COMISIÓN
EUROPEA

Bruselas, 21.12.2016
COM(2016) 882 final

2016/0408 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, que modifica el Reglamento (UE) n.º 515/2014 y que deroga el Reglamento (CE) n.º 1987/2006.

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

A lo largo de los dos últimos años, la Unión Europea ha trabajado para abordar simultáneamente los diferentes retos de la gestión de la migración, la gestión integrada de las fronteras exteriores de la UE y la lucha contra el terrorismo y la delincuencia transfronteriza. Un intercambio de información eficaz entre los Estados miembros y entre los Estados miembros y las agencias pertinentes de la UE es esencial para ofrecer una respuesta contundente a dichos retos y construir una Unión de la Seguridad real y efectiva.

El Sistema de Información de Schengen (SIS) es la mejor herramienta para la cooperación eficaz de las autoridades de inmigración, policiales, aduaneras y judiciales en la UE y en los países asociados de Schengen. Las autoridades competentes de los Estados miembros, como la policía, la guardia de fronteras y los funcionarios de aduanas necesitan tener acceso a información de alta calidad sobre las personas u objetos que controlan, con instrucciones claras sobre lo que debe hacerse en cada caso. Este sistema de información de gran escala constituye el núcleo de la cooperación de Schengen y desempeña un papel fundamental a la hora de facilitar la libre circulación de personas en el espacio Schengen. Asimismo, permite a las autoridades competentes introducir y consultar datos sobre personas buscadas, personas que puedan no tener derecho de entrada o de estancia en la UE, personas desaparecidas, en particular niños, y objetos que puedan haber sido robados, sustraídos o extraviados. El SIS no solo contiene información sobre una persona o un objeto particular, sino también instrucciones claras a las autoridades competentes sobre qué hacer con dicha persona u objeto una vez hallados.

En 2016, la Comisión llevó a cabo una evaluación exhaustiva del SIS[1], tres años después de la entrada en funcionamiento de la segunda generación. Esta evaluación puso de manifiesto que el SIS ha sido un verdadero éxito operativo. En 2015, las autoridades nacionales competentes comprobaron personas y objetos con los datos del SIS en casi 2 900 millones de ocasiones, e intercambiaron más de 1,8 millones de elementos de información complementaria. No obstante, tal como se anunció en el programa de trabajo de la Comisión para 2017, basándose en esta experiencia positiva, la eficacia y la eficiencia del sistema deberían reforzarse. Con este fin, la Comisión presenta un primer paquete de tres propuestas para mejorar y ampliar el uso del SIS como resultado de la evaluación, al tiempo que sigue trabajando para hacer que los sistemas de gestión de las fronteras y policiales actuales y futuros sean más interoperativos, siguiendo los trabajos en curso del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad.

Estas propuestas incluyen el uso del sistema para: a) la gestión de las fronteras; b) la cooperación policial y judicial en materia penal; y c) el retorno de nacionales de terceros países en situación irregular. Las dos primeras propuestas forman conjuntamente la base jurídica para el establecimiento, el funcionamiento y la utilización del SIS. La propuesta sobre la utilización del SIS para el retorno de nacionales de terceros países en situación irregular complementa la propuesta para la gestión de las fronteras y las disposiciones contenidas en

[1] Informe al Parlamento Europeo y al Consejo sobre la evaluación del Sistema de Información de Schengen de segunda generación (SIS II), de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006 y con el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, y un documento de trabajo de los servicios de la Comisión. DO …

ella. Crea un nuevo tipo de descripción y contribuye a la ejecución y el seguimiento de la Directiva 2008/115/CE[2].

Debido a la geometría variable de la participación de los Estados miembros en las políticas de la UE en el ámbito de la libertad, la seguridad y la justicia, es necesario adoptar tres instrumentos jurídicos separados que, sin embargo, operarán conjuntamente sin fisuras para permitir el funcionamiento y la utilización del sistema.

Paralelamente, con vistas a reforzar y mejorar la gestión de la información a nivel de la UE, en abril de 2016 la Comisión puso en marcha un proceso de reflexión sobre «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad»[3] con el objetivo general de garantizar que las autoridades competentes cuenten de manera sistemática con la información necesaria procedente de los distintos sistemas de información. Con el fin de lograr este objetivo, la Comisión ha revisado la actual arquitectura de información para identificar lagunas y fallos resultantes de deficiencias en las funcionalidades de los sistemas existentes, así como de la fragmentación de la arquitectura de gestión de datos de la UE. La Comisión creó un Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad para apoyar esta labor, cuyas conclusiones provisionales también se han tenido en cuenta en esta primera serie de propuestas en relación con las cuestiones de calidad de los datos[4]. El discurso sobre el estado de la Unión del presidente Juncker de septiembre de 2016 también aludió a la importancia de superar las deficiencias actuales en la gestión de la información y de mejorar la interoperabilidad y la interconexión entre los sistemas de información existentes.

A raíz de las conclusiones del susodicho Grupo, que se presentarán en el primer semestre de 2017, la Comisión estudiará la posibilidad de adoptar un segundo conjunto de propuestas a mediados de 2017 para seguir mejorando la interoperabilidad del SIS con otros sistemas de información. La revisión del Reglamento (UE) n.º 1077/2011[5] relativo a la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA) es también un elemento importante de este trabajo y probablemente será objeto de distintas propuestas de la Comisión también en 2017. Invertir en la gestión e intercambio de información cualitativos, eficaces y rápidos, así como garantizar la interoperabilidad de los sistemas de información y bases de datos de la UE es un aspecto importante para hacer frente a los actuales desafíos en materia de seguridad.

El actual marco jurídico del SIS de segunda generación, en lo que respecta a su uso a efectos de las inspecciones fronterizas de los nacionales de terceros países, se basa en un antiguo instrumento del primer pilar, el Reglamento (CE) n.º 1987/2006[6]. La presente propuesta[7] sustituye al actual instrumento jurídico con el fin de:

---

2 Directiva 2008/115/CE del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, relativa a normas y procedimientos comunes en los Estados miembros para el retorno de los nacionales de terceros países en situación irregular, DO L 348 de 24.12.2008, p. 98.

3 COM(2016) 205 final de 6.4.2016.

4 Decisión de la Comisión 2016/C 257/3 de 17.6.2016.

5 Reglamento (UE) n.º 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DO L 286 de 1.11.2011, p. 1.

6 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), DO L 381 de 28.12.2006, p. 4.

7 Véase la sección 2 «Elección del instrumento» donde se explica por qué se optó por una sustitución en lugar de una refundición de la legislación vigente.

- obligar a los Estados miembros a introducir la descripción en el SIS en todos los casos en que se haya emitido una prohibición de entrada a un nacional de un tercer país en situación irregular en virtud de disposiciones conformes a la Directiva 2008/115/CE;
- armonizar los procedimientos nacionales para el uso del SIS con respecto al procedimiento de consulta a fin de evitar que un nacional de un tercer país que esté sujeto a una prohibición de entrada sea titular de un permiso de residencia válido expedido por un Estado miembro;
- introducir modificaciones técnicas para mejorar la seguridad y contribuir a reducir las cargas administrativas;
- abordar el uso completo del SIS, abarcando no solo los sistemas central y nacionales, sino también las necesidades del usuario final, garantizando que este reciba toda la información necesaria para llevar a cabo sus tareas y cumplir todas las normas de seguridad cuando trate datos del SIS.

Las propuestas desarrollan y mejoran el sistema existente, en lugar de crear uno nuevo. La revisión del SIS apoyará y reforzará la actuación de la Unión Europea en sus Agendas europeas de Migración y de Seguridad, y establece:

1) la consolidación de los resultados de los trabajos sobre la aplicación del SIS realizados en los tres últimos años, que suponen modificaciones técnicas en el SIS Central con el fin de ampliar algunas de las actuales categorías de descripciones y aportar nuevas funcionalidades;

2) las recomendaciones de cambios técnicos y de procedimiento, resultantes de una evaluación general del SIS[8];

3) las propuestas de mejoras técnicas del SIS presentadas por los usuarios finales; y

4) los resultados provisionales del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad[9] en lo que se refiere a la calidad de los datos.

Teniendo en cuenta que la presente propuesta está estrechamente vinculada a la propuesta de la Comisión de un Reglamento relativo al establecimiento, funcionamiento y utilización del SIS en los ámbitos de la cooperación policial y judicial en materia penal, una serie de disposiciones son comunes a ambos textos. Entre estas figuran medidas que abordan el uso completo del SIS, abarcando no solo los sistemas central y nacionales, sino también las necesidades del usuario final; medidas reforzadas para garantizar la continuidad de la actividad; medidas sobre la calidad, protección y seguridad de los datos, y disposiciones relativas al seguimiento, evaluación e información. Ambas propuestas amplían también el uso de información biométrica[10].

Con la agravación de la crisis migratoria y de los refugiados en 2015, la necesidad de tomar medidas efectivas para abordar la inmigración irregular aumentó considerablemente. En su

---

8 Informe al Parlamento Europeo y al Consejo sobre la evaluación del Sistema de Información de Schengen de segunda generación (SIS II), de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006 y con el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, y un documento de trabajo de los servicios de la Comisión, DO …

9 Grupo de Expertos de Alto Nivel - Informe del presidente de 21 de diciembre de 2016.

10 Véase la sección 5 «Otros elementos» para una explicación detallada de las modificaciones incluidas en la presente propuesta.

Plan de Acción de la UE en materia de retorno[11], la Comisión anunció que propondría la obligatoriedad de que los Estados miembros introduzcan en el SIS todas las prohibiciones de entrada a fin de contribuir a evitar el regreso al espacio Schengen de los nacionales de terceros países que no estén autorizados a entrar y permanecer en el territorio de los Estados miembros. Las prohibiciones de entrada emitidas en virtud de disposiciones conformes a la Directiva 2008/115/CE tienen efecto en todo el espacio Schengen; por tanto, pueden aplicarse en las fronteras exteriores, también por las autoridades de un Estado miembro distinto del que emitió la prohibición. El Reglamento (CE) n.º 1987/2006 vigente solo permite, pero no exige, a los Estados miembros introducir en el SIS descripciones para la denegación de entrada y estancia basadas en prohibiciones de entrada. Puede lograrse un mayor nivel de eficacia y armonización mediante la obligatoriedad de introducir en el SIS todas las prohibiciones de entrada.

- **Coherencia con las disposiciones vigentes en el ámbito político en cuestión así como con los instrumentos jurídicos existentes y futuros**

La presente propuesta es plenamente coherente y conforme a las disposiciones de la Directiva 2008/115/CE sobre la emisión y la ejecución de las prohibiciones de entrada. Por tanto, complementa las disposiciones existentes sobre prohibiciones de entrada y contribuye a la eficaz aplicación de dichas prohibiciones en la frontera exterior, facilitando la aplicación de las obligaciones establecidas por la Directiva sobre el retorno y previniendo de forma eficaz el regreso al espacio Schengen de los nacionales de terceros países.

- **Coherencia con otras políticas de la Unión**

La presente propuesta complementa y está estrechamente vinculada con otras políticas de la Unión, en particular:

1) **la seguridad interior** en relación con la función del SIS para prevenir la entrada de nacionales de terceros países que suponen amenaza para la seguridad;

2) **la protección de datos** en la medida en que garantiza la protección de los derechos fundamentales de los individuos cuyos datos son tratados en el SIS.

3) La presente propuesta también complementa y está estrechamente relacionada con otras políticas de la Unión, a saber:

4) **la gestión de las fronteras exteriores** en la medida en que ayuda a los Estados miembros a controlar su parte de las fronteras exteriores de la UE y a reforzar la eficacia del sistema de controles en dichas fronteras;

5) una **política de retorno de la UE** eficaz que contribuye y potencia el sistema de la UE para detectar e impedir el regreso de nacionales de terceros países tras su retorno. La presente propuesta ayudará a reducir los incentivos a la migración irregular a la UE, uno de los principales objetivos de la Agenda Europea de Migración[12];

6) la **Guardia Europea de Fronteras y Costas** en lo que respecta a: i) la posibilidad de que el personal de la Agencia realice análisis de riesgos; ii) el acceso al SIS de la unidad central SEIAV de la Agencia a efectos de la propuesta del Sistema Europeo de Información y Autorización de Viajes (SEIAV)[13]; así como iii) la posibilidad de facilitar una interfaz técnica de acceso al SIS a los equipos de la Guardia Europea de Fronteras y Costas, a los equipos de personal implicados en tareas relacionadas con

---

11 COM(2015) 453 final.
12 COM(2015) 240 final.
13 COM(2016) 731 final.

el retorno y a los miembros de los equipos de apoyo a la gestión de la migración, con arreglo a su mandato, que tienen derecho de acceso y consulta de los datos introducidos en el SIS;

7) **Europol**, en la medida en que esta propuesta atribuye a Europol, con arreglo a su mandato, derechos adicionales de acceso y consulta de datos del SIS.

La presente propuesta también complementa y está estrechamente vinculada con la futura legislación de la Unión, en particular:

8) el **Sistema de Entradas y Salidas (SES).** La propuesta tiene por objeto reflejar el enfoque consistente en el uso de una combinación de imagen facial e impresiones dactilares como identificadores biométricos para el funcionamiento del SES;

9) el **SEIAV.** La propuesta tiene en cuenta el SEIAV propuesto, que prevé una rigurosa evaluación de seguridad incluyendo un control en el SIS de los nacionales de terceros países exentos de la obligación de visado que deseen viajar a la UE.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La presente propuesta se articula en torno al artículo 77, apartado 2, letras b) y d), y el artículo 79, apartado 2, letra c), del Tratado de Funcionamiento de la Unión Europea como base jurídica para las disposiciones relativas a la gestión integrada de fronteras y la inmigración ilegal.

• Geometría variable

La presente propuesta desarrolla las disposiciones del acervo de Schengen relativas a las inspecciones fronterizas. Por tanto, es preciso tener en cuenta las siguientes consecuencias en relación con los diversos protocolos y acuerdos con países asociados:

Dinamarca: de conformidad con el artículo 4 del Protocolo n.º 22 sobre la posición de Dinamarca anejo a los Tratados, Dinamarca decidirá, en un plazo de seis meses a partir de que el Consejo haya tomado una decisión sobre el presente Reglamento, si incorpora esta propuesta, que se basa en el acervo de Schengen, en su legislación nacional.

Reino Unido e Irlanda: de conformidad con los artículos 4 y 5 del Protocolo por el que se integra el acervo de Schengen en el marco de la Unión Europea y con la 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 y con la 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, el Reino Unido e Irlanda no participan en el Reglamento (UE) 2016/399 (Código de fronteras Schengen) ni en ningún otro de los instrumentos jurídicos que se conocen comúnmente como «acervo de Schengen», es decir, los instrumentos jurídicos que organizan y justifican la supresión de los controles en las fronteras interiores y las medidas de acompañamiento relativas a los controles en las fronteras exteriores. El presente Reglamento constituye un acto de desarrollo de dicho acervo, y por consiguiente, el Reino Unido e Irlanda no participarán en su adopción y no quedarán vinculados por él ni sujetos a su aplicación.

Bulgaria y Rumanía: el presente Reglamento constituye un acto que desarrolla o está relacionado con el acervo de Schengen en el sentido del artículo 4, apartado 2, del Acta de adhesión de 2005. El presente Reglamento debe leerse en relación con la Decisión del

Consejo de 29 de junio de 2010[14], que hace aplicable, con algunas restricciones, las disposiciones del acervo de Schengen relativas al Sistema de Información de Schengen en la República de Bulgaria y en Rumanía.

Chipre y Croacia: el presente Reglamento constituye un acto que desarrolla o está relacionado con el acervo de Schengen en el sentido, respectivamente, del artículo 3, apartado 2, del Acta de adhesión de 2003 y del artículo 4, apartado 2, del Acta de adhesión de 2011.

Países asociados: sobre la base de los respectivos acuerdos de asociación de estos países a la ejecución, aplicación y desarrollo del acervo de Schengen, Islandia, Noruega, Suiza y Liechtenstein estarán vinculados por el Reglamento propuesto.

- **Subsidiariedad**

La presente propuesta desarrollará y utilizará como base el actual SIS, que está operativo desde 1995. El marco intergubernamental original fue sustituido por instrumentos de la Unión el 9 de abril de 2013 [Reglamento (CE) n.º 1987/2006 y Decisión 2007/533/JAI del Consejo]. En anteriores ocasiones se ha realizado un análisis de subsidiariedad completo; esta iniciativa aspira a mejorar las disposiciones existentes, abordando las lagunas detectadas y mejorando los procedimientos operativos.

Este considerable nivel de intercambio de información entre los Estados miembros no puede alcanzarse con soluciones descentralizadas. En razón de la escala, los efectos y los impactos de la acción, esta propuesta puede ejecutarse mejor a nivel de la Unión.

Los objetivos de la presente propuesta abarcan, entre otras cosas, mejoras técnicas para aumentar la eficacia del SIS, así como esfuerzos para armonizar el uso del sistema en todos los Estados miembros participantes. Debido a la naturaleza transnacional de estos objetivos y de los retos para garantizar un intercambio de información eficaz para contrarrestar unas amenazas cada vez más diversificadas, la UE se encuentra en una posición favorable para proponer soluciones a estos problemas, que no puedan ser alcanzadas de manera suficiente por los Estados miembros por sí solos.

Si no se subsanan las limitaciones existentes del SIS, existe el riesgo de perder numerosas oportunidades para maximizar la eficiencia y el valor añadido de la UE y de que existan ángulos muertos que obstaculicen la labor de las autoridades competentes. Por ejemplo, la falta de normas armonizadas sobre la supresión de descripciones redundantes en el sistema puede conducir a que se obstaculice la libre circulación de las personas como principio fundamental de la Unión.

- **Proporcionalidad**

El artículo 5 del Tratado de la Unión Europea dispone que la acción de la Unión no deberá exceder de lo necesario para alcanzar los objetivos del Tratado. La forma escogida para esta intervención de la UE debe permitir que la propuesta alcance su objetivo y se aplique con la mayor eficacia posible. La iniciativa propuesta constituye una revisión del SIS en relación a las inspecciones fronterizas.

---

[14] Decisión 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.

La propuesta responde a los principios de *protección de la intimidad desde el diseño*. En cuanto al derecho a la protección de los datos personales, la presente propuesta es proporcionada, ya que establece normas específicas de supresión de descripciones y no exige la recopilación y el almacenamiento de datos durante más tiempo del absolutamente necesario para que el sistema funcione y cumpla sus objetivos. Las descripciones del SIS contienen tan solo los datos necesarios para identificar y localizar a una persona o un objeto y permitir tomar medidas adecuadas. Todos los demás detalles adicionales se proporcionan a través de las Oficinas SIRENE, lo que permite el intercambio de información complementaria.

Además, la propuesta prevé la aplicación de todas las salvaguardas y mecanismos necesarios para la protección efectiva de los derechos fundamentales de los interesados, en particular, la protección de su vida privada y sus datos personales. También incluye disposiciones destinadas específicamente a reforzar la protección de los datos personales en el SIS.

No serán necesarios procesos o medidas de armonización ulteriores a escala de la UE para que el sistema funcione. La medida prevista es proporcionada, en el sentido de que no va más allá de lo necesario en términos de acción a escala de la UE para alcanzar los objetivos definidos.

- **Elección del instrumento**

La revisión propuesta también adoptará la forma de Reglamento y sustituirá al Reglamento (CE) n.º 1987/2006. Este enfoque se ha seguido asimismo en relación con la Decisión 2007/533/JAI del Consejo, y dado que ambos instrumentos están intrínsecamente relacionados, debe aplicarse también en relación con el Reglamento (CE) n.º 1987/2006. La Decisión 2007/533/JAI se adoptó como un «instrumento del tercer pilar» en el marco del antiguo Tratado de la Unión Europea. Estos instrumentos «del tercer pilar» fueron adoptados por el Consejo sin el Parlamento Europeo como colegislador. La base jurídica de la presente propuesta es el Tratado de Funcionamiento de la Unión Europea (TFUE), dado que la estructura de pilares dejó de existir con la entrada en vigor del Tratado de Lisboa, el 1 de diciembre de 2009. La base jurídica exige la utilización del procedimiento legislativo ordinario. Debe elegirse la forma de Reglamento (del Parlamento Europeo y del Consejo), ya que las disposiciones serán vinculantes y directamente aplicables en todos los Estados miembros.

La propuesta completará y perfeccionará un sistema centralizado mediante el cual los Estados miembros cooperan entre sí, lo que requiere una arquitectura y normas de funcionamiento comunes vinculantes. Además, establece normas obligatorias sobre el acceso al sistema, en particular con fines policiales, que son comunes para todos los Estados miembros, así como para la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia[15] (eu-LISA). Desde el 9 de mayo de 2013, eu-LISA es responsable de la gestión operativa del SIS Central, que consiste en todas las tareas necesarias para asegurar el pleno funcionamiento ininterrumpido del SIS. La presente propuesta se basa en las responsabilidades de eu-LISA en relación con el SIS.

Asimismo, la propuesta prevé normas de aplicabilidad directa que permitan el acceso de los interesados a sus propios datos, así como vías de recurso sin necesidad de medidas de aplicación adicionales a este respecto.

---

[15] Establecida mediante el Reglamento (UE) n.º 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DO L 286 de 1.11.2011, p. 1.

Por consiguiente, solo puede elegirse un Reglamento como instrumento jurídico.

3. RESULTADOS DE LAS EVALUACIONES *A POSTERIORI*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Evaluaciones *a posteriori* y control de calidad de la legislación existente**

De conformidad con el Reglamento (CE) n.º 1987/2006 y la Decisión 2007/533/JAI del Consejo[16], tres años después de su entrada en funcionamiento la Comisión llevó a cabo una evaluación del sistema SIS II Central y del intercambio bilateral y multilateral de información complementaria entre los Estados miembros.

