento, la nacionalidad, el número y tipo de documento de viaje, así como información sobre el paso fronterizo de salida y entrada y detalles del transporte. Los datos API relacionados con el pasajero suelen recogerse en el momento de la facturación.

La información previa relativa al transporte por mar ha de transmitirse de conformidad con el Convenio para facilitar el tráfico marítimo internacional, 24 horas antes de la llegada prevista del buque. La Directiva 2010/65/UE[34] prevé un sistema de transmisión electrónica de los datos a través de una ventanilla única que conecta entre sí a SafeSeaNet, e-Customs y otros sistemas electrónicos.

No existe ningún sistema central de la UE para registrar los datos API.

6. Sistemas de información de Europol

El sistema de información de Europol (SIE) es una base de datos centralizada de información criminal para fines de investigación. Puede ser utilizada por los Estados miembros y Europol para almacenar y consultar datos relativos a la delincuencia grave y el terrorismo. La información almacenada en el SIE son datos relativos a personas, documentos de identidad, vehículos, armas de fuego, números de teléfono, direcciones de correo electrónico, impresiones dactilares, ADN e información relacionada con la ciberdelincuencia, que puede vincularse entre sí de diversas maneras a fin de crear una imagen más detallada y estructurada de un caso de delincuencia. El SIE apoya la cooperación policial y no está disponible para las autoridades de control fronterizo.

El intercambio de información se realiza utilizando la plataforma SIENA[35], que es una red de comunicaciones electrónicas segura entre Europol, las oficinas de enlace y las unidades nacionales de Europol, las autoridades competentes designadas (como las aduanas, los organismos de recuperación de activos, etc.) y terceras partes conectadas.

En mayo de 2017 entrará en vigor un nuevo marco jurídico para Europol. Este marco permitirá un refuerzo de las capacidades operativas de Europol para realizar análisis, así como para identificar mejor los vínculos entre la información disponible.

7. El marco de Prüm

El marco de Prüm se basa en un acuerdo multilateral[36] entre los Estados miembros que permite el intercambio de datos relacionados con el ADN, las impresiones dactilares y la matriculación de vehículos (DMV). Este concepto se basa en la interconexión de un sistema nacional con los sistemas nacionales de todos los demás Estados miembros de la UE, a fin de permitir la búsqueda cruzada remota. Cuando una búsqueda genera un resultado positivo en la base de datos de otros Estados miembros, los detalles del resultado positivo se intercambian a través de mecanismos bilaterales.

---

[34] Directiva 2010/65/UE del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, sobre las formalidades informativas exigibles a los buques a su llegada o salida de los puertos de los Estados miembros y por la que se deroga la Directiva 2002/6/CE.

[35] Aplicación de la Red de Intercambio Seguro de Información.

[36] Tratado de Prüm de 2005. El Tratado se integró en la normativa de la UE en 2008 mediante la Decisión 2008/615/JAI del Consejo.

8. Sistema Europeo de Información de Antecedentes Penales (ECRIS)

El sistema ECRIS es un sistema electrónico de intercambio de información sobre las condenas pronunciadas contra una persona por los tribunales penales en la UE a los efectos de un procedimiento penal y, si así lo permite el Derecho nacional, a otros efectos. El Estado miembro donde se pronuncia la condena de un nacional de otro Estado miembro deberá notificarla al Estado miembro de la nacionalidad. El Estado miembro de la nacionalidad debe almacenar esta información y puede así proporcionar, previa petición, información actualizada sobre los antecedentes penales de sus nacionales con independencia del lugar en el que se hayan pronunciado las condenas.

ECRIS permite asimismo el intercambio de información sobre las condenas de nacionales de terceros países y apátridas. Las autoridades centrales designadas en cada Estado miembro son los puntos de contacto en la red del sistema ECRIS, encargándose de todas las tareas, tales como la notificación, el almacenamiento, la solicitud y la provisión de información sobre antecedentes penales.