La evaluación se dirigió específicamente a la revisión de la aplicación del artículo 24 del Reglamento (CE) n.º 1987/2006, con el objetivo de formular las propuestas necesarias para modificar las disposiciones de este artículo a fin de obtener un mayor nivel de armonización de los criterios para introducir descripciones.

Los resultados de la evaluación pusieron de manifiesto la necesidad de efectuar cambios en la base jurídica del SIS para dar una mejor respuesta a los nuevos retos en materia de seguridad y migración. Esto incluye, por ejemplo, una propuesta sobre la inscripción obligatoria de las prohibiciones de entrada en el SIS para hacer cumplirlas mejor, la consulta obligatoria entre Estados miembros para evitar la coexistencia de una prohibición de entrada y un permiso de residencia, la posibilidad de identificar y localizar a personas a partir de sus impresiones dactilares mediante el uso de un nuevo sistema automatizado de identificación de dichas impresiones, y la ampliación de los identificadores biométricos en el sistema.

Los resultados de la evaluación también pusieron de manifiesto la necesidad de realizar modificaciones legislativas para mejorar el funcionamiento técnico del sistema y para racionalizar los procesos nacionales. Estas medidas mejorarán la eficiencia y eficacia del SIS facilitando su uso y reduciendo cargas innecesarias. Otras medidas están destinadas a mejorar la calidad de los datos y la transparencia del sistema, describiendo más claramente las tareas específicas de información de los Estados miembros y eu-LISA.

Los resultados de la evaluación exhaustiva (el informe de evaluación y el correspondiente documento de trabajo de los servicios se adoptaron el 21 de diciembre de 2016[17]) han constituido la base de las medidas contenidas en la presente propuesta.

Además, de conformidad con el artículo 19 de la Directiva 2008/115/CE sobre el retorno, la Comisión publicó en 2014 una Comunicación sobre la política de retorno de la UE[18], que informa sobre la aplicación de dicha Directiva y concluye que debe reforzarse el potencial del SIS en el ámbito de la política de retorno; indica asimismo que la revisión del SIS II ofrece la oportunidad de mejorar la coherencia entre la política de retorno y el SIS II, y sugiere añadir la obligación de que los Estados miembros introduzcan en el SIS II una descripción de prohibición de entrada para las denegaciones de entrada emitidas con arreglo a la Directiva sobre el retorno.

---

16 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.

17 Informe al Parlamento Europeo y al Consejo sobre la evaluación del Sistema de Información de Schengen de segunda generación (SIS II), de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006 y con el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, y un documento de trabajo de los servicios de la Comisión.

18 COM(2014) 199 final.

- **Consultas con las partes interesadas**

Durante la evaluación del SIS efectuada por la Comisión se solicitaron comentarios y sugerencias de las partes interesadas pertinentes, incluidos los delegados del Comité SISVIS conforme al procedimiento establecido en el artículo 51 del Reglamento (CE) n.º 1987/2006. Este Comité incluye representantes de los Estados miembros tanto en aspectos operativos de SIRENE (cooperación transfronteriza en relación con el SIS) como en aspectos técnicos de desarrollo y mantenimiento del SIS y de la aplicación SIRENE relacionada.

Los delegados respondieron a los cuestionarios detallados como parte del proceso de evaluación. Cuando se precisaron mayores aclaraciones o el tema requirió un mayor desarrollo esto se realizó mediante intercambio de correos electrónicos o entrevistas focalizadas.

Este proceso permitió plantear las cuestiones de una manera integral y transparente. A lo largo de 2015 y 2016, los delegados del Comité SISVIS debatieron estas cuestiones en reuniones y talleres específicos.

La Comisión también realizó consultas específicas con las autoridades de protección de datos de los Estados miembros y los miembros del Grupo de Coordinación de la Supervisión del SIS II en el ámbito de la protección de datos. Los Estados miembros compartieron sus experiencias sobre las solicitudes de acceso del interesado y la labor de las autoridades nacionales de protección de datos, respondiendo a un cuestionario específico. Las respuestas a este cuestionario han influido en la elaboración de la presente propuesta.

Internamente, la Comisión creó un Grupo Director Interservicios con la Secretaría General y las Direcciones Generales de Migración y Asuntos de Interior, Justicia y Consumidores, Recursos Humanos y Seguridad, e Informática. Este Grupo supervisó el proceso de evaluación y ofreció las orientaciones necesarias.

Las conclusiones de la evaluación también tuvieron en cuenta las pruebas recogidas durante las visitas de evaluación *in situ* a los Estados miembros, examinando en profundidad la forma en que el SIS se utiliza en la práctica. Esto incluye debates y entrevistas con profesionales, con personal de SIRENE y con las autoridades nacionales competentes.

En el contexto del Grupo de Contacto de la Directiva sobre retorno de la Comisión, durante sus reuniones de los días 16 de noviembre de 2015 y 18 de marzo y 20 de junio de 2016, también se pidieron comentarios y sugerencias de las autoridades de los Estados miembros competentes en materia de retorno, en particular en lo que respecta a las consecuencias de una posible obligación de introducir en el SIS descripciones de todas las prohibiciones de entrada emitidas de conformidad con la Directiva 2008/115/CE.

Teniendo en cuenta estas aportaciones, la presente propuesta prevé medidas para mejorar la eficiencia técnica y operativa y la eficacia del sistema.

- **Obtención y uso de asesoramiento especializado**

Además de la consulta a las partes interesadas, la Comisión también solicitó asesoramiento externo a través de cuatro estudios, cuyos resultados se han integrado en el desarrollo de la presente propuesta:

- Evaluación técnica del SIS (Kurt Salmon)[19]

En esta evaluación se determinaron las cuestiones clave del funcionamiento del SIS y las necesidades futuras que deben abordarse, identificando en primer lugar los problemas por lo que se refiere a potenciar al máximo la continuidad de la actividad y asegurarse de que la arquitectura general del SIS pueda adaptarse a las crecientes necesidades de capacidad.

- Evaluación del impacto de las tecnologías de la información y la comunicación en las posibles mejoras en la arquitectura del SIS II (Kurt Salmon)[20]

En este estudio se evaluó el coste actual de funcionamiento del SIS a nivel nacional y se evaluaron dos posibles hipótesis técnicas para la mejora del sistema. Ambas incluyen una serie de propuestas centradas en mejoras en el sistema central y la arquitectura general.

- Evaluación del impacto de las tecnologías de la información y la comunicación en las mejoras técnicas en la arquitectura del SIS II — Informe final, 10 de noviembre de 2016 (Wavestone)[21]

En este estudio se evaluó el impacto de los costes en los Estados miembros de la aplicación de una copia nacional, analizando tres hipótesis (un sistema plenamente centralizado, una aplicación N.SIS normalizada facilitada por eu-LISA a los Estados miembros, y una aplicación N.SIS diferenciada con normas técnicas comunes).

- Estudio sobre la viabilidad y las implicaciones de establecer, en el marco del Sistema de Información de Schengen, un sistema a escala de la UE para el intercambio de datos sobre las decisiones de retorno y el seguimiento del cumplimiento de las mismas (PwC)[22].

Este estudio analiza la viabilidad y las repercusiones técnicas y operativas de los cambios introducidos en el SIS con el fin de reforzar su utilización para el retorno de los migrantes irregulares y para impedir su regreso.

- **Evaluación de impacto**

La Comisión no realizó una evaluación de impacto.

Las tres evaluaciones independientes antes mencionadas constituyeron la base para analizar los efectos de los cambios introducidos en el sistema desde el punto de vista técnico. Además, la Comisión ha realizado dos revisiones del Manual SIRENE desde 2013, es decir, desde que entró en funcionamiento el SIS II el 9 de abril de 2013 y desde que entró en vigor la Decisión 2007/533/JAI. Esto incluye una evaluación de la revisión intermedia que dio lugar a un nuevo Manual SIRENE[23] el 29 de enero de 2015. La Comisión adoptó también un catálogo de

---

19 Informe final de la Comisión Europea — Evaluación técnica del SIS II.

20 Informe final de la Comisión Europea — Evaluación del impacto de las tecnologías de la información y la comunicación en las posibles mejoras en la arquitectura del SIS II de 2016.

21 Informe final de la Comisión Europea — Evaluación del impacto de las tecnologías de la información y la comunicación en las mejoras técnicas en la arquitectura del SIS II — Informe final, 10 de noviembre de 2016 (Wavestone).

22 Estudio sobre la viabilidad y las implicaciones de establecer, en el marco del SIS, un sistema a escala de la UE para el intercambio de datos sobre las decisiones de retorno y el seguimiento del cumplimiento de las mismas, 4 de abril de 2015, PwC.

23 Decisión de Ejecución (UE) 2015/219, de 29 de enero de 2015, por la que se sustituye el anexo de la Decisión de Ejecución 2013/115/UE relativa al Manual SIRENE y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II), DO L 44 de 18.2.2015, p. 75.

mejores prácticas y recomendaciones[24]. Además, eu-LISA y los Estados miembros realizan periódicamente mejoras técnicas en el sistema. Se considera que estas opciones ya se han agotado y que se requiere una modificación más general de la base jurídica. La claridad en ámbitos como la aplicación de sistemas para los usuarios finales, así como normas detalladas sobre supresión de descripciones no puede lograrse únicamente mediante una mejor aplicación y un mejor cumplimiento.

Asimismo, la Comisión ha realizado una evaluación exhaustiva del SIS, según lo exigido por el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006 y por el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, y ha publicado un documento de trabajo de los servicios de la Comisión. Los resultados de la evaluación exhaustiva (el informe de evaluación y el correspondiente documento de trabajo de los servicios se adoptaron el 21 de diciembre de 2016) han constituido la base de las medidas contenidas en la presente propuesta.

El mecanismo de evaluación de Schengen, establecido en el Reglamento (UE) n.º 1053/2013[25] prevé que periódicamente se efectúe una evaluación jurídica y operativa del funcionamiento del SIS en los Estados miembros. Las evaluaciones son llevadas a cabo conjuntamente por la Comisión y los Estados miembros. A través de este mecanismo, el Consejo formula recomendaciones a los Estados miembros, basadas en las evaluaciones efectuadas en el marco de los programas plurianuales y anuales. Debido a su naturaleza específica, estas recomendaciones no pueden sustituir a las normas jurídicamente vinculantes que son aplicables simultáneamente a todos los Estados miembros que utilizan el SIS.

El Comité SISVIS debate con regularidad cuestiones prácticas, técnicas y operativas. A pesar de que estas reuniones son útiles para la cooperación entre la Comisión y los Estados miembros, los resultados de las mismas (a falta de cambios en la legislación) no pueden solucionar problemas que surgen debido a la divergencia de las prácticas nacionales, por ejemplo.

Los cambios propuestos en el presente Reglamento no suponen un impacto económico o medioambiental significativo. Sin embargo, se espera que tengan un impacto social positivo significativo, dado que aportan una mayor seguridad al permitir una mejor identificación de las personas que utilizan identidades falsas, los delincuentes que cometido un delito grave y cuya identidad se desconoce, así como los migrantes irregulares que se aprovechan del espacio sin controles en las fronteras interiores. El impacto de estos cambios en los derechos fundamentales y la protección de datos se ha examinado y se expone con más detalle en el capítulo siguiente («Derechos fundamentales»).

La propuesta se ha elaborado utilizando las pruebas recogidas para apoyar la evaluación del SIS de segunda generación, que estudió el funcionamiento del sistema y los posibles ámbitos de mejora. Además, se realizó un estudio de evaluación de la repercusión de los costes, a fin de garantizar que la arquitectura elegida fuera la más apropiada y proporcionada.

---

[24] Recomendación de la Comisión por la que se establece un catálogo de recomendaciones y mejores prácticas para la correcta aplicación del Sistema de Información de Schengen de segunda generación (SIS II) y el intercambio de información complementaria por parte de las autoridades competentes de los Estados miembros que utilizan el SIS II, C(2015) 9169/1.

[25] Reglamento (UE) n.º 1053/2013 del Consejo, de 7 de octubre de 2013, por el que se establece un mecanismo de evaluación y seguimiento para verificar la aplicación del acervo de Schengen, y se deroga la Decisión del Comité Ejecutivo de 16 de septiembre de 1998 relativa a la creación de una Comisión permanente de evaluación y aplicación de Schengen, DO L 295 de 6.11.2013, p. 27.

- **Derechos fundamentales y protección de datos**

La presente propuesta desarrolla y perfecciona el sistema existente, en vez de crear uno nuevo, y por lo tanto se basa en salvaguardias importantes y eficaces ya establecidas. Sin embargo, dado que el sistema continúa tratando datos personales, y tratará otras categorías de datos biométricos sensibles, existen posibles repercusiones en los derechos fundamentales de las personas. Estos impactos se han examinado a fondo, y se han tomado medidas adicionales para limitar la recogida y posterior tratamiento de datos a lo estrictamente necesario e imprescindible a efectos del funcionamiento, y para restringir el acceso a los datos a quienes tienen necesidad operativa de tratarlos. En la presente propuesta se han definido claramente los plazos para la conservación de los datos, y se reconocen explícitamente y se especifican los derechos de los interesados de acceder y rectificar los datos que les conciernan y de solicitar la supresión de conformidad con sus derechos fundamentales (véase la sección sobre protección de datos y seguridad).

Además, la propuesta refuerza las medidas dirigidas a proteger los derechos fundamentales, dado que legisla sobre los requisitos para suprimir una descripción y se introduce una evaluación de la proporcionalidad si se amplía una descripción. La propuesta define amplias y sólidas salvaguardias para el uso de identificadores biométricos a fin de evitar perjudicar a personas inocentes.

La propuesta vela también por la seguridad en todas las fases de funcionamiento del sistema, garantizando una mayor protección de los datos almacenados en él. Con la introducción de un procedimiento claro de gestión de incidentes, así como la mejora de la continuidad de las actividades del SIS, la presente propuesta es plenamente conforme con la Carta de los Derechos Fundamentales de la Unión Europea[26] en lo que respecta al derecho a la protección de los datos personales. El desarrollo y la eficacia permanente del SIS contribuirá a la seguridad de las personas en el seno de la sociedad.

La propuesta prevé cambios significativos en relación con los identificadores biométricos. Además de las impresiones dactilares, también deberán recogerse y almacenarse impresiones palmares si se cumplen los requisitos legales. Los registros de las impresiones dactilares figuran adjuntos a las descripciones alfanuméricas del SIS según lo previsto en el artículo 24. En el futuro deberá ser posible hacer consultas de estos datos (impresiones dactilares y palmares) con las impresiones dactilares encontradas en un lugar del delito, siempre que se trate de un delito grave o terrorista y que exista un alto grado de probabilidad de que pertenezcan al autor. En caso de incertidumbre sobre la identidad de una persona basándose en su documentación, las autoridades competentes deben comparar sus impresiones dactilares con las almacenadas en la base de datos del SIS.

La propuesta exige la recopilación y almacenamiento de datos adicionales (como detalles relativos a los documentos de identificación personal) que faciliten el trabajo de los agentes sobre el terreno para comprobar la identidad de una persona.

La propuesta garantiza al interesado el derecho al recurso efectivo para impugnar las decisiones, lo que incluirá, en cualquier caso, la tutela judicial efectiva ante un órgano jurisdiccional de conformidad con el artículo 47 de la Carta de los Derechos Fundamentales.

---

[26] Carta de los Derechos Fundamentales de la Unión Europea, DO C 326 de 2012, p. 2.

4. REPERCUSIONES PRESUPUESTARIAS

El SIS es un sistema de información único. Por consiguiente, los gastos previstos en dos de las propuestas (la actual y la propuesta de Reglamento relativo al establecimiento, funcionamiento y utilización del SIS en los ámbitos de la cooperación policial y judicial en materia penal) no deberían considerarse dos importes separados, sino uno solo. Las repercusiones presupuestarias de los cambios requeridos para la aplicación de ambas propuestas se incluyen en una ficha financiera legislativa.

Debido a la naturaleza complementaria de la tercera propuesta (relativa al retorno de los nacionales de terceros países en situación irregular), las repercusiones presupuestarias se abordan por separado y en una ficha financiera independiente dedicada únicamente al establecimiento de esta categoría de descripción específica.

Sobre la base de la evaluación de los diferentes aspectos de los trabajos necesarios en relación con la red, el SIS Central por parte de eu-LISA y los desarrollos nacionales en los Estados miembros, las dos propuestas de Reglamento requerirán un importe total de 64,3 millones EUR para el periodo 2018-2020.

Esto incluye un aumento del ancho de banda de TESTA-NG debido a que, de conformidad con las dos propuestas, la red transmitirá archivos con impresiones dactilares e imágenes faciales que requieren más caudal de tráfico y más capacidad (9,9 millones EUR). Cubre asimismo los gastos de eu-LISA en relación con el personal y el funcionamiento (17,6 millones EUR). eu-LISA informó a la Comisión de que la contratación de tres nuevos agentes contractuales tendrá lugar en enero de 2018, a fin de iniciar la fase de desarrollo a su debido tiempo y garantizar la operatividad de las funcionalidades actualizadas del SIS en 2020. La presente propuesta implica modificaciones técnicas en el SIS Central con el fin de ampliar algunas de las categorías de descripciones y aportar nuevas funcionalidades. La ficha financiera adjunta a la presente propuesta refleja estos cambios.

Por otra parte, la Comisión llevó a cabo un estudio para evaluar los costes de desarrollo nacionales requeridos por la presente propuesta[27]. El coste estimado es de 36,8 millones EUR, que deben distribuirse a través de una cantidad a tanto alzado entre los Estados miembros. Por tanto, cada Estado miembro recibirá un importe de 1,2 millones EUR para adaptar su sistema nacional de conformidad con los requisitos establecidos en la presente propuesta, incluida la creación de una copia nacional parcial en caso de que aún no la tengan, o un sistema de copia de seguridad.

Se ha previsto una reprogramación del resto del paquete «fronteras inteligentes» del Fondo de Seguridad Interior para llevar a cabo las mejoras y aplicar las funcionalidades previstas en ambas propuestas. El Reglamento de Fronteras FSI[28] es el instrumento financiero en el que se ha incluido el presupuesto de ejecución del paquete de medidas sobre «fronteras inteligentes». El artículo 5 del Reglamento establece que se ejecutarán 791 millones EUR a través de un programa encaminado a la creación de sistemas de tecnología de la información en apoyo de la gestión de los flujos migratorios en las fronteras exteriores en las condiciones establecidas en el artículo 15. De los citados 791 millones EUR, 480 están reservados para el desarrollo

---

27 Wavestone - Evaluación del impacto de las tecnologías de la información y la comunicación en las mejoras técnicas en la arquitectura del SIS II - Informe final, 10 de noviembre de 2016. Hipótesis 3, Aplicación segregada del N.SIS II.

28 Reglamento (UE) n.º 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, DO L 150 de 20.5.2014, p. 143.

del Sistema de Entradas y Salidas, y 210 para el desarrollo del Sistema Europeo de Información y Autorización de Viajes (SEIAV). El resto se utilizarán en parte para financiar los costes de los cambios previstos en las dos propuestas relativas al SIS.

5. OTROS ELEMENTOS

• Planes de ejecución y modalidades de seguimiento, evaluación e información

La Comisión, los Estados miembros y eu-LISA revisarán periódicamente y supervisarán la utilización del SIS, con el fin de garantizar que sigue funcionando de manera eficaz y eficiente. La Comisión estará asistida por el Comité SISVIS para establecer las medidas técnicas y operativas descritas en la propuesta.

Además, la presente propuesta de Reglamento prevé, en el artículo 54, apartados 7 y 8, un proceso de revisión y evaluación formal periódico.

Cada dos años, eu-LISA deberá informar al Parlamento Europeo y al Consejo sobre el funcionamiento técnico del SIS, incluida la seguridad, la infraestructura de comunicación que lo sostiene y el intercambio bilateral y multilateral de información complementaria entre los Estados miembros.

Además, cada cuatro años, la Comisión deberá realizar, y compartir con el Parlamento y el Consejo, una evaluación del SIS y el intercambio de información entre los Estados miembros. Esta evaluación:

- examinará los resultados comparándolos con los objetivos;
- evaluará si la lógica en que se basa el sistema sigue siendo válida;
- estudiará la forma en que el Reglamento se aplica al sistema central;
- evaluará la seguridad del sistema central;
- estudiará las implicaciones para el futuro funcionamiento del sistema.

eu-LISA tendrá la responsabilidad de facilitar estadísticas diarias, mensuales y anuales sobre la utilización del SIS, efectuando un seguimiento continuo del sistema y su funcionamiento en función de los objetivos.

• Explicación detallada de las nuevas disposiciones de la propuesta

Disposiciones comunes a la presente propuesta y a la propuesta de Reglamento relativo al establecimiento, funcionamiento y utilización del SIS en los ámbitos de la cooperación policial y judicial en materia penal:

- Disposiciones generales (artículos 1-3)
- Arquitectura técnica y funcionamiento del SIS (artículos 4-14)
- Responsabilidades de eu-LISA (artículos 15-18)
- Derecho de acceso a las descripciones y periodo de conservación (artículos 29, 30, 31, 33 y 34)
- Normas generales sobre tratamiento y protección de datos (artículos 36-53)
- Seguimiento y estadísticas (artículo 54)

Utilización del SIS en todas sus fases de funcionamiento

Con más de dos millones de usuarios finales entre las autoridades competentes en toda Europa, el SIS es una herramienta muy utilizada y eficaz de intercambio de información. Estas propuestas incluyen normas que regulan el funcionamiento del sistema en todas sus fases, incluido el SIS Central gestionado por eu-LISA, los sistemas nacionales y las aplicaciones de los usuarios finales. Se abordan no solo los sistemas central y nacionales, sino también las necesidades técnicas y operativas de los usuarios finales.

El artículo 9, apartado 2, especifica que los usuarios finales deben recibir la información necesaria para llevar a cabo sus tareas (en particular todos los datos requeridos para la identificación del interesado y para adoptar las medidas necesarias). Establece, asimismo, un modelo común para la aplicación del SIS por los Estados miembros, garantizando la armonización en todos los sistemas nacionales. El artículo 6 establece que los Estados miembros deberán garantizar que los usuarios finales dispongan ininterrumpidamente de los datos del SIS, con el fin de maximizar los beneficios operativos al reducir los momentos de indisponibilidad del sistema.

El artículo 10, apartado 3, garantiza que la seguridad del tratamiento de los datos incluya también las actividades de tratamiento de datos del usuario final. El artículo 14 obliga a los Estados miembros a garantizar que el personal con acceso al SIS reciba formación periódica y continua en materia de seguridad de datos y normas de protección de datos.

Como consecuencia de la inclusión de dichas medidas, esta propuesta abarca todo el funcionamiento del SIS, con normas y obligaciones relativos a los millones de usuarios finales en toda Europa. Con el fin de que el SIS sea plenamente efectivo, los Estados miembros deben garantizar que cada vez que sus usuarios finales estén facultados para realizar una consulta en una base de datos nacional policial o de inmigración, realicen paralelamente la consulta en el SIS. De esta manera, el SIS podrá cumplir su objetivo de ser la principal medida compensatoria en el espacio sin controles en las fronteras interiores y los Estados miembros podrán abordar mejor la dimensión transfronteriza de la delincuencia y la movilidad de los delincuentes. Esta consulta paralela deberá ser conforme con el artículo 4 de la Directiva (UE) 2016/680[29].

Continuidad de las actividades

La propuesta refuerza las disposiciones sobre continuidad de las actividades, tanto a nivel nacional como para eu-LISA (artículos 4, 6, 7 y 15). De este modo se asegura que el SIS siga siendo operativo y accesible para el personal sobre el terreno, incluso en caso de que se produzcan problemas que afecten al sistema.

Calidad de los datos

La propuesta mantiene el principio de que el Estado miembro, que es el propietario de los datos, también será responsable de la exactitud de los introducidos en el SIS (artículo 39). Sin embargo, es necesario prever un mecanismo central gestionado por eu-LISA que permita a los Estados miembros revisar periódicamente las descripciones en las que los campos de datos obligatorios puedan plantear problemas de calidad. Por tanto, el artículo 15 de la propuesta

[29] 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 la libre circulación de dichos datos, DO L 119 de 4.5.2016, p. 89.

faculta a eu-LISA para elaborar periódicamente informes de calidad de los datos, destinados a los Estados miembros. Esta actividad podrá facilitarse mediante un repositorio para elaborar informes estadísticos y de calidad de los datos (artículo 54). Estas mejoras reflejan los resultados provisionales del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad.

Fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN

La posibilidad de efectuar consultas con las impresiones dactilares para identificar a una persona ya está prevista en el artículo 22 del Reglamento (CE) n.º 1987/2006 y en la Decisión 2007/533/JAI del Consejo. Las propuestas hacen que esta consulta sea obligatoria si la identidad de la persona no puede determinarse de otra forma. Actualmente, las imágenes faciales solo pueden utilizarse para confirmar la identidad de una persona a raíz de una consulta alfanumérica, y no como base para una consulta. Además, los cambios en los artículos 22 y 28 prevén que las imágenes faciales, las fotografías y las impresiones palmares se utilizarán para consultar el sistema e identificar a las personas, cuando sea técnicamente posible. La dactiloscopia consiste en el estudio científico de las impresiones dactilares como método de identificación. Los expertos en dactiloscopia afirman que las impresiones palmares tienen la característica de su singularidad y que contienen puntos de referencia que permiten hacer comparaciones precisas y concluyentes al igual que las impresiones dactilares por lo que pueden utilizarse para establecer la identidad de una persona de la misma forma que las impresiones dactilares. La toma de impresiones palmares junto con las diez impresiones dactilares rodadas y planas de una persona ha sido la práctica de la policía durante muchos decenios. Existe un uso principal de las impresiones palmares, a saber, la identificación cuando el sujeto ha dañado de forma deliberada o involuntariamente las yemas de los dedos para evitar ser identificado o evitar que se tomen las impresiones dactilares, o por daños causados por accidentes o trabajos manuales pesados. En el transcurso del debate sobre las normas técnicas del SIS AFIS, los Estados miembros comunicaron un éxito considerable en la identificación de los migrantes irregulares que habían dañado deliberadamente las yemas de sus dedos, en un intento por evitar su identificación. La toma de las impresiones palmares por las autoridades de los Estados miembros permitió la posterior identificación.

El uso de imágenes faciales para la identificación garantizará una mejor coherencia entre el SIS y el Sistema de Entradas y Salidas propuesto, las barreras electrónicas y los quioscos de autoservicio. Esta funcionalidad se limitará a los pasos fronterizos regulares.

Acceso al SIS por parte de las autoridades - usuarios institucionales

En este apartado se describen los elementos nuevos en términos de derechos de acceso al SIS por lo que respecta a las agencias de la UE (usuarios institucionales). Los derechos de acceso de las autoridades nacionales competentes no se han modificado.

Europol (artículo 30) y la Agencia Europea de la Guardia de Fronteras y Costas (así como sus equipos, los equipos de personal implicados en tareas relacionadas con el retorno y los miembros del equipo de apoyo a la gestión de la migración) y la unidad central del SEIAV de la Agencia (artículos 31 y 32) tienen acceso al SIS y a los datos del SIS que necesiten. Se han instaurado unas salvaguardias adecuadas para garantizar que los datos del sistema estén debidamente protegidos (incluidas también las disposiciones del artículo 33, que exigen que estos organismos podrán acceder únicamente a los datos que necesiten para llevar a cabo sus tareas).

Estos cambios amplían el acceso de Europol al SIS en cuanto a las descripciones para la denegación de entrada, garantizando que pueda hacer el mejor uso del sistema en la

realización de sus tareas, y añaden nuevas disposiciones para garantizar que la Agencia Europea de la Guardia de Fronteras y Costas, así como sus equipos, puedan acceder al sistema cuando realicen las distintas operaciones bajo su mandato para asistir a los Estados miembros. Además, en virtud de la propuesta de la Comisión de un Reglamento del Parlamento Europeo y del Consejo por el que se crea un Sistema Europeo de Información y Autorización de Viajes (SEIAV)[30], la unidad central de la Agencia Europea de la Guardia de Fronteras y Costas efectuará consultas en el SIS a través del SEIAV para determinar si el nacional de un tercer país que solicite una autorización de viaje es objeto de una descripción en el SIS. Para ello, la unidad central SEIAV también tendrá pleno acceso al SIS[31].

El artículo 29, apartado 3, establece que las autoridades competentes en materia de visados nacionales también podrán, en el ejercicio de sus funciones, acceder a las descripciones relativas a documentos expedidos con arreglo al Reglamento 2008/...., relativo al establecimiento, funcionamiento y utilización del SIS en el ámbito de la cooperación policial y judicial en materia penal.

Esto permitirá a dichos organismos acceder al SIS y a los datos del SIS que necesiten para llevar a cabo sus tareas, al tiempo que se establecen las salvaguardias apropiadas para asegurar que los datos del sistema estén debidamente protegidos (incluidas también las disposiciones del artículo 35, que exigen que estos organismos podrán acceder únicamente a los datos que necesiten para llevar a cabo sus tareas).

Denegación de entrada y de estancia

En la actualidad, de conformidad con el artículo 24, apartado 3, del Reglamento SIS II, un Estado miembro podrá introducir una descripción en el SIS de personas sujetas a prohibición de entrada por razón del incumplimiento de la legislación nacional en materia de migración. El artículo 24, apartado 3, revisado obliga a introducir la descripción en el SIS en todos los casos en que se haya emitido una prohibición de entrada a un nacional de un tercer país en situación irregular en virtud de disposiciones conformes a la Directiva 2008/115/CE. Asimismo, establece los plazos y condiciones para introducir dichas descripciones después de que haya abandonado el territorio de los Estados miembros en cumplimiento de una obligación de retorno. Esta disposición se inserta con el fin de evitar que las prohibiciones de entrada sean visibles en el SIS mientras el nacional de un tercer país esté aún presente en el territorio de la UE. Dado que las prohibiciones de entrada prohíben el reingreso en el territorio de los Estados miembros, solo pueden entrar en vigor tras el retorno de los nacionales de terceros países. Al mismo tiempo, los Estados miembros deben tomar todas las medidas necesarias para garantizar que no exista ningún lapso de tiempo entre el momento del retorno y la activación en el SIS de la descripción relativa a la prohibición de entrada y estancia.

La presente propuesta está estrechamente vinculada a la propuesta de la Comisión[32] relativa al uso del SIS para el retorno de nacionales de terceros países en situación irregular, que establece las condiciones y procedimientos para la introducción en el SIS de descripciones sobre las decisiones de retorno. La propuesta incluye un mecanismo para comprobar si los nacionales de terceros países objeto de un decisión de retorno salen efectivamente del territorio de la UE, y un mecanismo de alerta en caso de incumplimiento. El artículo 26 establece el proceso de consulta que deben seguir los Estados miembros cuando encuentren

---

30 COM(2016) 731 final.

31 La unidad central SEIAV tendrá acceso a efectos de los artículos 24 y 27 del presente Reglamento.

32 COM(2016) …

descripciones sobre denegación de entrada y estancia, o deseen introducir tales descripciones, que interfieran con decisiones de otros Estados miembros, como por ejemplo un permiso de residencia válido. Tales normas deben servir para evitar la aparición de instrucciones contradictorias que puedan crear estas situaciones, o para resolverlas, al tiempo que ofrecen una orientación clara a los usuarios finales sobre las medidas que han de adoptarse en tales situaciones y a las autoridades de los Estados miembros sobre si debe suprimirse una descripción.

El artículo 27 [antiguo artículo 26 del Reglamento (CE) n.º 1987/2006], tiene por objetivo aplicar el régimen de sanciones de la UE que afecta a los nacionales de terceros países que estén sujetos a una restricción para ser admitidos en el territorio de la UE de conformidad con el artículo 29 del Tratado de la Unión Europea. A fin de permitir introducir dichas descripciones era necesario exigir los datos mínimos necesarios para la identificación de la persona, a saber, nombre y fecha de nacimiento. El hecho de que el Reglamento (CE) n.º 1987/2006 eximiera de la obligación de indicar la fecha de nacimiento generó grandes problemas, pues sin una fecha de nacimiento no puede crearse ninguna descripción en el SIS, de conformidad con las normas técnicas y los parámetros de consulta del sistema. Puesto que el artículo 27 es indispensable para contar con un régimen de sanciones eficaz en la UE, el requisito de proporcionalidad no se aplica a este respecto.

Con el fin de garantizar una mayor coherencia con la Directiva 2008/115/CE, la terminología empleada al hacer referencia a la finalidad de la descripción («denegación de entrada y estancia») se ha armonizado con la redacción empleada en la Directiva.

Distinción entre personas con características similares

Con el fin de garantizar que los datos sean tratados y almacenados de modo adecuado, y para reducir el riesgo de duplicación e identificación errónea, el artículo 41 establece el procedimiento a seguir cuando, al introducir una nueva descripción, resulte que ya hay una inscripción en el SIS con características similares.

Seguridad y protección de datos

La presente propuesta aclara la responsabilidad de prevenir, denunciar y responder a incidentes que puedan afectar a la seguridad o la integridad de la infraestructura del SIS, los datos del SIS o información adicional (artículos 10, 16 y 40).

El artículo 12 establece disposiciones sobre el mantenimiento y la consulta de los registros que incluyan el historial de las descripciones.

El artículo 15, apartado 3, mantiene el artículo 15, apartado 3, del Reglamento (CE) n.º 1987/2006 y dispone que la Comisión será responsable de la gestión contractual de la infraestructura de comunicación, así como de las tareas relacionadas con la ejecución del presupuesto y la adquisición y renovación. Estas tareas se transferirán a eu-LISA en la segunda serie de propuestas del SIS en junio de 2017.

El artículo 21 amplía la obligación de los Estados miembros de examinar la proporcionalidad antes de emitir descripciones, para aplicarla también a las decisiones sobre si debe prorrogarse el periodo de validez de la descripción. Como novedad, no obstante, el artículo 21, apartado 2, letra c), dispone que los Estados miembros deberán crear en todo caso una descripción sobre las personas cuyas actividades estén contempladas en los artículos 1, 2, 3 y 4 de la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo.

Categorías de datos y tratamiento de datos

Con el fin de proporcionar más información y más precisa a los usuarios finales para facilitar y acelerar la adopción de la medida requerida, así como para permitir una mejor identificación del sujeto de la descripción, la presente propuesta amplía los tipos de información (artículo 20) que pueden conservarse respecto de las personas para las que se haya introducido una descripción, para incluir también:

- si la persona participa en una actividad que corresponda a los artículos 1, 2, 3 y 4 de la Decisión Marco 2002/475/JAI del Consejo;
- si la descripción está relacionada con un ciudadano de la UE u otra persona que goce de derechos de libre circulación equivalentes a los de los ciudadanos de la UE;
- si una decisión sobre la denegación de entrada se basa en lo dispuesto en los artículos 24 o 27;
- el tipo de delito (para las descripciones previstas en el artículo 24, apartado 2,);
- datos del documento de identidad o de viaje de una persona;
- copia en color del documento de identidad o de viaje de una persona;
- fotografías e imágenes faciales;
- impresiones dactilares e impresiones palmares.

Contar con datos adecuados es fundamental para garantizar la identificación precisa de una persona que sea objeto de un control en un paso fronterizo o de un control interno o que solicite un permiso de residencia. Una identificación inexacta puede dar lugar a problemas relativos a los derechos fundamentales; también puede provocar una situación en la que no puedan tomarse medidas de seguimiento adecuadas puesto que no se conoce la existencia o el contenido de una descripción.

En cuanto a la información sobre la decisión subyacente, se pueden distinguir cuatro motivos: una condena anterior según lo previsto en el artículo 24, apartado 2, letra a); una amenaza grave para la seguridad según lo previsto en el artículo 24, apartado 2, letra b); una prohibición de entrada según lo previsto en el artículo 24, apartado 3; y una medida restrictiva según lo previsto en el artículo 27. Con el fin de garantizar que se toman las medidas adecuadas en caso de una respuesta positiva, es también preciso indicar si la alerta está relacionada con un ciudadano de la UE o con otra persona que goce de derechos de libre circulación equivalentes a los de los ciudadanos de la UE. Contar con datos adecuados es fundamental para garantizar la identificación precisa de una persona que sea objeto de un control en un paso fronterizo o de un control interno o que solicite un permiso de residencia. Una identificación inexacta puede dar lugar a problemas relativos a los derechos fundamentales; también puede provocar una situación en la que no puedan tomarse medidas de seguimiento adecuadas puesto que no se conoce la existencia o el contenido de una descripción.

También (artículo 42) se amplía la lista de datos personales que pueden introducirse y tratarse en el SIS a fin de tratar la usurpación de identidad, pues el contar con más datos facilita la identificación de la víctima y del autor de la usurpación de identidad. La ampliación de esta disposición no entraña riesgos, ya que todos estos datos solo pueden introducirse con el consentimiento de la víctima de la usurpación de identidad. Ahora también se incluirán:

- imágenes faciales;

- impresiones palmares;
- datos de los documentos de identidad;
- dirección de la víctima;
- nombre de su padre y de su madre.

El artículo 20 prevé una información más detallada en las descripciones. Incluye categorías para el motivo de la denegación de entrada y de estancia y detalles de los documentos de identificación personal de los interesados. La mejora de la información permite una mejor identificación de la persona afectada, y permite a los usuarios finales tomar decisiones con más conocimiento de causa. Para la protección de los usuarios finales que realizan los controles, el SIS también mostrará si la persona que motivó la descripción entra en alguna de las categorías previstas en los artículos 1, 2, 3 y 4 de la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo[33].

La propuesta deja claro que los Estados miembros no deberán copiar a otros ficheros de datos nacionales los datos introducidos por otro Estado miembro (artículo 37).

Conservación

El artículo 34 establece el plazo para la revisión de las descripciones. El periodo máximo de conservación de las descripciones de denegación de entrada y estancia se ha armonizado con el plazo máximo posible de las prohibiciones de entrada emitidas con arreglo al artículo 11 de la Directiva 2008/115/CE. Por consiguiente, el periodo máximo de retención será de cinco años; no obstante, los Estados miembros podrán fijar periodos más cortos.

Supresión

El artículo 35 establece las circunstancias en las que se suprimirán las descripciones, en aras de una mayor armonización de las prácticas nacionales en este ámbito; establece disposiciones particulares para que el personal de las Oficinas SIRENE suprima descripciones que dejen de ser necesarias si no se recibe respuesta alguna de las autoridades competentes.

Derechos de los interesados a acceder a sus datos, rectificar datos inexactos y suprimir los datos almacenados ilegalmente

Las disposiciones detalladas sobre los derechos del interesado se han mantenido sin cambios, dado que la normativa vigente ya garantiza un elevado nivel de protección y está en consonancia con el Reglamento (UE) 2016/679[34] y la Directiva 2016/680[35]. Además, el artículo 48 establece las circunstancias en las que los Estados miembros pueden decidir no comunicar información a los interesados. Ello ha de deberse a uno de los motivos enumerados

---

33 Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, DO L 164 de 22.6.2002, p. 3.

34 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.

35 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 la libre circulación de dichos datos, DO L 119 de 4.5.2016, p. 89.

en dicho artículo, y debe ser una medida proporcionada y necesaria, conforme con la legislación nacional.

Estadísticas

Con el fin de mantener una visión general del funcionamiento de los recursos en la práctica, el artículo 49 prevé un sistema de estadísticas normalizado que realice informes anuales sobre el número de:

- solicitudes de acceso de los interesados;
- solicitudes de rectificación de datos inexactos y supresión de datos que se hayan almacenado de manera ilegal;
- asuntos pendientes ante los órganos jurisdiccionales;
- asuntos en que el órgano jurisdiccional haya fallado a favor del demandante; y
- observaciones sobre casos de reconocimiento mutuo de resoluciones definitivas dictadas por órganos jurisdiccionales o autoridades de otros Estados miembros sobre descripciones creadas por el Estado que haya emitido la descripción.

Seguimiento y estadísticas

El artículo 54 establece los mecanismos que deben ponerse en marcha para garantizar el seguimiento adecuado del SIS y su funcionamiento con respecto a sus objetivos. Para ello, eu-LISA deberá proporcionar estadísticas diarias, mensuales y anuales sobre cómo se utiliza el sistema.

El artículo 54, apartado 5, prevé que eu-LISA facilitará a los Estados miembros, la Comisión, Europol y la Agencia Europea de la Guardia de Fronteras y Costas informes estadísticos que elabore, y permitirá a la Comisión solicitar más informes estadísticos e informes de calidad de los datos del SIS y de las comunicaciones SIRENE.

El artículo 54, apartado 6, prevé la creación y el alojamiento de un repositorio central de datos, como parte de la labor de eu-LISA de seguimiento del funcionamiento del SIS. Esto permitirá que el personal autorizado de los Estados miembros, la Comisión, Europol y la Agencia Europea de la Guardia de Fronteras y Costas acceda a los datos enumerados en el artículo 54, apartado 3, a fin de elaborar las estadísticas necesarias.

2016/0408 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, que modifica el Reglamento (UE) n.º 515/2014 y que deroga el Reglamento (CE) n.º 1987/2006.

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 77, apartado 2, letras b) y d), y su artículo 79, apartado 2, letra c),

Vista la propuesta de la Comisión Europea,

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

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) El Sistema de Información de Schengen (SIS) constituye un instrumento esencial para la aplicación de las disposiciones del acervo de Schengen integrado en el marco de la Unión Europea. El SIS es una de las principales medidas compensatorias que contribuye al mantenimiento de un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión Europea, mediante el apoyo de la cooperación operativa entre guardias de fronteras, autoridades policiales, aduaneras y otras, autoridades judiciales en materia penal y autoridades de inmigración.

(2) El SIS fue creado de conformidad con las disposiciones del título IV del Convenio de 19 de junio de 1990 de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes[36] (el Convenio de Schengen). El desarrollo del SIS de segunda generación (SIS II) se confió a la Comisión en virtud del Reglamento (CE) n.º 2424/2001 del Consejo[37] y la Decisión 2001/886/JAI del Consejo (SIS)[38] y fue creado por el Reglamento (CE) n.º 1987/2006[39] así como por la Decisión

[36] DO L 239 de 22.9.2000, p. 19. Convenio modificado por el Reglamento (CE) n.º 1160/2005 del Parlamento Europeo y del Consejo, DO L 191 de 22.7.2005, p. 18.

[37] DO L 328 de 13.12.2001, p. 4.

[38] Decisión 2001/886/JAI del Consejo, de 6 de diciembre de 2001, sobre el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II), DO L 328 de 13.12.2001, p. 1.

[39] 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), DO L 381 de 28.12.2006, p. 4.

2007/533/JAI del Consejo[40]. El SIS II sustituyó al SIS, tal como fue creado en virtud del Convenio de Schengen.

(3) Tres años después de la entrada en funcionamiento del SIS II, la Comisión evaluó el sistema con arreglo a lo dispuesto en el artículo 24, apartado 5, el artículo 43, apartado 5, y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006, así como en los artículos 59 y 65, apartado 5, de la Decisión 2007/533/JAI. El informe de evaluación y el correspondiente documento de trabajo se adoptaron el 21 de diciembre de 2016[41]. Las recomendaciones que figuran en dichos documentos deben reflejarse, en su caso, en el presente Reglamento.

(4) El presente Reglamento constituye la base legislativa necesaria para regular el SIS en las materias que entran en el ámbito de aplicación del capítulo 2 del título V del Tratado de Funcionamiento de la Unión Europea. El Reglamento (UE) 2018/... del Parlamento Europeo y del Consejo relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y judicial en materia penal[42] constituye la base legislativa necesaria para regular el SIS en las materias que entran en el ámbito de aplicación de los capítulos 4 y 5 del título V del Tratado de Funcionamiento de la Unión Europea.

(5) El hecho de que la base legislativa necesaria para la regulación del SIS consista en dos instrumentos separados no afecta al principio de que el SIS constituye un único sistema de información que debe funcionar como tal. En consecuencia, algunas disposiciones de dichos instrumentos deben ser idénticas.

(6) Es necesario especificar los objetivos del SIS, su arquitectura técnica y su financiación para establecer las normas relativas a su funcionamiento completo y utilización y para definir las responsabilidades, las categorías de datos que se introducirán en el sistema, los fines para los que se introducirán, los criterios de introducción, las autoridades autorizadas para acceder a los datos, el uso de identificadores biométricos y otras normas sobre tratamiento de datos.

(7) El SIS incluye un sistema central (SIS Central) y unos sistemas nacionales con una copia completa o parcial de la base de datos del SIS. Considerando que el SIS es el instrumento de intercambio de información más importante de Europa, es necesario garantizar su funcionamiento ininterrumpido tanto a nivel central como a nivel nacional. Por consiguiente, cada Estado miembro debe dotarse de una copia completa o parcial de la base de datos del SIS y debe crear su sistema de copia de seguridad.

(8) Es necesario mantener un manual que establezca normas detalladas sobre el intercambio de información complementaria en relación con la acción requerida por las descripciones. Las autoridades nacionales de cada Estado miembro (Oficinas SIRENE) deberán garantizar el intercambio de esta información.

(9) Con el fin de mantener la eficacia del intercambio de información complementaria sobre las medidas que vayan a tomarse especificadas en las descripciones, es preciso

---

40 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.

41 Informe al Parlamento Europeo y al Consejo sobre la evaluación del Sistema de Información de Schengen de segunda generación (SIS II), de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006 y con el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, y un documento de trabajo de los servicios de la Comisión.

42 Reglamento (UE) 2018/...

reforzar el funcionamiento de las Oficinas SIRENE, precisando las exigencias relativas a los recursos disponibles, la formación de los usuarios y el tiempo de respuesta a las consultas recibidas de otras Oficinas SIRENE.

(10) La gestión operativa de los componentes centrales del SIS es ejercida por la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia[43] («la Agencia»). Con el fin de permitir a la Agencia a dedicar los recursos personales y financieros necesarios para abarcar todos los aspectos de la gestión operativa del SIS Central, el presente Reglamento debe establecer sus tareas en detalle, en particular por lo que se refiere a los aspectos técnicos del intercambio de información complementaria.

(11) Sin perjuicio de la responsabilidad de los Estados miembros en cuanto a la exactitud de los datos introducidos en el SIS, la Agencia será responsable de mejorar la calidad de los datos mediante la creación a nivel central de un instrumento de supervisión de la calidad de los datos, así como de suministrar informes periódicamente a los Estados miembros.

(12) Con el fin de permitir una mejor supervisión del uso del SIS para analizar las tendencias relativas a la presión migratoria y la gestión de fronteras, la Agencia deberá poder desarrollar una capacidad de vanguardia para la elaboración de informes estadísticos destinados a los Estados miembros, la Comisión y la Agencia Europea de la Guardia de Fronteras y Costas, sin poner en peligro la integridad de los datos. Por tanto, debe crearse un repositorio central de estadísticas. Las estadísticas elaboradas no deberán contener datos personales.

(13) El SIS deberá incluir más categorías de datos para permitir a los usuarios finales tomar decisiones con pleno conocimiento de causa basándose en una descripción, sin pérdida de tiempo. Por tanto, las descripciones a efectos de la denegación de entrada y estancia deberán contener información sobre la decisión en la que se base la descripción. Además, para facilitar la identificación de personas y detectar las identidades múltiples, la descripción deberá incluir una referencia al documento de identidad personal o su número y una copia de dicho documento, cuando se disponga de ella.

(14) El SIS no deberá conservar ningún dato empleado para efectuar consultas, con excepción de la llevanza de registros para comprobar si la consulta es legal, para controlar la legalidad del tratamiento de datos, para llevar a cabo un control interno y para garantizar el correcto funcionamiento del N.SIS, así como la integridad y seguridad de los datos.

(15) El SIS deberá permitir tratar datos biométricos para ayudar a la identificación fiable de las personas en cuestión. En esta misma perspectiva, el SIS también deberá permitir el tratamiento de datos sobre personas cuya identidad haya sido usurpada (a fin de evitar perjuicios causados por una identificación incorrecta), con las garantías adecuadas; en particular, con el consentimiento de la persona en cuestión y una limitación estricta de los fines para los que dichos datos pueden ser tratados legalmente.

(16) Los Estados miembros deberán adoptar las disposiciones técnicas necesarias para que cada vez que los usuarios finales sean facultados para realizar una consulta en una base de datos nacional de policía o de inmigración consulten también el SIS en

---

[43] Establecida mediante el Reglamento (UE) n.º 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DO L 286 de 1.11.2011, p. 1.

paralelo, con arreglo a lo dispuesto en el artículo 4 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[44]. Esto deberá garantizar que el SIS funcione como la principal medida compensatoria en el espacio sin controles en las fronteras interiores y pueda abordar mejor la dimensión transfronteriza de la delincuencia y la movilidad de los delincuentes.

(17) El presente Reglamento deberá establecer las condiciones para el uso de datos dactiloscópicos e imágenes faciales a efectos de identificación. El uso de imágenes faciales para fines de identificación en el SIS también deberá ayudar a asegurar la coherencia en los procedimientos de inspección fronteriza en los que se requiera la identificación y la comprobación de la identidad mediante el uso de datos dactiloscópicos e imágenes faciales. La consulta mediante datos dactiloscópicos deberá ser obligatoria en caso de que existan dudas sobre la identidad de una persona. Las imágenes faciales para fines de identificación deberán utilizarse únicamente en el marco de las inspecciones fronterizas periódicas en los quioscos de autoservicio y las barreras electrónicas.

(18) Las impresiones dactilares encontradas en el lugar del delito deberán poder cotejarse con los datos dactiloscópicos almacenados en el SIS si puede acreditarse con un alto grado de probabilidad que pertenecen al autor del delito grave o delito de terrorismo. Los delitos graves serán los enumerados en la Decisión Marco 2002/584/JAI del Consejo[45], y los «delitos de terrorismo» serán los tipificados en la legislación nacional a que se refiere la Decisión Marco 2002/475/JAI del Consejo[46]

(19) Deberá existir la posibilidad de que los Estados miembros establezcan conexiones entre las descripciones en el SIS. La creación por un Estado miembro de conexiones entre dos o más descripciones no debe afectar a las medidas que deban tomarse, al periodo de conservación ni a los derechos de acceso a las descripciones.

(20) Puede lograrse un mayor nivel de eficacia, coherencia y armonización haciendo obligatoria la introducción en el SIS de todas las prohibiciones de entrada emitidas por las autoridades competentes de los Estados miembros con arreglo a procedimientos conformes con la Directiva 2008/115/CE[47], y estableciendo normas comunes para introducir dichas descripciones tras el retorno de los nacionales de terceros países en situación irregular. Los Estados miembros deberán adoptar todas las medidas necesarias para garantizar que no exista ningún lapso entre el momento en que el nacional de un tercer país abandona el espacio Schengen y la activación en el SIS de la descripción. Esto deberá asegurar el éxito en la ejecución de las prohibiciones de entrada en los pasos fronterizos exteriores, evitando de forma efectiva el regreso al espacio Schengen.

---

44 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 la libre circulación de dichos datos, y por la que se deroga la Decisión 2008/977/JAI, DO L 119 de 4.5.2016, p. 89.

45 Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, DO L 190 de 18.7.2002. p. 1.

46 Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, DO L 164 de 22.6.2002, p. 3.

47 Directiva 2008/115/CE del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, relativa a normas y procedimientos comunes en los Estados miembros para el retorno de los nacionales de terceros países en situación irregular, DO L 348 de 24.12.2008, p. 98.

(21) El presente Reglamento deberá establecer normas obligatorias para la consulta a las autoridades nacionales en caso de que un nacional de un país tercero sea titular o pueda obtener un permiso de residencia válido u otra autorización o derecho de estancia concedido por un Estado miembro, y otro Estado miembro prevea emitir una descripción, o ya la haya introducido, para la denegación de entrada y estancia a dicho nacional de un tercer país. Tales situaciones generan graves incertidumbres para los guardias de fronteras, la policía y las autoridades de inmigración. Por tanto, es conveniente prever un plazo obligatorio para la consulta rápida con un resultado definitivo a fin de evitar que personas que representan una amenaza puedan entrar en el espacio Schengen.

(22) El presente Reglamento no afectará a la aplicación de la Directiva 2004/38[48].

(23) Las descripciones no deberán mantenerse en el SIS por más tiempo del necesario para cumplir el fin para el que fueron emitidas. A fin de reducir la carga administrativa para las distintas autoridades que participan en el tratamiento de los datos de particulares a distintos efectos, procede adecuar el periodo de conservación de las descripciones de denegación de entrada y estancia con el plazo máximo posible de las prohibiciones de entrada emitidas con arreglo a procedimientos conformes con la Directiva 2008/115/CE. Por tanto, el plazo de conservación de las descripciones sobre personas deberá ser como máximo de cinco años. Por regla general, las descripciones de personas deberán suprimirse automáticamente del SIS transcurrido un periodo de cinco años. Las decisiones de mantener descripciones de personas deberán basarse en una evaluación del caso concreto. Los Estados miembros deberán revisar las descripciones de personas en el periodo de revisión establecido y elaborar estadísticas del número de descripciones cuyo periodo de conservación se haya prorrogado.

(24) La introducción y prórroga de la fecha de expiración de una descripción del SIS deberán estar sujetas al requisito de proporcionalidad, examinando si un caso concreto es adecuado, pertinente y suficientemente importante como para introducir una descripción en el SIS. En casos de delitos con arreglo a los artículos 1, 2, 3 y 4 de la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo[49] siempre deberá crearse una descripción sobre nacionales de terceros países a efectos de denegación de entrada y estancia, teniendo en cuenta el nivel elevado de amenaza y la repercusión general negativa que dicha actividad podría conllevar.

(25) La integridad de los datos del SIS reviste una importancia primordial. Por tanto, deben fijarse salvaguardias apropiadas para tratar los datos del SIS a nivel central y a nivel nacional, a fin de garantizar la seguridad de los datos durante todas las fases de su funcionamiento y utilización. Las autoridades que intervengan en el tratamiento de los datos deberán estar sujetas a los requisitos de seguridad del presente Reglamento y a un procedimiento uniforme de notificación de incidentes.

(26) Los datos tratados en el SIS en aplicación del presente Reglamento no deberán transmitirse ni ponerse a disposición de terceros países ni de organizaciones internacionales.

(27) A fin de aumentar la eficacia del trabajo de las autoridades de inmigración a la hora de decidir sobre el derecho de los nacionales de terceros países a entrar y residir en el

---

[48] Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros, DO L 158 de 30.4.2004, p. 77.

[49] Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, DO L 164 de 22.6.2002, p. 3.

territorio de los Estados miembros, así como sobre el retorno de los nacionales de terceros países en situación irregular, procede concederles acceso al SIS en virtud del presente Reglamento.

(28) El Reglamento (UE) 2016/679[50] deberá aplicarse al tratamiento de datos personales en virtud del presente Reglamento por las autoridades de los Estados miembros cuando la Directiva (UE) 2016/680[51] no sea aplicable. El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo[52] deberá aplicarse al tratamiento de datos personales por las instituciones y los órganos de la Unión en el ejercicio de sus responsabilidades con arreglo al presente Reglamento. Las disposiciones de la Directiva (UE) 2016/680, del Reglamento (UE) 2016/679 y del Reglamento (CE) n.º 45/2001 deberán especificarse en el presente Reglamento cuando sea necesario. En lo que respecta al tratamiento de datos personales por parte de Europol, se aplicará el Reglamento (UE) 2016/794 sobre la Agencia de la Unión Europea para la Cooperación Policial[53] (Reglamento Europol).

(29) Por lo que respecta a la confidencialidad, a los funcionarios y otros agentes que trabajen en SIS se les aplicarán las disposiciones pertinentes del Estatuto de los funcionarios y el Régimen aplicable a los otros agentes de la Unión Europea.

(30) Tanto los Estados miembros como la Agencia deberán disponer de planes de seguridad para facilitar la aplicación de las obligaciones en materia de seguridad, y deberán cooperar entre sí para abordar las cuestiones de seguridad desde una perspectiva común.

(31) Las autoridades nacionales de control independientes deberán controlar la legalidad del tratamiento de datos personales por los Estados miembros en el marco del presente Reglamento. Deberán establecerse los derechos de los interesados con respecto al acceso, la rectificación y la supresión de sus datos personales almacenados en el SIS y el posterior recurso ante los órganos jurisdiccionales nacionales, así como el reconocimiento mutuo de las resoluciones judiciales. Por tanto, procede solicitar estadísticas anuales a los Estados miembros.

(32) Las autoridades nacionales de supervisión deberán velar por que, al menos cada cuatro años, se lleve a cabo una auditoría de las operaciones de tratamiento de datos en los N.SIS de acuerdo con las normas internacionales de auditoría. La auditoría deberá ser realizada por las autoridades de supervisión, o bien las autoridades nacionales de supervisión deberán ordenar directamente la auditoría a un auditor independiente para

---

50 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.

51 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 la libre circulación de dichos datos, DO L 119 de 4.5.2016, p. 89.

52 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.

53 Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, DO L 135 de 25.5.2016, p. 53.

la protección de datos. El auditor independiente deberá seguir estando bajo el control y la responsabilidad de la autoridad o autoridades nacionales de supervisión que, por tanto, deberán ordenar la propia auditoría y ofrecer una definición clara de su objetivo, alcance y metodología, así como orientaciones y supervisión respecto a las auditorías y sus resultados finales.

(33) El Reglamento (UE) 2016/794 (Reglamento Europol) dispone que Europol apoyará y reforzará las acciones llevadas a cabo por las autoridades competentes de los Estados miembros y su cooperación en la lucha contra el terrorismo y los delitos graves y elaborará análisis y evaluaciones de amenazas. Con el fin de facilitar a Europol el desempeño de sus tareas, en particular en el Centro europeo sobre el tráfico ilícito de migrantes, procede permitir a Europol acceso a las categorías de descripciones definidas en el presente Reglamento. Dicho Centro desempeña un importante papel estratégico para luchar contra la facilitación de la migración irregular, por lo que deberá tener acceso a las descripciones de personas a las que se deniegue la entrada y la estancia en el territorio de un Estado miembro, ya sea por motivos delictivos o por el incumplimiento de las condiciones de entrada y estancia.

(34) Con el fin de colmar la brecha en el intercambio de información en materia de terrorismo, en particular sobre los combatientes terroristas extranjeros (pues el seguimiento de sus movimientos es crucial), los Estados miembros deberán intercambiar información sobre actividades relacionadas con el terrorismo con Europol paralelamente a la introducción de una descripción en el SIS, así como las respuestas positivas y la información relacionada. Esto permitiría al Centro Europeo de Lucha contra el Terrorismo de Europol comprobar si existe información contextual adicional en las bases de datos de Europol y realizar análisis de gran calidad, contribuyendo al desmantelamiento de las redes terroristas y, cuando sea posible, impidiendo sus ataques.

(35) Además, es necesario establecer normas claras para Europol sobre el tratamiento y la descarga de datos del SIS a fin de permitir el más amplio uso del SIS, siempre que se respeten las normas de protección de datos con arreglo a lo dispuesto en el presente Reglamento y en el Reglamento (UE) 2016/794. En caso de que las consultas realizadas por Europol en el SIS revelen la existencia de una descripción emitida por un Estado miembro, Europol no puede adoptar las medidas necesarias. Por consiguiente, deberá informar de ello al Estado miembro en cuestión para que pueda realizar el seguimiento del caso.

(36) A efectos del presente Reglamento, el Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo[54] establece que el Estado miembro de acogida debe autorizar a los miembros de los equipos de la Guardia Europea de Fronteras y Costas o a los equipos de personal implicados en tareas relacionadas con el retorno, desplegados por la Agencia Europea de la Guardia de Fronteras y Costas, a consultar las bases de datos europeas, cuando dicha consulta sea necesaria para cumplir objetivos operativos especificados en el plan operativo sobre controles en las fronteras, vigilancia fronteriza y retorno. Otras agencias de la Unión competentes, especialmente la Oficina Europea de Apoyo al Asilo y Europol, pueden también desplegar expertos en el marco de los equipos de apoyo a la gestión de la migración, que no sean miembros del personal de

[54] 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.

los organismos de la Unión. El objetivo del despliegue de los equipos de la Guardia Europea de Fronteras y Costas, los equipos de personal implicados en tareas relacionadas con el retorno y los equipos de apoyo a la gestión de la migración es reforzar operativa y técnicamente a los Estados miembros que lo soliciten, especialmente a aquellos que se enfrentan a desafíos de migración desproporcionados. El cumplimiento de las tareas asignadas a los equipos de la Guardia Europea de Fronteras y Costas, los equipos de personal implicados en tareas relacionadas con el retorno y los equipos de apoyo a la gestión de la migración, requiere el acceso al SIS a través de una interfaz técnica de la Agencia Europea de la Guardia de Fronteras y Costas conectada al SIS Central. En caso de que las consultas efectuadas por el equipo o los equipos de personal en el SIS revelen la existencia de una descripción emitida por un Estado miembro, el miembro del personal o el equipo no podrá llevar a cabo la medida pertinente a menos que esté autorizado para ello por el Estado miembro de acogida. Por consiguiente, deberá informar de ello a los Estados miembros afectados para permitir el seguimiento del asunto.

(37) De conformidad con el Reglamento (UE) 2016/1624, la Agencia Europea de la Guardia de Fronteras y Costas deberá elaborar análisis de riesgos. Estos análisis deberán abarcar todos los aspectos pertinentes de la gestión integrada de las fronteras europeas, en particular las amenazas que puedan afectar al funcionamiento o a la seguridad de las fronteras exteriores. Las descripciones introducidas en el SIS de conformidad con el presente Reglamento, y en especial las descripciones a efectos de la denegación de entrada y estancia, son información pertinente para evaluar las posibles amenazas que puedan afectar a las fronteras exteriores, por lo que deberán estar disponibles con vistas a los análisis de riesgos que deberá elaborar la Agencia Europea de la Guardia de Fronteras y Costas. El cumplimiento de las tareas asignadas a la Agencia Europea de la Guardia de Fronteras y Costas en relación con el análisis de riesgos requiere el acceso al SIS. Además, en el marco de la propuesta de la Comisión de un Reglamento del Parlamento Europeo y del Consejo por el que se crea un Sistema Europeo de Información y Autorización de Viajes (SEIAV)[55], la unidad central SEIAV de la Agencia Europea de la Guardia de Fronteras y Costas realizará las comprobaciones en el SIS a través del SEIAV con el fin de evaluar las solicitudes de autorización de viaje, lo que requiere, entre otras cosas, determinar si el nacional de un tercer país que solicite una autorización de viaje es objeto de una descripción en el SIS. Para ello, la unidad central SEIAV de la Agencia Europea de la Guardia de Fronteras y Costas también deberá tener acceso al SIS en la medida necesaria con arreglo a su mandato, a saber, a todas las categorías de descripciones sobre nacionales de terceros países respecto de los cuales se haya emitido una descripción a efectos de entrada y estancia, y sobre aquellos que sean objeto de una medida restrictiva destinada a impedir la entrada o el tránsito a través de los Estados miembros.

(38) Debido a su naturaleza técnica, nivel de detalle y necesidad de actualización regular, determinados aspectos del SIS no pueden ser regulados exhaustivamente por las disposiciones del presente Reglamento. Esto incluye, por ejemplo, las normas técnicas sobre introducción, actualización, supresión y consulta de datos, las normas sobre calidad de los datos y las normas de consulta relativas a los identificadores biométricos, las normas sobre compatibilidad y prioridad de las descripciones, la introducción de indicaciones, las conexiones entre descripciones, el establecimiento de la fecha de expiración de descripciones en el plazo máximo y el intercambio de información complementaria. En consecuencia, las competencias de ejecución en estas

---

55 COM(2016) 731 final.

materias deberán delegarse en la Comisión. Las normas técnicas sobre la consulta de descripciones deberán tener en cuenta la necesidad de que las aplicaciones nacionales funcionen con fluidez.

(39) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deberán atribuirse a la Comisión competencias de ejecución. Dichas competencias deberán ejercerse de conformidad con el Reglamento (UE) n.º 182/2011[56]. El procedimiento para la adopción de medidas de ejecución en virtud del presente Reglamento y del Reglamento (UE) 2018/xxx (cooperación policial y judicial) deberá ser el mismo.

(40) A fin de garantizar la transparencia, la Agencia deberá presentar cada dos años un informe sobre el funcionamiento técnico del SIS Central y de la infraestructura de comunicación, así como sobre su seguridad y sobre el intercambio de información complementaria. La Comisión deberá realizar una evaluación general cada cuatro años.

(41) Dado que los objetivos del presente Reglamento, a saber, el establecimiento y regulación de un sistema común de información y el intercambio de información complementaria, no pueden, por su propia naturaleza, ser alcanzados de manera suficiente por los Estados miembros y, por consiguiente, pueden lograrse mejor a nivel de la Unión, la Unión puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar estos objetivos.

(42) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos en particular por la Carta de los Derechos Fundamentales de la Unión Europea. Concretamente, el presente Reglamento aspira a garantizar un entorno seguro para todas las personas que residen en el territorio de la Unión Europea y la protección de los migrantes irregulares frente a la explotación y la trata de seres humanos, permitiendo su identificación a la vez que se respeta plenamente la protección de los datos personales.

(43) 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 TFUE, Dinamarca no participa en la adopción del presente Reglamento y no está vinculada por él ni sujeta a su aplicación. Dado que el presente Reglamento desarrolla el acervo de Schengen, Dinamarca, de conformidad con el artículo 4 de dicho Protocolo, decidirá, en un periodo de seis meses a partir de que el Consejo haya tomado una medida sobre el presente Reglamento, si lo incorpora a su legislación nacional.

(44) El presente Reglamento desarrolla disposiciones del acervo de Schengen en las que el Reino Unido no participa, de conformidad con la Decisión 2000/365/CE del Consejo[57]. El Reino Unido no participa en la adopción del presente Reglamento, que no será vinculante ni aplicable en ese país.

---

56 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.

57 DO L 131 de 1.6.2000, p. 43.

(45) El presente Reglamento desarrolla disposiciones del acervo de Schengen en las que Irlanda no participa, de conformidad con la Decisión 2002/192/CE del Consejo[58]; Irlanda no participa en la adopción del presente Reglamento, que no será vinculante ni aplicable en ese país.

(46) Por lo que se refiere 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 estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen[59], que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE del Consejo[60], relativa a determinadas normas de desarrollo de dicho Acuerdo.

(47) Por lo que se refiere 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, que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE, leído en relación con el artículo 4, apartado 1, de las Decisiones 2004/849/CE[61] y 2004/860/CE del Consejo[62].

(48) Por lo que se refiere 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, aplicación y desarrollo del acervo de Schengen[63], que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE, leído en relación con el artículo 3 de la Decisión 2011/349/UE del Consejo[64] y el artículo 3 de la Decisión 2011/350/UE del Consejo[65].

---

58 DO L 64 de 7.3.2002, p. 20.

59 DO L 176 de 10.7.1999, p. 36.

60 DO L 176 de 10.7.1999, p. 31.

61 Decisión 2004/849/CE del Consejo, de 25 de octubre de 2004, relativa a la firma, en nombre de la Unión Europea, y a la aplicación provisional de determinadas disposiciones del Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de este Estado a la ejecución, aplicación y desarrollo del acervo de Schengen, DO L 368 de 15.12.2004, p. 26.

62 Decisión 2004/860/CE del Consejo, de 25 de octubre de 2004, relativa a la firma, en nombre de la Comunidad Europea, y a la aplicación provisional de determinadas disposiciones del Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de este Estado a la ejecución, aplicación y desarrollo del acervo de Schengen, DO L 370 de 17.12.2004, p. 78.

63 DO L 160 de 18.6.2011, p. 21.

64 Decisión 2011/349/UE del Consejo, de 7 de marzo de 2011, relativa a la celebración, en nombre de la Unión Europea, 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, aplicación y desarrollo del acervo de Schengen, en particular sobre la cooperación judicial en materia penal y la cooperación policial, DO L 160 de 18.6.2011, p. 1.

65 Decisión 2011/350/UE del Consejo, de 7 de marzo de 2011, relativa a la celebración, en nombre de la Unión Europea, 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, aplicación y desarrollo del acervo de Schengen, sobre la supresión de controles en las fronteras internas y la circulación de personas, DO L 160 de 18.6.2011, p. 19.

(49) Por lo que se refiere a Bulgaria y Rumanía, el presente Reglamento constituye un acto que desarrolla o está relacionado con el acervo de Schengen en el sentido definido en el artículo 4, apartado 2, del Acta de adhesión de 2005 y debe leerse conjuntamente con la Decisión 2010/365/UE del Consejo relativa a la aplicación de las disposiciones del acervo de Schengen relativas al Sistema de Información de Schengen en la República de Bulgaria y Rumanía[66].

(50) Por lo que se refiere a Chipre y Croacia, el presente Reglamento constituye un acto que desarrolla o está relacionado con el acervo de Schengen en el sentido, respectivamente, del artículo 3, apartado 2, del Acta de adhesión de 2003 y del artículo 4, apartado 2, del Acta de adhesión de 2011.

(51) Los costes estimados de la actualización del SIS y de los sistemas nacionales, y de la aplicación de las nuevas funcionalidades, previstos en el presente Reglamento, son inferiores al importe restante en la línea presupuestaria para la iniciativa «fronteras inteligentes» en el Reglamento (UE) n.º 515/2014 del Parlamento Europeo y del Consejo[67]. Por consiguiente, el presente Reglamento debe reasignar el importe atribuido para el desarrollo de sistemas de tecnología de la información en apoyo de la gestión de los flujos migratorios en las fronteras exteriores, de conformidad con el artículo 5, apartado 5, letra b), del Reglamento (UE) n.º 515/2014.

(52) Por tanto, procede derogar el Reglamento (CE) n.º 1987/2006.

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

---

66 DO L 166 de 1.7.2010, p. 17.

67 Reglamento (UE) n.º 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, DO L 150 de 20.5.2014, p. 143.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1
Finalidad general del SIS

El SIS tiene por finalidad garantizar un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, incluidos el mantenimiento de la seguridad y el orden públicos y la salvaguardia de la seguridad en el territorio de los Estados miembros, y aplicar las disposiciones del capítulo 2 del título V de la tercera parte del Tratado de Funcionamiento de la Unión Europea relativas a la circulación de personas en dicho territorio, con la ayuda de la información transmitida por este sistema.

Artículo 2
Ámbito de aplicación

1. El presente Reglamento establece las condiciones y los procedimientos de tratamiento de las descripciones de nacionales de terceros países introducidas en el SIS, así como de intercambio de información complementaria y datos adicionales a efectos de la denegación de entrada y estancia en el territorio de los Estados miembros.

2. El presente Reglamento establece también disposiciones sobre la arquitectura técnica del SIS; 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; el tratamiento general de los datos; los derechos de los interesados; y la responsabilidad.

Artículo 3
Definiciones

1. A efectos del presente Reglamento, se entenderá por:

   a) «descripción»: conjunto de datos, incluidos los identificadores biométricos según lo previsto en el artículo 22, introducidos en el SIS que permiten a las autoridades competentes identificar a una persona con vistas a la adopción de una medida específica;

   b) «información complementaria»: información que no forma parte de los datos de una descripción almacenada en el SIS, pero que está relacionada con dicha descripción, que se intercambiará:

      1) a fin de que los Estados miembros puedan consultarse o informarse entre sí al introducir una descripción;

      2) tras la obtención de una respuesta positiva, a fin de poder adoptar una medida adecuada;

      3) cuando no pueda ejecutarse la medida requerida;

      4) al tratar de la calidad de los datos del SIS;

      5) al tratar de la compatibilidad y prioridad de las descripciones;

6) al tratar del ejercicio del derecho de acceso;

c) «datos adicionales»: datos almacenados en el SIS y relacionados con las descripciones del SIS que deben estar inmediatamente a disposición de las autoridades competentes cuando, como resultado de la consulta de este sistema, se localice a personas sobre las cuales se hayan introducido datos en el SIS;

d) «nacional de un tercer país»: cualquier persona que no sea ciudadano de la Unión en el sentido del artículo 20 del TFUE, a excepción de las personas que disfruten de derechos de libre circulación equivalentes a los de los ciudadanos de la Unión en virtud de acuerdos celebrados entre la Unión, o la Unión y sus Estados miembros, por una parte, y terceros países, por otra parte;

e) «datos personales»: toda información sobre una persona física identificada o identificable («interesado»);

f) «persona física identificable»: toda persona cuya identidad pueda determinarse, directa o indirectamente, en concreto mediante elementos identificadores tales como un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos específicos, característicos de su identidad morfológica, fisiológica, genética, psíquica, económica, cultural o social;

g) «tratamiento de datos personales»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

h) «respuesta positiva» en el SIS significa que:

1) un usuario realiza una consulta,

2) la consulta da como resultado la existencia de una descripción introducida por otro Estado miembro en el SIS,

3) los datos relativos a la descripción en el SIS coinciden con los datos utilizados para la consulta, y

4) como consecuencia de la respuesta positiva, se requiere la adopción de nuevas medidas;

i) «Estado miembro emisor»: Estado miembro que ha introducido la descripción en el SIS;

j) «Estado miembro de ejecución»: Estado miembro que adopta las medidas necesarias a raíz de una respuesta positiva;

k) «usuarios finales»: autoridades competentes que consultan directamente la CS-SIS, el N.SIS o una copia técnica de estos;

l) «retorno»: el definido en el artículo 3, punto 3, de la Directiva 2008/115/CE;

m) «prohibición de entrada»: la prohibición de entrada definida en el artículo 3, punto 6, de la Directiva 2008/115/CE;

n) «datos dactiloscópicos»: datos relativos a impresiones dactilares o impresiones palmares que, debido a su carácter único y a los puntos de referencia que

contienen, permiten comparaciones concluyentes y precisas sobre la identidad de una persona;

o) «delitos graves»: los enumerados en el artículo 2, apartados 1 y 2, de la Decisión Marco 2002/584/JAI, de 13 de junio de 2002[68];

p) «delitos de terrorismo»: los delitos con arreglo a la legislación nacional a que se refieren los artículos 1 a 4 de la Decisión Marco 2002/475/JAI de 13 de junio de 2002[69].

Artículo 4
Arquitectura técnica y funcionamiento del SIS

1. El SIS se compondrá de:

a) un sistema central («SIS Central») compuesto por:

– una unidad de apoyo técnico («CS-SIS»), que contendrá la base de datos del SIS;

– una interfaz nacional uniforme («NI-SIS»);

b) un sistema nacional («N.SIS») en cada Estado miembro, compuesto por los sistemas de datos nacionales que se comunican con el SIS Central. El N.SIS contendrá un fichero de datos («copia nacional») con una copia total o parcial de la base de datos del SIS, así como una copia de seguridad del N.SIS; El N.SIS y su copia de seguridad podrán utilizarse simultáneamente para garantizar una disponibilidad ininterrumpida a los usuarios finales;

c) una estructura de comunicación entre la CS-SIS y la NI-SIS («infraestructura de comunicación») que establezca una red virtual codificada dedicada a los datos del SIS y al intercambio de datos entre las Oficinas SIRENE a que se refiere el artículo 7, apartado 2.

2. La introducción, actualización, supresión y consulta de datos del SIS se hará a través de los distintos N.SIS. En el territorio de cada Estado miembro habrá una copia nacional parcial o completa disponible para la realización de consultas automatizadas. La copia nacional parcial contendrá, como mínimo, los datos enumerados en el artículo 20, apartado 2, letras a) a v), del presente Reglamento. No se permitirá la consulta de ficheros de datos del N.SIS de otros Estados miembros.

3. La CS-SIS realizará funciones de supervisión y gestión técnicas y conservará una copia de seguridad de la CS-SIS, capaz de realizar todas las funciones de la CS-SIS principal en caso de fallo de este sistema. La CS-SIS y la CS-SIS de seguridad deberán estar situadas en los dos emplazamientos técnicos de la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia, creada por el Reglamento (UE) n.º 1077/2011[70] («la Agencia»). La CS-SIS o la CS-SIS de seguridad podrán contener una copia

---

68 Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, DO L 190 de 18.7.2002. p. 1.

69 Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, DO L 164 de 22.6.2002, p. 3.

70 Establecida mediante el Reglamento (UE) n.º 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DO L 286 de 1.11.2011, p. 1.

adicional de la base de datos del SIS y podrán utilizarse simultáneamente en operación activa, siempre que cada una de ellas tenga capacidad para tratar todas las transacciones relacionadas con las descripciones del SIS.

4. La CS-SIS prestará los servicios necesarios para la introducción y el tratamiento de datos del SIS, incluida la realización de consultas en la base de datos del SIS. La CS-SIS garantizará:

   a) la actualización en línea de las copias nacionales;

   b) la sincronización y coherencia entre las copias nacionales y la base de datos del SIS;

   c) la inicialización y restauración de las copias nacionales.

   d) una disponibilidad ininterrumpida.

Artículo 5
Costes

1. Los costes de funcionamiento, mantenimiento y ulterior desarrollo del SIS Central y de la infraestructura de comunicación correrán a cargo del presupuesto general de la Unión Europea.

2. Dichos costes incluirán los trabajos realizados en relación con la CS-SIS que garanticen la prestación de los servicios a que se refiere el artículo 4, apartado 4.

3. Los costes de creación, funcionamiento, mantenimiento y ulterior desarrollo de cada N.SIS correrán a cargo del Estado miembro de que se trate.

CAPÍTULO II

RESPONSABILIDADES DE LOS ESTADOS MIEMBROS

Artículo 6
Sistemas nacionales

Cada Estado miembro será responsable de la creación, el funcionamiento, el mantenimiento y el ulterior desarrollo de su N.SIS y de la conexión de su N.SIS a la NI-SIS.

Cada Estado miembro será responsable de asegurar el funcionamiento continuo del N.SIS, su conexión con la NI.SIS y la disponibilidad ininterrumpida de los datos del SIS para los usuarios finales.

Artículo 7
Oficina N.SIS y Oficina SIRENE

1. Cada Estado miembro designará una autoridad («Oficina N.SIS») que asumirá la responsabilidad central respecto de su N.SIS.

   Dicha autoridad será responsable del correcto funcionamiento y la seguridad del N.SIS, garantizará el acceso de las autoridades competentes al SIS y adoptará las medidas necesarias para garantizar el cumplimiento de lo dispuesto en el presente Reglamento. Tendrá la responsabilidad de velar por que todas las funcionalidades del SIS se pongan debidamente a disposición de los usuarios finales.

   Cada Estado miembro transmitirá sus descripciones a través de la Oficina N.SIS.

2. Cada Estado miembro designará a la autoridad encargada de garantizar el intercambio y la disponibilidad de toda la información complementaria («Oficina SIRENE»), de conformidad con las disposiciones que figuran en el Manual SIRENE, según se indica en el artículo 8.

   Esta Oficina coordinará asimismo la verificación de la calidad de la información introducida en el SIS. Para ello, tendrá acceso a los datos tratados en el SIS.

3. Los Estados miembros comunicarán a la Agencia los datos relativos a su Oficina N.SIS II y a su Oficina SIRENE. La Agencia publicará la lista de estas autoridades junto con la lista a la que se refiere el artículo 36, apartado 8.

Artículo 8
Intercambio de información complementaria

1. La información complementaria se intercambiará de conformidad con las disposiciones del Manual SIRENE y a través de la infraestructura de comunicación. Los Estados miembros aportarán los recursos personales y técnicos necesarios para garantizar la disponibilidad continua y el intercambio de información complementaria. En caso de fallo del funcionamiento de la infraestructura de comunicación, los Estados miembros podrán emplear otros medios técnicos dotados de características adecuadas de seguridad para intercambiar información complementaria.

2. La información complementaria se utilizará únicamente para el fin para el que haya sido transmitida de conformidad con el artículo 43, a menos que se haya obtenido el consentimiento previo del Estado miembro emisor.

3. Las Oficinas SIRENE llevarán a cabo su cometido de manera rápida y eficiente, en particular respondiendo a una solicitud lo antes posible, y como máximo 12 horas después de la recepción de la misma.

4. Se adoptarán normas detalladas para el intercambio de información complementaria a través de medidas de ejecución con arreglo al procedimiento de examen contemplado en el artículo 55, apartado 2, en forma de un manual denominado «Manual SIRENE».

Artículo 9
Conformidad técnica y operativa

1. Al establecer su N.SIS, cada Estado miembro deberá ajustarse a las normas comunes, protocolos y procedimientos técnicos establecidos para garantizar la compatibilidad de su N-SIS con la CS-SIS para la transmisión rápida y eficaz de los datos. Dichas normas comunes, protocolos y procedimientos técnicos deberán establecerse y desarrollarse a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 55, apartado 2.

2. Los Estados miembros se asegurarán, mediante los servicios prestados por la CS-SIS, de que los datos almacenados en la copia nacional son, por medio de las actualizaciones automáticas mencionadas en el artículo 4, apartado 4, idénticos a los de la base de datos del SIS y coherentes con ellos, y de que una consulta en su copia nacional genere un resultado equivalente al de una consulta en la base de datos del SIS. Los usuarios finales recibirán los datos necesarios para llevar a cabo sus tareas, en particular todos los necesarios para la identificación del interesado y para adoptar las medidas necesarias.

Artículo 10
Seguridad - Estados miembros

1. Cada Estado miembro adoptará, en lo referente a su N.SIS, las medidas adecuadas, incluido 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 que cualquier persona no autorizada acceda a las instalaciones utilizadas para el tratamiento de datos de carácter personal (control en la entrada de las instalaciones);

   c) impedir que los soportes de datos puedan ser leídos, copiados, modificados o suprimidos por personas no autorizadas (control de los soportes de datos);

   d) impedir la introducción no autorizada de datos y la inspección, modificación o supresión no autorizadas de datos personales almacenados (control del almacenamiento);

   e) impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de los usuarios);

   f) garantizar que, para la utilización de un sistema de tratamiento automatizado de datos, las personas autorizadas solo puedan tener acceso a los datos que sean de su competencia y ello únicamente con identificaciones de usuario personales e intransferibles y con modos de acceso confidenciales (control de acceso a los datos);

   g) garantizar que todas las autoridades con derecho de acceso al SIS o a las instalaciones utilizadas para el tratamiento de datos establezcan perfiles que describan las funciones y responsabilidades de las personas autorizadas a acceder a los datos, y a introducir, actualizar, suprimir y consultar dichos datos, y los pongan a disposición de las autoridades nacionales de control a que se refiere el artículo 50, apartado 1, sin dilación a petición de estas (perfiles del personal);

   h) garantizar la posibilidad de verificar y determinar a qué autoridades pueden ser transmitidos datos de carácter personal a través de equipos de transmisión de datos (control de la comunicación);

   i) garantizar que pueda verificarse y comprobarse *a posteriori* qué datos de carácter personal se han introducido en el sistema de tratamiento automatizado de datos, en qué momento, por qué persona y para qué fines han sido introducidos (control de la introducción);

   j) impedir, en particular mediante técnicas adecuadas de criptografiado, que en el momento de la transferencia de datos de carácter personal y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

   k) controlar la eficacia de las medidas de seguridad mencionadas en el presente apartado y adoptar las medidas necesarias de organización relativas al control interno (auditoría interna).

2. Los Estados miembros tomarán medidas equivalentes a las mencionadas en el apartado 1 en materia de seguridad en relación con el tratamiento y el intercambio de

información complementaria, en particular para garantizar la seguridad de las instalaciones de la Oficina SIRENE.

3. Los Estados miembros tomarán medidas equivalentes a las mencionadas en el apartado 1 en materia de seguridad en relación con el tratamiento de los datos del SIS por las autoridades mencionadas en el artículo 29.

Artículo 11
Confidencialidad – Estados miembros

Cada Estado miembro aplicará sus normas sobre secreto profesional u otras obligaciones equivalentes de confidencialidad a toda persona y organismo que vaya a trabajar con datos del SIS y con información complementaria, 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.

Artículo 12
Registros nacionales

1. Los Estados miembros velarán por que todo acceso a datos personales y todos los intercambios de los mismos en la CS-SIS queden registrados en su N.SIS, con el fin de que se pueda controlar la legalidad de la consulta y del tratamiento de datos, proceder a un control interno y garantizar el correcto funcionamiento del N.SIS y la integridad y seguridad de los datos.

2. Los registros contendrán, en particular, el historial de las descripciones, la fecha y hora de la actividad de tratamiento de los datos, el tipo de datos utilizados para realizar una consulta, la referencia al tipo de datos transmitidos y los nombres de la autoridad competente y de la persona responsable del tratamiento de los datos.

3. Si la consulta se realiza con datos dactiloscópicos o imágenes faciales de conformidad con el artículo 22, los registros mostrarán, en particular, el tipo de datos utilizados para realizar una consulta, la referencia al tipo de datos transmitidos y los nombres de la autoridad competente y de la persona responsable del tratamiento de los datos.

4. Los registros solo podrán utilizarse para los fines a que se refiere el apartado 1 y se suprimirán en un plazo mínimo de un año y máximo de tres años después de su creación.

5. Los registros podrán conservarse más tiempo si son necesarios para procedimientos de control ya en curso.

6. Las autoridades nacionales competentes encargadas de controlar la legalidad de la consulta y del tratamiento de datos, de proceder a un control interno y de garantizar el correcto funcionamiento del N.SIS y la integridad y seguridad de los datos, tendrán acceso a dichos registros, dentro de los límites de sus competencias y previa petición, a fin de poder desempeñar sus funciones.

Artículo 13
Control interno

Los Estados miembros velarán por que toda autoridad habilitada para acceder a los datos del SIS tome las medidas necesarias para garantizar el cumplimiento del presente Reglamento y coopere, en caso necesario, con la autoridad nacional de control.

Artículo 14
Formación del personal

Antes de ser autorizado a tratar los datos almacenados en el SIS, y periódicamente tras la concesión del acceso a los datos del SIS, el personal de las autoridades con derecho de acceso al SIS recibirá la formación adecuada sobre seguridad de los datos, normas de protección de datos y los procedimientos para el tratamiento de datos con arreglo a lo dispuesto en el Manual SIRENE. El personal será informado de los delitos y sanciones penales pertinentes.

CAPÍTULO III

COMPETENCIAS DE LA AGENCIA

Artículo 15
Gestión operativa

1. La Agencia será responsable de la gestión operativa del SIS Central. La Agencia se asegurará, en cooperación con los Estados miembros, de que en el SIS Central se utilice en todo momento la mejor tecnología disponible, sobre la base de un análisis de costes y beneficios.

2. La Agencia será responsable asimismo de las siguientes funciones relacionadas con la infraestructura de comunicación:

   a) supervisión;

   b) seguridad;

   c) coordinación de las relaciones entre los Estados miembros y el proveedor.

3. La Comisión será responsable de todas las demás funciones relacionadas con la infraestructura de comunicación, a saber:

   a) ejecución del presupuesto;

   b) adquisición y renovación;

   c) cuestiones contractuales.

4. La Agencia será responsable asimismo de las siguientes funciones relacionadas con las Oficinas SIRENE y la comunicación entre las Oficinas SIRENE:

   a) coordinación y gestión de pruebas;

   b) mantenimiento y actualización de las especificaciones técnicas relativas al intercambio de información complementaria entre las Oficinas SIRENE y la infraestructura de comunicación y la gestión del impacto de los cambios técnicos cuando afecten al SIS y al intercambio de información complementaria entre las Oficinas SIRENE.

5. La Agencia desarrollará y mantendrá un mecanismo y procedimientos para realizar controles de calidad de los datos de la CS-SIS y presentará informes regulares a los Estados miembros. La Agencia presentará a la Comisión un informe periódico sobre los problemas encontrados y los Estados miembros afectados. Este mecanismo, los procedimientos y la interpretación del cumplimiento de los normas de calidad de los datos deberán establecerse y desarrollarse a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 55, apartado 2.

6. La gestión operativa del SIS Central consistirá en todas las funciones necesarias para mantenerlo en funcionamiento ininterrumpido, de conformidad con el presente Reglamento y, en particular, en el trabajo de mantenimiento y de adaptación técnica necesario para el buen funcionamiento del sistema. Estas tareas incluyen asimismo actividades de prueba que garanticen que el SIS Central y los sistemas nacionales funcionan con arreglo a los requisitos técnicos y operativos de conformidad con lo dispuesto en el artículo 9 del presente Reglamento.

Artículo 16
Seguridad

1. La Agencia adoptará las medidas necesarias, incluido un plan de seguridad, un plan de continuidad de las actividades y un plan de recuperación en caso de catástrofe para el SIS Central y la infraestructura de comunicación 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 que cualquier persona no autorizada acceda a las instalaciones utilizadas para el tratamiento de datos de carácter personal (control en la entrada de las instalaciones);

c) impedir que los soportes de datos puedan ser leídos, copiados, modificados o suprimidos por personas no autorizadas (control de los soportes de datos);

d) impedir la introducción no autorizada de datos y la inspección, modificación o supresión no autorizadas de datos personales almacenados (control del almacenamiento);

e) impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de los usuarios);

f) garantizar que, para la utilización de un sistema de tratamiento automatizado de datos, las personas autorizadas solo puedan tener acceso a los datos que sean de su competencia y ello únicamente con identificaciones de usuario personales e intransferibles y con modos de acceso confidenciales (control de acceso a los datos);

g) establecer perfiles que describan las funciones y responsabilidades de las personas autorizadas a acceder a los datos o a las instalaciones de tratamiento de datos, y ponerlos a disposición del Supervisor Europeo de Protección de Datos a que se refiere el artículo 51, sin dilación a petición de este (perfiles del personal);

h) garantizar la posibilidad de verificar y determinar a qué autoridades pueden ser transmitidos datos de carácter personal a través de equipos de transmisión de datos (control de la comunicación);

i) garantizar que pueda verificarse y comprobarse *a posteriori* qué datos de carácter personal se han introducido en el sistema de tratamiento automatizado de datos, en qué momento y por qué persona han sido introducidos (control de la introducción);

j) impedir, en particular mediante técnicas adecuadas de criptografiado, que, en el momento de la transferencia de datos de carácter personal y durante el

transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

k) vigilar la eficacia de las medidas de seguridad a que se refiere el presente apartado y adoptar las medidas de organización que sean necesarias en relación con la supervisión interna, a fin de garantizar el cumplimiento del presente Reglamento (auditoría interna).

2. La Agencia adoptará, en relación con el tratamiento y el intercambio de información complementaria mediante la infraestructura de comunicación, medidas equivalentes a las medidas de seguridad mencionadas en el apartado 1.

Artículo 17
Confidencialidad – Agencia

1. Sin perjuicio del artículo 17 del Estatuto de los funcionarios y el Régimen aplicable a los otros agentes de la Unión Europea, la Agencia aplicará normas adecuadas sobre secreto profesional u otras obligaciones equivalentes de confidencialidad a todo miembro de su personal que trabaje con datos del SIS, a niveles comparables a los previstos en el artículo 11 del presente Reglamento. Esta obligación seguirá siendo aplicable después del cese en el cargo o el empleo de dichas personas o tras la terminación de sus actividades.

2. La Agencia adoptará medidas equivalentes a las mencionadas en el apartado 1 por lo que se refiere a la confidencialidad con respecto al intercambio de información complementaria a través de la infraestructura de comunicación.

Artículo 18
Registros centrales

1. La Agencia garantizará que todo acceso a datos personales y todo intercambio de datos personales en la CS-SIS queden registrados a los efectos que establece el artículo 12, apartado 1.

2. Los registros contendrán, en particular, el historial de las descripciones, la fecha y hora de transmisión de los datos, los tipos de datos utilizados para realizar una consulta, la referencia al tipo de datos transmitidos y la identificación de la autoridad competente responsable del tratamiento de los datos.

3. Si la consulta se realiza con datos dactiloscópicos o imágenes faciales de conformidad con los artículos 22 y 28, los registros mostrarán, en particular, el tipo de datos utilizados para realizar la consulta, la referencia al tipo de datos transmitidos y los nombres de la autoridad competente y de la persona responsable del tratamiento de los datos.

4. Los registros solo podrán utilizarse para los fines establecidos en el apartado 1 y se suprimirán en un plazo mínimo de un año y máximo de tres años desde de su creación. Los registros que incluyan el historial de las descripciones serán borrados transcurrido un plazo de uno a tres años tras la supresión de las descripciones.

5. Los registros podrán conservarse más tiempo si fueran necesarios para procedimientos de control ya en curso.

6. Las autoridades competentes encargadas de controlar la legalidad de la consulta y del tratamiento de datos, proceder a un control interno y garantizar el correcto funcionamiento de la CS-SIS y la integridad y seguridad de los datos, tendrán acceso

a dichos registros, dentro de los límites de sus competencias y previa solicitud, a fin de poder desempeñar sus funciones.

CAPÍTULO IV

INFORMACIÓN AL PÚBLICO

Artículo 19
Campañas de información del SIS

La Comisión, en cooperación con las autoridades nacionales de control y el Supervisor Europeo de Protección de Datos, realizará periódicamente campañas para informar al público sobre los objetivos del SIS, los datos almacenados, las autoridades con acceso al SIS y los derechos de los interesados. Los Estados miembros, en cooperación con las autoridades nacionales de control, idearán y realizarán las actuaciones necesarias para informar al conjunto de sus ciudadanos sobre el SIS en general.

CAPÍTULO V

DESCRIPCIONES SOBRE NACIONALES DE TERCEROS PAÍSES INTRODUCIDAS A EFECTOS DE DENEGACIÓN DE ENTRADA O DE ESTANCIA

Artículo 20
Categorías de datos

1. Sin perjuicio de lo dispuesto en el artículo 8, apartado 1, ni de las disposiciones del presente Reglamento relativas al almacenamiento de datos adicionales, el SIS incluirá exclusivamente las categorías de datos que facilite cada Estado miembro y que sean necesarios para los fines previstos en el artículo 24.

2. La información sobre las personas descritas solo contendrá los datos siguientes:

   a) apellido(s);

   b) nombre(s);

   c) nombre(s) de nacimiento;

   d) nombres usados con anterioridad y alias;

   e) rasgos físicos particulares, objetivos e inalterables;

   f) lugar de nacimiento;

   g) fecha de nacimiento;

   h) sexo;

   i) nacionalidad(es);

   j) si la persona en cuestión está armada, es violenta, se ha evadido o participa en alguna de las actividades a las que se refieren los artículos 1, 2, 3 y 4 de la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo;

k) motivo de la descripción;

l) autoridad que emite la descripción;

m) referencia a la decisión que haya dado lugar a la introducción de la descripción;

n) medidas que deben adoptarse;

o) conexión o conexiones con otras descripciones introducidas en el SIS de conformidad con el artículo 38;

p) si la persona en cuestión es miembro de la familia de un ciudadano de la UE u otra persona que disfrute de los derechos de libre circulación a que se refiere el artículo 25;

q) si la decisión sobre la denegación de entrada se basa en:

– una condena anterior según lo previsto en el artículo 24, apartado 2, letra a);

– una amenaza grave para la seguridad según lo previsto en el artículo 24, apartado 2, letra b);

– una prohibición de entrada según lo previsto en el artículo 24, apartado 3; o

– una medida restrictiva según lo previsto en el artículo 27;

r) tipo de delito (para las descripciones emitidas con arreglo al artículo 24, apartado 2, del presente Reglamento);

s) tipo de documento de identidad;

t) país de expedición del documento de identidad;

u) número del documento de identidad;

v) fecha de expedición del documento de identidad;

w) fotografías e imágenes faciales;

x) datos dactiloscópicos;

y) fotocopia en color del documento de identidad.

3. Las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en el apartado 2 deberán establecerse y desarrollarse a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 55, apartado 2.

4. Las normas técnicas necesarias para la consulta de los datos mencionados en el apartado 2 deberán establecerse y desarrollarse con arreglo al procedimiento de examen a que se refiere el artículo 55, apartado 2. Estas normas técnicas serán iguales para las consultas en la CS-SIS, en las copias nacionales y en las copias técnicas, según lo mencionado en el artículo 36, y se basarán en normas comunes establecidas y desarrolladas a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 55, apartado 2.

Artículo 21
Proporcionalidad

1. Antes de emitir una descripción y al prorrogar el periodo de validez de la misma, los Estados miembros determinarán si el caso es adecuado, pertinente e importante como para justificar la introducción de la descripción en el SIS.

2. Al aplicar el artículo 24, apartado 2, los Estados miembros deberán crear en todo caso una descripción sobre los nacionales de terceros países si el delito está contemplado en los artículos 1 a 4 de la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo[71].

Artículo 22
Normas específicas para introducir fotografías, imágenes faciales y datos dactiloscópicos

1. Los datos a que se refiere el artículo 20, apartado 2, letras w) y x) solo se introducirán tras ser sometidos a un control para verificar que satisfacen unas normas mínimas de calidad.

2. Se establecerán normas de calidad para el almacenamiento de los datos mencionados en el apartado 1. Dichas normas se establecerán a través de medidas de ejecución y se actualizarán de conformidad con el procedimiento de examen a que se refiere el artículo 55, apartado 2.

Artículo 23
Requisitos para la introducción de una descripción

1. No podrá introducirse una descripción sin los datos a que se refieren el artículo 20, apartado 2, letras a), g), k), m), n) y q). En el caso de que una descripción se base en una decisión adoptada de conformidad con el artículo 24, apartado 2, se introducirán asimismo los datos a que se hace referencia en el artículo 20, apartado 2, letra r).

2. Además, cuando estén disponibles, se introducirán todos los demás datos a los que se refiere el artículo 20, apartado 2.

Artículo 24
Condiciones para la introducción de descripciones a efectos de denegación de entrada y estancia

1. Los datos relativos a los nacionales de terceros países para los que se haya introducido una descripción a efectos de denegación de entrada y estancia se introducirán en el SIS sobre la base de una descripción nacional resultante de una decisión adoptada, observando las normas de procedimiento previstas por la legislación nacional, por las autoridades administrativas o judiciales competentes. Esta decisión solo podrá tomarse sobre la base de una evaluación del caso concreto. Los recursos contra esas decisiones se interpondrán con arreglo a la legislación nacional.

2. Podrá introducirse una descripción cuando la decisión a que se refiere el apartado 1 se base en la amenaza que para el orden público o la seguridad nacional pueda

[71] Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, DO L 164 de 22.6.2002, p. 3.

constituir la presencia de un nacional de un tercer país en el territorio de un Estado miembro. Este será particularmente el caso de:

a) un nacional de un tercer país que haya sido condenado en un Estado miembro por un delito sancionado con una pena privativa de libertad de un año como mínimo;

b) un nacional de un tercer país sobre el cual existan razones fundadas para creer que ha cometido delitos graves, o sobre el cual existan indicios claros de que piensa cometer tales delitos en el territorio de un Estado miembro.

3. Podrá introducirse una descripción cuando la decisión a que se refiere el apartado 1 sea una prohibición de entrada emitida con arreglo a unos procedimientos conformes a la Directiva 2008/115/CE. El Estado miembro emisor deberá garantizar que la descripción surta efecto en el SIS en el punto de retorno del nacional de un tercer país. La confirmación del retorno se comunicará al Estado miembro emisor, de conformidad con el artículo 6 del Reglamento (UE) 2018/xxx [Reglamento sobre retorno].

Artículo 25
Condiciones para la introducción de descripciones de nacionales de terceros países beneficiarios del derecho a la libre circulación en la Unión

1. Una descripción relativa a un nacional de un tercer país beneficiario del derecho de libre circulación en la Unión, en el sentido de la Directiva 2004/38/CE del Parlamento Europeo y del Consejo[72], se introducirá de conformidad con las disposiciones adoptadas en aplicación de dicha Directiva.

2. Si se obtiene una respuesta positiva en relación con una descripción introducida de conformidad con el artículo 24 relativa a un nacional de un tercer país que goce del derecho de libre circulación en la Unión, el Estado miembro de ejecución de la descripción consultará inmediatamente al Estado miembro emisor, mediante el intercambio de información complementaria, para decidir sin dilación la acción que debe emprenderse.

Artículo 26
Procedimiento de consulta

1. Cuando un Estado miembro prevea conceder un permiso de residencia u otra autorización que otorgue un derecho de estancia a un nacional de un tercer país que sea objeto de una descripción de denegación de entrada y estancia introducida por otro Estado miembro, consultará en primer lugar, mediante el intercambio de información complementaria, al Estado miembro que haya introducido la descripción y tendrá en cuenta los intereses de dicho Estado. El Estado miembro emisor deberá responder en el plazo de siete días. Cuando el Estado miembro que prevea conceder un permiso de residencia u otra autorización que otorgue un derecho de estancia decida concederlo, la descripción sobre la denegación de entrada y estancia será suprimida.

2. Cuando un Estado miembro considere introducir una descripción para la denegación de entrada y estancia de un nacional de un tercer país que sea titular de un permiso de residencia válido u otra autorización que otorgue un derecho de estancia expedido

[72] DO L 158 de 30.4.2004, p. 77.

por otro Estado miembro, consultará en primer lugar, mediante el intercambio de información complementaria, al Estado miembro que haya expedido el permiso, y tendrá en cuenta los intereses de dicho Estado. El Estado miembro que haya expedido el permiso deberá responder en el plazo de siete días. Si el Estado miembro que haya expedido el permiso decide mantenerlo, no se introducirá la descripción a efectos de denegación de entrada y estancia.

3. En caso de obtenerse una respuesta positiva respecto de una descripción para la denegación de entrada y estancia relativa a un nacional de un tercer país que sea titular de un permiso de residencia válido u otra autorización que otorgue un derecho de estancia, el Estado miembro de ejecución consultará inmediatamente al Estado miembro que haya expedido el permiso de residencia y al Estado miembro que haya introducido la descripción, mediante el intercambio de información complementaria, a fin de decidir lo antes posible si deben tomarse medidas. Si se decide mantener el permiso de residencia, se suprimirá la descripción.

4. Los Estados miembros facilitarán anualmente a la Agencia estadísticas sobre las consultas realizadas de conformidad con los apartados 1 a 3.

Artículo 27

Condiciones para la introducción de descripciones de nacionales de terceros países sujetos a medidas restrictivas

1. En la medida en que puedan satisfacerse los requisitos de calidad de los datos, podrán introducirse en el SIS, a efectos de denegación de entrada y estancia, las descripciones de los nacionales de terceros países objeto de una medida restrictiva destinada a impedir la entrada en el territorio de los Estados miembros o el tránsito por él, cuando dicha medida haya sido adoptada de conformidad con actos jurídicos adoptados por el Consejo, incluidas las medidas de aplicación de una prohibición de viajar decidida por el Consejo de Seguridad de las Naciones Unidas.

2. El Estado miembro que deba introducir, actualizar y suprimir dichas descripciones en nombre de todos los Estados miembros será designado en el momento de adoptarse la correspondiente medida, de conformidad con el artículo 29 del Tratado de la Unión Europea. El procedimiento para designar al Estado miembro responsable deberá establecerse y desarrollarse a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 55, apartado 2.

CAPÍTULO VI

CONSULTA MEDIANTE DATOS BIOMÉTRICOS

Artículo 28

Normas específicas para la comprobación o consulta mediante fotografías, imágenes faciales y datos dactiloscópicos

1. Las fotografías, imágenes faciales y datos dactiloscópicos se extraerán del SIS para verificar la identidad de una persona que haya sido localizada como consecuencia de una consulta alfanumérica realizada en el SIS.

2. Los datos dactiloscópicos también podrán utilizarse para identificar a una persona. Los datos dactiloscópicos almacenados en el SIS se utilizarán a tal efecto si la identidad de la persona no pueda determinarse por otros medios.

3. Los datos dactiloscópicos almacenados en el SIS por lo que respecta a las descripciones emitidas con arreglo al artículo 24 también podrán consultarse con conjuntos completos o incompletos de impresiones dactilares o impresiones palmares descubiertas en los lugares de los delitos investigados y cuando pueda demostrarse con un alto grado de probabilidad que pertenecen al autor del delito, siempre y cuando las autoridades competentes no puedan establecer la identidad de la persona utilizando cualquier otra base de datos nacional, europea o internacional.

4. Tan pronto como sea técnicamente posible y, al tiempo que se garantiza un alto nivel de fiabilidad de la identificación, podrán utilizarse fotografías e imágenes faciales para identificar a una persona. La identificación basada en fotografías o imágenes faciales solo podrá utilizarse en los pasos fronterizos regulares en los que se utilicen sistemas de autoservicio y sistemas automatizados de control de fronteras.

CAPÍTULO VII

DERECHO DE ACCESO Y PERIODO DE CONSERVACIÓN DE LAS DESCRIPCIONES

Artículo 29
Autoridades con derecho de acceso a las descripciones

1. El acceso a los datos integrados en el SIS y el derecho a consultarlos, directamente o mediante una copia, estará reservado a las autoridades competentes de la identificación de nacionales de terceros países a efectos de:

   a) los controles fronterizos, de conformidad con el 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 (Código de fronteras Schengen);

   b) las comprobaciones de policía y de aduanas realizadas en el Estado miembro de que se trate, así como su coordinación por las autoridades designadas;

   c) otras actividades policiales que tengan por objeto la prevención, detección e investigación de delitos en el Estado miembro de que se trate;

   d) el examen de las condiciones y la toma de decisiones relativas a la entrada y estancia de nacionales de terceros países en el territorio de los Estados miembros, en particular sobre los permisos de residencia y visados para estancias de larga duración, y sobre el retorno de nacionales de terceros países;

   e) el examen de las solicitudes de visado y la toma de decisiones relativas a dichas solicitudes, incluidas las decisiones de anulación, retirada o prórroga de visados, de conformidad con el Reglamento (UE) n.º 810/2009 del Parlamento Europeo y del Consejo[73].

2. A efectos del artículo 24, apartados 2 y 3, y del artículo 27, el derecho de acceso a los datos introducidos en el SIS y el derecho a consultarlos directamente podrán ser ejercidos asimismo por las autoridades judiciales nacionales, incluidas las autoridades competentes para incoar el proceso penal y la instrucción judicial previa

[73] Reglamento (CE) n.º 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un código comunitario sobre visados (Código de visados), DO L 243 de 15.9.2009, p. 1.

a una acusación, en el desempeño de sus funciones, con arreglo a lo dispuesto en la legislación nacional, así como por sus autoridades de coordinación.

3. El derecho de acceso a los datos relativos a documentos referentes a personas introducidos de conformidad con el artículo 38, apartado 2, letras j) y k), del Reglamento (UE) 2018/xxx (cooperación policial y judicial en materia penal), así como el derecho a consultarlos, podrán también ser ejercidos por las autoridades a que se refiere el apartado 1, letra d). El acceso a los datos por parte de dichas autoridades estará regulado por la legislación nacional de cada Estado miembro.

4. Las autoridades a que se refiere el presente artículo estarán incluidas en la lista a que se refiere el artículo 36, apartado 8.

Artículo 30
Acceso de Europol a los datos del SIS

1. La Agencia de la Unión Europea para la Cooperación Policial (Europol) tendrá derecho, con arreglo a su mandato, a acceder y consultar los datos introducidos en el SIS.

2. En caso de que una consulta efectuada por Europol revele la existencia de una descripción en el SIS, Europol informará al Estado miembro emisor a través de los canales establecidos por el Reglamento (UE) 2016/794.

3. El uso de la información obtenida en una consulta del SIS estará sujeto al consentimiento del Estado miembro de que se trate. Si este permite el uso de dicha información por parte de Europol, su tratamiento se regirá por el Reglamento (UE) 2016/794. Europol solamente podrá transmitir esta información a terceros países u organismos con el consentimiento del Estado miembro de que se trate.

4. Europol podrá solicitar más información a los Estados miembros en cuestión de conformidad con lo dispuesto en el Reglamento (UE) 2016/794.

5. Europol deberá:

   a) sin perjuicio de los apartados 3, 4 y 6, abstenerse de conectar las partes del SIS a las que acceda, de transferir los datos contenidos en las mismas a ningún sistema informático de recopilación y tratamiento de datos gestionado por Europol o que se halle en sus locales, y de descargar o copiar de cualquier manera parte alguna del SIS;

   b) limitar el acceso a los datos introducidos en el SIS al personal de Europol expresamente autorizado para ello;

   c) adoptar y aplicar las medidas contempladas en los artículos 10 y 11;

   d) permitir que el Supervisor Europeo de Protección de Datos controle las actividades de Europol en el ejercicio de su derecho a acceder a los datos introducidos en el SIS y a consultarlos.

6. Los datos solo podrán copiarse con fines técnicos, siempre que sea necesario para la consulta directa por el personal autorizado de Europol. Las disposiciones del presente Reglamento se aplicarán a esas copias. La copia técnica se utilizará con fines de almacenamiento de datos del SIS, mientras se consultan dichos datos. Una vez los datos hayan sido consultados, deberán suprimirse. Estos usos no se interpretarán como descargas ilegales o copia de datos del SIS. Europol no deberá copiar datos de las descripciones ni datos adicionales emitidos por Estados miembros o de la CS-SIS a otros sistemas de Europol.

7. Las copias mencionadas en el apartado 6 que den lugar a bases de datos fuera de línea, solo podrán conservarse un periodo máximo de 48 horas. Dicho periodo podrá prorrogarse en caso de una emergencia hasta que concluya la misma. Europol deberá comunicar toda prórroga al Supervisor Europeo de Protección de Datos.

8. Europol podrá recibir y tratar información complementaria sobre las descripciones correspondientes introducidas en el SIS siempre que las normas de tratamiento de datos mencionadas en los apartados 2 a 7 se apliquen adecuadamente.

9. A fin de verificar la legalidad del tratamiento de datos, el control interno y la adecuada integridad y seguridad de los datos, Europol deberá conservar un registro de cada acceso y consulta en el SIS. Los registros y la documentación no se considerarán copias o descargas ilegales de parte alguna del SIS.

Artículo 31

Acceso a los datos del SIS por parte de los equipos de la Guardia Europea de Fronteras y Costas, de los equipos de personal implicados en tareas relacionadas con el retorno y de los miembros de los equipos de apoyo a la gestión de la migración

1. De conformidad con el artículo 40, apartado 8, del Reglamento (UE) 2016/1624, los miembros de los equipos de la Guardia Europea de Fronteras y Costas o de los equipos de personal implicados en tareas relacionadas con el retorno, así como los miembros de los equipos de apoyo a la gestión de la migración tendrán derecho a acceder y consultar datos introducidos en el SIS con arreglo a su mandato.

2. Los miembros de los equipos de la Guardia Europea de Fronteras y Costas o de los equipos de personal implicados en tareas relacionadas con el retorno, así como los miembros de los equipos de apoyo a la gestión de la migración podrán acceder y consultar los datos introducidos en el SIS de conformidad con el apartado 1 a través de la interfaz técnica elaborada y mantenida por la Agencia Europea de la Guardia de Fronteras y Costas según lo previsto en el artículo 32, apartado 2.

3. Cuando una consulta efectuada por un miembro de los equipos de la Guardia Europea de Fronteras y Costas o de los equipos de personal implicados en tareas relacionadas con el retorno o de los equipos de apoyo a la gestión de la migración revele la existencia de una descripción en el SIS, se informará al Estado miembro de emisión. De conformidad con el artículo 40 del Reglamento (UE) 2016/1624, los miembros de los equipos solo podrán actuar en respuesta a una descripción en el SIS siguiendo las instrucciones, y por regla general, en presencia de agentes de la guardia de fronteras o del personal participante en tareas relacionadas con el retorno, de un Estado miembro de acogida en el que estén actuando. El Estado miembro de acogida podrá autorizar a los miembros de los equipos para que actúen en su nombre.

4. Cada acceso y cada consulta que efectúe un miembro de los equipos de la Guardia Europea de Fronteras y Costas o de los equipos de personal implicados en tareas relacionadas con el retorno o de los equipos de apoyo a la gestión de la migración serán registrados de conformidad con lo dispuesto en el artículo 12, así como toda utilización que hayan hecho de los datos a los que hayan accedido.

5. El acceso a los datos introducidos en el SIS se limitará a un miembro de los equipos de la Guardia Europea de Fronteras y Costas o de los equipos de personal implicados en tareas relacionadas con el retorno o de los equipos de apoyo a la gestión de la migración y no se extenderá a ningún otro miembro del equipo.

6. Se adoptarán y aplicarán las medidas para garantizar la seguridad y la confidencialidad contempladas en los artículos 10 y 11.

Artículo 32

Acceso a los datos del SIS por parte de la Agencia Europea de la Guardia de Fronteras y Costas

1. La Agencia Europea de la Guardia de Fronteras y Costas, con el fin de analizar las amenazas que puedan afectar al funcionamiento o a la seguridad de las fronteras exteriores, podrá acceder y consultar los datos introducidos en el SIS, de conformidad con los artículos 24 y 27.

2. A efectos del artículo 31, apartado 2, y del apartado 1 del presente artículo, la Agencia Europea de la Guardia de Fronteras y Costas creará y mantendrá una interfaz técnica que permita una conexión directa al SIS Central.

3. Cuando una consulta efectuada por la Agencia Europea de la Guardia de Fronteras y Costas revele la existencia de una descripción en el SIS, informará de ello al Estado miembro emisor.

4. A efectos del cumplimiento de las funciones que le confiere el Reglamento por el que se crea un Sistema Europeo de Información y Autorización de Viajes (SEIAV), la Agencia Europea de la Guardia de Fronteras y Costas tendrá derecho a acceder y consultar los datos introducidos en el SIS, de conformidad con los artículos24 y 27.

5. Cuando una verificación realizada por la Agencia Europea de la Guardia de Fronteras y Costas a efectos del apartado 2 revele la existencia de una descripción en el SIS, será aplicable el procedimiento contemplado en el artículo 22 del Reglamento por el que se crea un Sistema Europeo de Información y Autorización de Viajes (SEIAV).

6. Nada en el presente artículo deberá interpretarse en el sentido de que afecta a las disposiciones del Reglamento (UE) 2016/1624 por lo que respecta a la protección de datos y a la responsabilidad por el tratamiento no autorizado o incorrecto de esos datos por parte de la Agencia Europea de la Guardia de Fronteras y Costas.

7. Cada acceso y cada consulta que efectúe la Agencia Europea de la Guardia de Fronteras y Costas serán registrados de conformidad con lo dispuesto en el artículo 12, así como la utilización que haga la Agencia Europea de la Guardia de Fronteras y Costas de los datos a los que haya accedido.

8. Salvo cuando sea necesario para realizar las tareas a efectos del Reglamento por el que se crea un Sistema Europeo de Información y Autorización de Viajes (SEIAV), ninguna parte del SIS deberá estar conectada a ningún sistema informático de tratamiento y recopilación de datos gestionado por la Agencia Europea de la Guardia de Fronteras y Costas, ni los datos contenidos en el SIS a los que la Agencia Europea de la Guardia de Fronteras y Costas tenga acceso se transferirán a dicho sistema. No se descargará ninguna parte del SIS. El registro de los accesos y consultas no se considerará descarga o copia de los datos del SIS.

9. Se adoptarán y aplicarán las medidas para garantizar la seguridad y la confidencialidad contempladas en los artículos 10 y 11.

Artículo 33

Alcance del acceso

Los usuarios finales, en particular Europol, y Agencia Europea de la Guardia de Fronteras y Costas, podrán acceder únicamente a los datos que precisen para el cumplimiento de sus funciones.

Artículo 34
Periodo de conservación de las descripciones

1. Las descripciones de personas introducidas en el SIS con arreglo al presente Reglamento solo se conservarán durante el tiempo necesario para alcanzar los fines para los que hayan sido introducidas.

2. En un plazo máximo de cinco años tras la introducción de una descripción en el SIS, el Estado miembro que la haya introducido examinará la necesidad de mantenerla.

3. Cada Estado miembro fijará, cuando corresponda, unos plazos de examen más cortos con arreglo a su legislación nacional.

4. En los casos en que resulte evidente para el personal de la Oficina SIRENE responsable de la coordinación y el control de la calidad de los datos, que una descripción sobre una persona ha cumplido su objetivo y debe suprimirse del SIS, deberá notificarlo a la autoridad que haya creado la descripción. La autoridad dispondrá de un plazo de 30 días naturales desde de la recepción de esta notificación para indicar que la descripción se ha suprimido o se suprimirá, o para motivar su conservación. Si expira el plazo de 30 días sin respuesta, el personal de la Oficina SIRENE suprimirá la descripción. Las Oficinas SIRENE comunicarán los problemas recurrentes en este ámbito a las autoridades nacionales de control.

5. El Estado miembro emisor podrá decidir durante el plazo de examen, tras una evaluación individual del caso concreto de la que deberá quedar constancia, que se prorrogue la descripción, siempre que ello sea necesario para los fines que motivaron la descripción. En este caso, el apartado 2 se aplicará también a la prórroga. La prórroga de la descripción deberá comunicarse a la CS-SIS.

6. Las descripciones se suprimirán automáticamente una vez transcurrido el periodo de examen a que se refiere el apartado 2, salvo cuando el Estado miembro que haya introducido la descripción haya comunicado la prórroga de la descripción a la CS-SIS, tal como se contempla en el apartado 5. La CS-SIS informará automáticamente a los Estados miembros de la supresión programada de datos del sistema, con un preaviso de cuatro meses.

7. Los Estados miembros llevarán estadísticas del número de descripciones cuyo periodo de conservación se haya prorrogado con arreglo al apartado 5.

Artículo 35
Supresión de las descripciones

1. Las descripciones a efectos de denegación de entrada y estancia con arreglo al artículo 24 se suprimirán cuando la decisión en base a la cual se introdujo la descripción haya sido retirada por la autoridad competente, en su caso siguiendo el procedimiento de consulta indicado en el artículo 26.

2. Las descripciones relacionadas con los nacionales de terceros países objeto de una medida restrictiva contemplada en el artículo 27 se suprimirán cuando la medida que aplique la prohibición de viajar se haya extinguido, suspendido o anulado.

3. Las descripciones de personas que hayan adquirido la ciudadanía de cualquiera de los Estados cuyos nacionales sean beneficiarios del derecho de libre circulación en la Unión serán suprimidas en cuanto el Estado miembro emisor tenga conocimiento, o sea informado con arreglo al artículo 38, de que la persona en cuestión ha adquirido dicha ciudadanía.

CAPÍTULO VIII

NORMAS GENERALES DE TRATAMIENTO DE DATOS

Artículo 36
Tratamiento de los datos del SIS

1. Los Estados miembros podrán tratar los datos contemplados en el artículo 20 a efectos de la denegación de entrada y estancia en sus territorios.

2. Los datos solo podrán copiarse con fines técnicos, siempre que dicha copia sea necesaria para la consulta directa por las autoridades mencionadas en el artículo 29. Las disposiciones del presente Reglamento se aplicarán a esas copias. Un Estado miembro no deberá copiar las descripciones ni datos adicionales introducidos por otro Estado miembro desde su N.SIS o de la CS-SIS a otros ficheros de datos nacionales.

3. Las copias técnicas mencionadas en el apartado 2 que den lugar a bases de datos fuera de línea, solo podrán conservarse un periodo de 48 horas como máximo. Dicho periodo podrá prorrogarse en caso de emergencia hasta que haya finalizado la misma.

   No obstante lo dispuesto en el párrafo primero, las copias técnicas que den lugar a bases de datos fuera de línea para uso de las autoridades responsables de la expedición de visados no estarán permitidas, salvo las copias que se hagan con el único fin de utilizarlas en situaciones de emergencia ante la imposibilidad de acceder a la red durante más de 24 horas.

   Los Estados miembros mantendrán un inventario actualizado de esas copias, pondrán dicho inventario a disposición de las autoridades nacionales de control y se asegurarán de que las disposiciones del presente Reglamento, en particular su artículo 10, se apliquen respecto de dichas copias.

4. El acceso a los datos solo se autorizará dentro de los límites de la competencia de las autoridades nacionales a que se refiere el artículo 29 y al personal debidamente autorizado.

5. Todo tratamiento de la información contenida en el SIS para fines distintos de aquellos para los que se introdujeron deberá estar relacionado con algún caso concreto y justificarse por la necesidad de prevenir una amenaza grave inminente para el orden y la seguridad públicos, por razones graves de seguridad del Estado o con vistas a prevenir un delito grave. A tal fin, deberá obtenerse la autorización previa del Estado miembro emisor.

6. Los datos referentes a los documentos relativos a las personas inscritas con arreglo al artículo 38, apartado 2, letras j) y k), del Reglamento (UE) 2018/xxx podrán ser utilizados por las autoridades a que se refiere el artículo 29, apartado 1, letra d), de conformidad con la legislación nacional de cada Estado miembro.

7. Toda utilización de datos que no sea conforme con los apartados 1 a 6 se considerará como una desviación de la finalidad con arreglo a la legislación nacional de cada Estado miembro.

8. Cada Estado miembro remitirá a la Agencia la lista de las autoridades competentes que estén autorizadas a consultar directamente los datos contenidos en el SIS con arreglo al presente Reglamento, así como cualquier modificación introducida en ella. La lista indicará, para cada autoridad, los datos que puede consultar y para qué fines.

La Agencia garantizará la publicación anual de la lista en el *Diario Oficial de la Unión Europea*.

9. En la medida en que la legislación de la Unión no establezca disposiciones particulares, la legislación de cada Estado miembro se aplicará a los datos introducidos en sus N.SIS respectivos.

Artículo 37
Datos del SIS y ficheros nacionales

1. El artículo 36, apartado 2, se entenderá sin perjuicio del derecho de los Estados miembros a conservar en sus ficheros nacionales datos del SIS en relación con los cuales se haya adoptado una medida en su territorio. Dichos datos se conservarán en los ficheros nacionales durante un periodo máximo de tres años, salvo si la legislación nacional contiene disposiciones específicas que prevean un periodo de conservación más largo.

2. El artículo 36, apartado 2, se entenderá sin perjuicio del derecho de los Estados miembros a conservar en sus ficheros nacionales los datos contenidos en una descripción concreta que hayan introducido en el SIS.

Artículo 38
Información en caso de no ejecución de la descripción

Si no fuera posible ejecutar una medida requerida, el Estado miembro requerido informará de ello inmediatamente al Estado miembro que haya introducido la descripción.

Artículo 39
Calidad de los datos tratados en el SIS

1. El Estado miembro emisor será responsable de la exactitud y actualidad de los datos y de la legalidad de su introducción en el SIS.

2. El Estado miembro emisor será el único autorizado para modificar, completar, rectificar, actualizar o suprimir los datos que haya introducido.

3. Si un Estado miembro distinto del que haya emitido la descripción dispusiera de indicios que hagan presumir que un dato contiene errores de hecho o que ha sido almacenado ilícitamente, informará, mediante el intercambio de información complementaria, al Estado miembro emisor en cuanto sea posible y, a más tardar, 10 días después de que dicha prueba haya llegado a su conocimiento. El Estado miembro emisor comprobará dicha información y, en caso necesario, corregirá o suprimirá ese dato sin demora.

4. Si los Estados miembros no pudieran llegar a un acuerdo en el plazo de dos meses a partir del momento en que se tuvo conocimiento de los elementos de prueba, tal como se describe en el apartado 3, el Estado miembro que no haya emitido la descripción someterá el asunto a las autoridades nacionales de supervisión competentes para que adopten una decisión.

5. Los Estados miembros intercambiarán información complementaria siempre que una persona alegue que no es la persona buscada objeto de la descripción. Si del resultado de la comprobación se desprende que se trata en efecto de dos personas diferentes, se informará al denunciante de las medidas establecidas en el artículo 42.

6. En caso de que una persona ya haya sido objeto de una descripción en el SIS, un Estado miembro que introduzca una nueva descripción deberá ponerse de acuerdo sobre la introducción de la descripción con el Estado miembro que hubiere introducido la primera descripción. El acuerdo se alcanzará mediante el intercambio de información complementaria.

Artículo 40
Incidentes relativos a la seguridad

1. Todo acontecimiento que repercuta o pueda repercutir en la seguridad del SIS y pueda causar un daño al SIS o una pérdida de datos será considerado un incidente relativo a la seguridad, especialmente cuando se haya podido acceder a los datos o cuando se haya puesto o se haya podido poner en peligro la disponibilidad, integridad y confidencialidad de estos.

2. Los incidentes relativos a la seguridad se gestionarán para garantizar una respuesta rápida, efectiva y adecuada.

3. Los Estados miembros notificarán a la Comisión, a la Agencia y al Supervisor Europeo de Protección de Datos los incidentes relativos a la seguridad que se produzcan. La Agencia notificará a la Comisión y al Supervisor Europeo de Protección de Datos los incidentes relativos a la seguridad.

4. La información sobre un incidente relativo a la seguridad que repercuta o pueda repercutir en el funcionamiento del SIS en un Estado miembro o en la Agencia, o en la disponibilidad, integridad y confidencialidad de los datos introducidos o enviados por otros Estados miembros, deberá transmitirse a los Estados miembros y se comunicará de conformidad con el plan de gestión de incidentes facilitado por la Agencia.

Artículo 41
Distinción entre personas con características similares

Cuando, al introducirse una nueva descripción, se ponga de manifiesto que ya hay una persona en el SIS con el mismo elemento descriptivo de identidad, deberá aplicarse el siguiente procedimiento:

a) la Oficina SIRENE se pondrá en contacto con la autoridad solicitante para comprobar si se trata de la misma persona o no;

b) si la comprobación entre la nueva descripción y la persona que ya está en el SIS pone de manifiesto que se trata efectivamente de la misma persona, la Oficina SIRENE aplicará el procedimiento de integración de descripciones múltiples previsto en el artículo 39, apartado 6. Si el resultado de la comprobación indicase que se trata en efecto de dos personas diferentes, la Oficina SIRENE aprobará la solicitud de introducción de la segunda descripción añadiendo los elementos necesarios para evitar cualquier error de identificación.

Artículo 42
Datos adicionales en caso de usurpación de identidad

1. En caso de que pueda surgir confusión entre la persona a la que realmente se refiere una descripción y otra persona cuya identidad haya sido usurpada, el Estado miembro emisor deberá, con el consentimiento expreso de dicha persona, añadir

datos sobre esta a la descripción, a fin de evitar las consecuencias negativas de los errores de identificación.

2. Los datos relacionados con una persona cuya identidad ha sido usurpada solo se utilizarán para los siguientes fines:

   a) permitir a la autoridad competente diferenciar a la persona cuya identidad ha sido usurpada de la persona a la que realmente se refiere la descripción;

   b) permitir a la persona cuya identidad ha sido usurpada demostrar su identidad y establecer que su identidad ha sido usurpada.

3. A efectos del presente artículo, solo podrán introducirse y tratarse en el SIS los siguientes datos personales:

   a) apellido(s)

   b) nombre(s)

   c) apellido(s) de soltera

   d) nombres y apellidos anteriores y alias, en su caso registrados por separado

   e) rasgos físicos particulares, objetivos e inalterables

   f) lugar de nacimiento

   g) fecha de nacimiento

   h) sexo

   i) imágenes faciales

   j) impresiones dactilares

   k) nacionalidad o nacionalidades

   l) categoría de documento de identidad

   m) país de expedición del documento de identidad

   n) número del documento de identidad

   o) fecha de expedición del documento de identidad

   p) dirección de la víctima

   q) nombre del padre de la víctima

   r) nombre de la madre de la víctima

4. Las normas técnicas necesarias para introducir y tratar los datos mencionadas en el apartado 3 deberán establecerse mediante medidas de ejecución establecidas y desarrolladas con arreglo al procedimiento de examen a que se refiere el artículo 55, apartado 2.

5. Los datos a que se refiere el apartado 3 se suprimirán al mismo tiempo que la descripción correspondiente, o antes si la persona lo solicita.

6. Solo las autoridades que tienen derecho de acceso a la descripción correspondiente podrán acceder a los datos a que se refiere el apartado 3. Podrán acceder a ellos únicamente para evitar errores de identificación.

Artículo 43
Conexiones entre descripciones

1. Los Estados miembros podrán crear conexiones entre las descripciones que introduzcan en el SIS. El efecto de estas conexiones será establecer una relación entre dos o más descripciones.

2. La creación de una conexión no afectará a la acción específica que deba emprenderse en función de cada descripción conectada, ni al periodo de conservación de cada una de las descripciones conectadas.

3. La creación de una conexión no afectará a los derechos de acceso regulados en el presente Reglamento. Las autoridades que no tengan derecho de acceso a determinadas categorías de descripciones no podrán ver las conexiones con una descripción a la que no tengan acceso.

4. Los Estados miembros crearán una conexión entre descripciones cuando exista una necesidad operativa.

5. Cuando un Estado miembro considere que la creación por otro Estado miembro de una conexión entre descripciones es incompatible con su legislación nacional o sus obligaciones internacionales, podrá adoptar las medidas necesarias para garantizar que no pueda accederse a la conexión desde su territorio nacional ni por parte de sus propias autoridades nacionales situadas fuera de su territorio.

6. Las normas técnicas para la conexión entre descripciones deberán establecerse y desarrollarse con arreglo al procedimiento de examen definido en el artículo 55, apartado 2.

Artículo 44
Finalidad y periodo de conservación de la información complementaria

1. Los Estados miembros conservarán en la Oficina SIRENE una referencia de las decisiones que han dado lugar a una descripción, a fin de apoyar el intercambio de información complementaria.

2. Los datos personales conservados en ficheros por la Oficina SIRENE como resultado de un intercambio de información solo se conservarán el tiempo que sea necesario para lograr los fines para los que hayan sido facilitados. En cualquier caso, se suprimirán a más tardar un año después de que se haya suprimido del SIS la descripción correspondiente.

3. El apartado 2 se entenderá sin perjuicio del derecho de un Estado miembro a conservar en los ficheros nacionales datos relativos a una descripción particular que dicho Estado miembro haya introducido o a una descripción en relación con la cual se haya emprendido una acción en su territorio. El periodo durante el que podrán conservarse dichos datos en esos ficheros se regirá por la legislación nacional.

Artículo 45
Transferencia de datos personales a terceras partes

Los datos tratados en el SIS y la correspondiente información complementaria con arreglo al presente Reglamento no se transmitirán ni se pondrán a disposición de terceros países ni de organizaciones internacionales.

CAPÍTULO IX

PROTECCIÓN DE DATOS

Artículo 46
Legislación aplicable

1. El Reglamento (CE) n.º 45/2001 se aplicará al tratamiento de datos personales por la Agencia en virtud del presente Reglamento.

2. El Reglamento (UE) 2016/679 se aplicará al tratamiento de datos personales por las autoridades a que se refiere el artículo 29 del presente Reglamento, siempre que no se apliquen las disposiciones nacionales de transposición de la Directiva (UE) 2016/680.

3. Las disposiciones nacionales de transposición de la Directiva (UE) 2016/680 se aplicarán al tratamiento de datos por parte de las autoridades nacionales competentes para fines de prevención, investigación, detección o enjuiciamiento de delitos, o de ejecución de sanciones penales, y en particular para la protección frente a amenazas a la seguridad pública y la prevención de estas.

Artículo 47
Derecho de acceso, rectificación de datos que contengan errores y borrado de datos almacenados ilegalmente

1. El derecho de los interesados a acceder a los datos que se refieran a ellos y que hayan sido introducidos en el SIS, y a que se rectifiquen o borren dichos datos, se ejercerá respetando la legislación del Estado miembro ante el que se hubiere invocado tal derecho.

2. Si la legislación nacional así lo prevé, la autoridad nacional de control decidirá si se facilita información y por qué medios.

3. Un Estado miembro que no sea el Estado emisor no podrá facilitar información relativa a dichos datos, a no ser que previamente hubiere dado al Estado miembro emisor la ocasión de pronunciarse al respecto. Esto se llevará a cabo a través del intercambio de información complementaria.

4. Un Estado miembro adoptará la decisión de no transmitir la información al interesado, en su totalidad o en parte, de conformidad con la legislación nacional, en la medida y siempre que dicha limitación total o parcial constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física en cuestión, con el fin de:

   a) evitar la obstrucción de procedimientos de instrucción, investigaciones o procedimientos;

   b) evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de delitos o la ejecución de sanciones penales;

   c) proteger la seguridad pública;

   d) proteger la seguridad nacional;

   e) proteger los derechos y libertades de otras personas.

5. Se informará al interesado lo antes posible, y en cualquier caso antes de que hayan transcurrido 60 días desde la fecha en que solicitó el acceso, o antes si la legislación nacional así lo dispone.

6. Se informará a la persona interesada lo antes posible del resultado del ejercicio de sus derechos de rectificación y supresión y, en todo caso, en el plazo máximo de tres meses desde la fecha en que solicitó la rectificación o la supresión, o antes si la legislación nacional así lo dispone.

Artículo 48
Derecho de información

1. Los nacionales de terceros países objeto de una descripción introducida con arreglo al presente Reglamento serán informados de ello en virtud de los artículos 10 y 11 de la Directiva 95/46/CE. Esta información se facilitará por escrito, junto con una copia de la decisión nacional que causó la introducción de la descripción, mencionada en el artículo 24, apartado 1, o una referencia a dicha decisión.

2. En ningún caso se facilitará esta información

   a) cuando:

      i) los datos personales no se hayan obtenido del nacional del tercer país en cuestión;

      y

      ii) facilitar esta información resulte imposible o requiera un esfuerzo desproporcionado;

   b) el nacional del país tercero en cuestión ya disponga de la información;

   c) la legislación nacional permita la restricción del derecho de información, en particular para salvaguardar la seguridad nacional, la defensa, la seguridad pública y la prevención, investigación, detección y persecución de delitos.

Artículo 49
Recursos

1. Toda persona podrá emprender acciones ante el órgano jurisdiccional o la autoridad competente en virtud de la legislación nacional de cualquier Estado miembro, para acceder, rectificar, suprimir u obtener información o para obtener una indemnización en relación con una descripción que se refiera a ella.

2. Los Estados miembros se comprometen mutuamente a ejecutar las resoluciones definitivas dictadas por los órganos jurisdiccionales o las autoridades mencionadas en el apartado 1 del presente artículo, sin perjuicio de lo dispuesto en el artículo 53.

3. Con objeto de obtener una visión general coherente del funcionamiento de las vías de recurso, las autoridades nacionales deberán desarrollar un sistema estadístico normalizado para la presentación de informes anuales sobre:

   a) el número de solicitudes de acceso presentadas al responsable del tratamiento de los datos y el número de casos en que se haya concedido el acceso a los datos;

b) el número de solicitudes de acceso presentadas a la autoridad nacional de supervisión y el número de casos en que se haya concedido el acceso a los datos;

c) el número de solicitudes de rectificación de datos inexactos y de borrado de datos introducidos ilegalmente presentadas al responsable del tratamiento de datos, y el número de casos en que los datos se hayan rectificado o borrado;

d) el número de solicitudes de rectificación de datos inexactos y de borrado de datos introducidos ilegalmente presentadas a la autoridad nacional de supervisión;

e) el número de casos que se hayan dirimido en los tribunales;

f) el número de casos en los que el órgano jurisdiccional se haya pronunciado a favor de la parte demandante en cualquier aspecto del asunto;

g) las posibles observaciones sobre casos de reconocimiento mutuo de las resoluciones definitivas dictadas por órganos jurisdiccionales o autoridades de otros Estados miembros sobre descripciones creadas por el Estado miembro emisor.

Los informes de las autoridades nacionales de supervisión se remitirán al mecanismo de cooperación establecido en el artículo 52.

Artículo 50
Supervisión de los N.SIS

1. Cada Estado miembro velará por que las autoridades nacionales de supervisión independientes designadas en cada Estado miembro y dotadas de los poderes mencionados en el anexo VI de la Directiva (UE) 2016/680 y el capítulo VI del Reglamento (UE) 2016/679 supervisen con independencia la legalidad del tratamiento de los datos personales del SIS en su territorio y su transmisión a partir de él, incluido el intercambio y posterior tratamiento de la información complementaria.

2. Las autoridades nacionales de supervisión velarán por que se lleve a cabo una auditoría de las operaciones de tratamiento de datos en los N.SIS de acuerdo con las normas internacionales de auditoría, al menos cada cuatro años. La auditoría será llevada a cabo por las autoridades nacionales de supervisión o dichas autoridades deberán ordenar directamente la auditoría a un auditor independiente para la protección de datos. La autoridad nacional de supervisión mantendrá en todo momento el control y asumirá las responsabilidades del auditor independiente.

3. Los Estados miembros velarán por que la autoridad nacional de supervisión disponga de medios suficientes para desempeñar las funciones que le encomienda el presente Reglamento.

Artículo 51
Supervisión de la Agencia

1. El Supervisor Europeo de Protección de Datos velará por que las actividades de tratamiento de datos personales de la Agencia se lleven a cabo conforme al presente Reglamento. En consecuencia, serán de aplicación las disposiciones sobre funciones y competencias del Supervisor Europeo de Datos previstas en los artículos 46 y 47 del Reglamento (CE) n.º 45/2001.

2. El Supervisor Europeo de Protección de Datos velará por que, al menos cada cuatro años, se lleve a cabo una auditoría de las actividades de tratamiento de datos personales de la Agencia siguiendo normas de auditoría internacionales. El informe de auditoría se enviará al Parlamento Europeo, el Consejo, la Agencia, la Comisión y las autoridades nacionales de supervisión. Deberá darse a la Agencia la oportunidad de formular comentarios antes de que se adopte el informe.

Artículo 52
Cooperación entre las autoridades nacionales de supervisión y el Supervisor Europeo de Protección de Datos

1. Las autoridades nacionales de supervisión y el Supervisor Europeo de Protección de Datos, cada uno dentro del ámbito de sus competencias respectivas, cooperarán activamente en el marco de sus responsabilidades y garantizarán una supervisión coordinada del SIS.

2. Cada una dentro del ámbito de sus competencias respectivas, intercambiarán la información pertinente, se asistirán mutuamente en la realización de inspecciones y auditorías, examinarán las dificultades de interpretación y aplicación del presente Reglamento y otros actos jurídicos aplicables de la Unión, estudiarán los problemas que se planteen en el ejercicio del control independiente o al ejercer sus derechos los interesados, elaborarán propuestas armonizadas para hallar soluciones comunes a los problemas y fomentarán el conocimiento de los derechos en materia de protección de datos, en la medida necesaria.

3. A efectos de lo dispuesto en el apartado 2, las autoridades nacionales de supervisión y el Supervisor Europeo de Protección de Datos se reunirán al menos dos veces al año en el marco del Consejo Europeo de Protección de Datos creado por el Reglamento (UE) 2016/679. Los gastos y la organización de estas reuniones correrán a cargo de la Junta creada por el Reglamento (UE) 2016/679. El Reglamento interno se adoptará en la primera reunión. Los métodos de trabajo se irán desarrollando conjuntamente en función de las necesidades.

4. Cada dos años, la Junta creada por el Reglamento (UE) 2016/679 enviará al Parlamento Europeo, al Consejo y a la Comisión un informe conjunto de actividades en lo que respecta a la supervisión coordinada.

CAPÍTULO X

RESPONSABILIDAD

Artículo 53
Responsabilidad

1. Cada Estado miembro será responsable de todo daño ocasionado a una persona como consecuencia de la utilización del N.SIS. Lo mismo ocurrirá cuando los daños hayan sido causados por el Estado miembro emisor, si este hubiere introducido datos que contengan errores de hecho o los hubiere almacenado ilegalmente.

2. Si el Estado miembro contra el que se entable una acción no fuera el Estado miembro emisor, este último estará obligado a reembolsar, previa petición, las cantidades pagadas en concepto de indemnización, a no ser que los datos hubieren sido utilizados por el Estado miembro que requiera el reembolso incumpliendo el presente Reglamento.

3. Si el incumplimiento por un Estado miembro de las obligaciones que le impone el presente Reglamento causase daños al SIS, dicho Estado será considerado responsable de los daños, salvo en caso de que la Agencia u otro Estado miembro que participe en el SIS no haya adoptado medidas razonables para prevenir los daños o para reducir al mínimo sus efectos.

CAPÍTULO XI

DISPOSICIONES FINALES

Artículo 54
Seguimiento y estadísticas

1. La Agencia garantizará el establecimiento de procedimientos para el control del funcionamiento del SIS en relación con los objetivos, los resultados, la rentabilidad, la seguridad y la calidad del servicio.

2. A efectos de mantenimiento técnico y de elaboración de informes y estadísticas, la Agencia tendrá acceso a la información necesaria relacionada con las operaciones de tratamiento que se realizan en el SIS Central.

3. La Agencia elaborará estadísticas diarias, mensuales y anuales que muestren el número de registros por categoría de descripción, el número de respuestas positivas anuales por categoría de descripción, el número de ocasiones en que se ha consultado el SIS, y el número de ocasiones en que se ha accedido al SIS para introducir, actualizar o suprimir una descripción, en total y para cada Estado miembro, así como estadísticas sobre el procedimiento de consulta mencionado en el artículo 26. Las estadísticas no contendrán datos personales. El informe estadístico anual se publicará.

4. Los Estados miembros, así como Europol y la Agencia Europea de la Guardia de Fronteras y Costas, facilitarán a la Agencia y a la Comisión la información necesaria para elaborar los informes a que se refieren los apartados 7 y 8.

5. La Agencia facilitará a los Estados miembros, la Comisión, Europol y la Agencia Europea de la Guardia de Fronteras y Costas los informes estadísticos que elabore. Con el fin de controlar la aplicación de los actos jurídicos de la Unión, la Comisión podrá solicitar a la Agencia que emita informes estadísticos específicos adicionales, ya sea de forma periódica o *ad hoc*, sobre el funcionamiento o el uso del SIS y de las comunicaciones SIRENE.

6. A efectos de los apartados 3 a 5 del presente artículo y del artículo 15, apartado 5, la Agencia establecerá y alojará un repositorio central en sus centros técnicos que contenga los datos a que se refiere el apartado 3 del presente artículo y el artículo 15, apartado 5; que no permitirá la identificación de los individuos pero sí permitirá a la Comisión y a las agencias a que se refiere el apartado 5 obtener los mencionados informes y estadísticas. La Agencia concederá acceso a los Estados miembros, la Comisión, Europol y la Agencia Europea de la Guardia de Fronteras y Costas al repositorio central por medio de un acceso seguro a través de la infraestructura de comunicación, con control de acceso y perfiles de usuario específicos únicamente a efectos de la presentación de informes y estadísticas.

Deberán establecerse y desarrollarse normas detalladas sobre el funcionamiento del repositorio central y las normas de seguridad y protección de datos aplicables al repositorio, a través de medidas de ejecución adoptadas de conformidad con el procedimiento de examen contemplado en el artículo 55, apartado 2.

7. Transcurridos dos años desde la entrada en funcionamiento del SIS y, a continuación cada dos años, la Agencia presentará al Parlamento Europeo y al Consejo un informe sobre el funcionamiento técnico del SIS Central y la infraestructura de comunicación, incluida su seguridad, y el intercambio bilateral y multilateral de información complementaria entre los Estados miembros.

8. Transcurridos tres años desde la entrada en funcionamiento del SIS, y a continuación cada cuatro años, la Comisión elaborará una evaluación del SIS Central y del intercambio bilateral y multilateral de información complementaria entre los Estados miembros. Dicha evaluación incluirá un examen de los resultados obtenidos en relación con los objetivos, evaluará si los principios básicos siguen siendo válidos, la aplicación del presente Reglamento con respecto al SIS Central, la seguridad del SIS Central, así como cualquier consecuencia de las futuras operaciones. La Comisión remitirá los informes de evaluación al Parlamento Europeo y al Consejo.

Artículo 55
Procedimiento de comité

1. La Comisión estará asistida por 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 56
Modificaciones del Reglamento (UE) n.º 515/2014

El Reglamento (UE) n.º 515/2014[74] queda modificado como sigue:

En el artículo 6, se añade el apartado 6 siguiente:

«6. Durante la fase de desarrollo, los Estados miembros recibirán una asignación adicional de 36,8 millones EUR que se distribuirán mediante un importe a tanto alzado que se añadirá a su asignación básica, y dedicarán esta financiación en su totalidad a los sistemas SIS nacionales para garantizar su rápida y eficaz actualización en consonancia con la aplicación del SIS Central de conformidad con lo dispuesto en el Reglamento (UE) 2018/... [*] y en el Reglamento (UE) 2018/... [**]

[*]Reglamento relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y judicial en materia penal y en el Reglamento (DO...

[**]Reglamento (UE) 2018/... relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas y en el Reglamento (DO ...)».

---

[74] Reglamento (UE) n.º 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, DO L 150 de 20.5.2014, p. 143.

Artículo 57
Derogación

Reglamento (CE) n.º 1987/2006 relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación;

Decisión 2010/261/UE de la Comisión, de 4 de mayo de 2010, relativa al plan de seguridad para el SIS II Central y la infraestructura de comunicación[75].

Artículo 25 del Convenio de aplicación del Acuerdo de Schengen[76].

Artículo 58
Entrada en vigor y aplicabilidad

1. El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

2. Será aplicable a partir de la fecha que fije la Comisión, una vez que:

   a) se hayan adoptado las medidas de aplicación necesarias;

   b) los Estados miembros hayan notificado a la Comisión que han adoptado todas las medidas técnicas y legales necesarias para tratar los datos del SIS e intercambiar la información complementaria de conformidad con el presente Reglamento;

   c) la Agencia haya informado a la Comisión acerca de la realización de todas las actividades de ensayo por lo que respecta a la CS-SIS y a la interacción entre la CS-SIS y el N.SIS.

3. El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro, de conformidad con el Tratado de Funcionamiento de la Unión Europea.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*

[75] Decisión 2010/261/UE de la Comisión, de 4 de mayo de 2010, relativa al plan de seguridad para el SIS II Central y la infraestructura de comunicación, DO L 112 de 5.5.2010, p. 31.

[76] DO L 239 de 22.9.2000, p. 19.

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. Modos de gestión previstos

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. Contribuciones 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, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas y que deroga el Reglamento (CE) n.º 1987/2006.

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA[77]

Ámbito político: Migración y Asuntos de Interior (título 18)

1.3. Naturaleza de la propuesta/iniciativa

☐ 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 prórroga de una acción existente**

☐ La propuesta/iniciativa se refiere a **una acción reorientada hacia una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivo(s) estratégico(s) plurianual(es) de la Comisión contemplado(s) en la propuesta/iniciativa

Objetivo - «Hacia una nueva política sobre migración»

La necesidad de revisar la base jurídica del SIS con el fin de hacer frente a los nuevos retos en materia de seguridad y migración ha sido destacada por la Comisión en repetidas ocasiones. En la «Agenda Europea de Migración»[79], por ejemplo, la Comisión afirmó que la gestión de las fronteras de manera más eficiente implica hacer un mejor uso de las oportunidades que ofrecen las tecnologías y los sistemas informáticos. En la «Agenda Europea de Seguridad»[80], la Comisión anunció su intención de evaluar el SIS en 2015-2016 y estudiar las posibilidades de ayudar a los Estados miembros a aplicar las prohibiciones de viajar establecidas a nivel nacional. En el «Plan de Acción de la UE contra el tráfico ilícito de migrantes»[81], la Comisión indicó que estaba estudiando la posibilidad de que sea obligatorio para las autoridades de los Estados miembros introducir en el SIS todas las prohibiciones de entrada, a fin de permitir su ejecución a escala de la UE. Por otra parte, la Comisión también indicó que estudiaría la posibilidad y la proporcionalidad de introducir las decisiones de retorno dictadas por las autoridades de los Estados miembros para verificar si un migrante irregular interceptado está sujeto a una decisión de retorno dictada por otro Estado miembro. Por último, en la Comunicación «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la

---

77 GPA: gestión por actividades; PPA: presupuestación por actividades.

78 Tal como se contempla en el artículo 54, apartado 2, letras a) o b), del Reglamento Financiero.

79 COM(2015) 240 final.

80 COM(2015) 185 final.

81 COM(2015) 285 final.

seguridad»[82], la Comisión subrayó que estaba explorando posibles funcionalidades adicionales en el SIS con las correspondientes propuestas de revisión de la base jurídica del sistema.

Como resultado de la evaluación global del sistema y en plena consonancia con los objetivos plurianuales de la Comisión, recogidos en las mencionadas Comunicaciones y el Plan estratégico 2016-2020 de la DG de Migración y Asuntos de Interior[83], la presente propuesta tiene por objeto reformar la estructura, funcionamiento y utilización del Sistema de Información de Schengen en el ámbito de las inspecciones fronterizas.

1.4.2. Objetivo(s) específico(s) y actividad(es) GPA/PPA afectada(s)

Objetivo específico n.º

Plan de gestión 2017 de la DG Migración y Asuntos de Interior - Objetivo específico n.º 1.2:

Gestión eficaz de las fronteras - salvar vidas y asegurar las fronteras exteriores de la UE

Actividad(es) GPA/PPA afectada(s)

Capítulo 18 02 - Seguridad interior

82 COM(2016) 205 final.

83 Ares(2016)2231546 – 12.5.2016.

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 principales de la política son los siguientes:

1) contribuir a un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la UE;

2) reforzar la eficacia y la eficiencia de los controles fronterizos;

La evaluación global del SIS, realizada por la DG HOME en 2015-2016, recomendó mejoras técnicas del sistema y la armonización de los procedimientos nacionales en materia de gestión de las denegaciones de entrada y estancia. Por ejemplo, el actual Reglamento SIS II solo permite y no obliga a los Estados miembros a introducir en el sistema descripciones para la denegación de entrada y de estancia. Algunos Estados miembros introducen sistemáticamente todas las prohibiciones de entrada en el SIS, mientras que otros no lo hacen. Por consiguiente, la presente propuesta contribuirá a alcanzar un mayor nivel de armonización en este ámbito, haciendo obligatoria la introducción en el SIS de todas las prohibiciones de entrada, y definirá normas comunes sobre la introducción de las descripciones en el sistema y especificará el motivo que dio lugar a la descripción.

La nueva propuesta introduce medidas que abordan las necesidades operativas y técnicas de los usuarios finales. En particular, nuevos campos de datos para las descripciones existentes permitirán a la guardia de fronteras disponer de toda la información necesaria para llevar a cabo sus tareas eficazmente. Por otra parte, la propuesta hace especial hincapié en la importancia de la disponibilidad ininterrumpida del SIS, dado que los periodos de no funcionamiento pueden tener una incidencia significativa en la capacidad para realizar controles en las fronteras exteriores. Por tanto, la presente propuesta tendrá un efecto muy positivo en la eficacia de los controles fronterizos.

Una vez adoptadas y aplicadas, estas propuestas también reforzarán la continuidad de las actividades. Los Estados miembros estarán obligados a tener una copia de seguridad total o parcial. Esto permitirá que el sistema siga siendo plenamente funcional y operativo para los agentes sobre el terreno.

1.4.4. Indicadores de resultados e incidencia

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

Durante la actualización del sistema

Tras la aprobación del proyecto de propuesta y la adopción de las especificaciones técnicas, el SIS se actualizará para armonizar mejor los procedimientos nacionales para su uso, ampliar el ámbito de aplicación del régimen mediante la mejora de los niveles de información a disposición de los usuarios finales a fin de informar mejor a los agentes que realizan los controles, e introducir cambios técnicos para mejorar la seguridad y ayudar a reducir las cargas administrativas. eu-LISA coordinará la gestión del proyecto de modernización del sistema, establecerá una estructura de gestión del proyecto y propondrá un calendario detallado con objetivos intermedios para la aplicación de los cambios propuestos que permitirá a la Comisión seguir de cerca la aplicación de la propuesta.

Objetivo específico – Entrada en funcionamiento de las funcionalidades actualizadas del SIS en 2020

Indicador – Conclusión con éxito del ensayo global previo al lanzamiento del sistema revisado.

Una vez el sistema esté operativo

Una vez el sistema esté operativo, eu-LISA garantizará el establecimiento de procedimientos para el control del funcionamiento del SIS en relación con los objetivos, los resultados, la rentabilidad, la seguridad y la calidad del servicio. Transcurridos dos años desde la entrada en funcionamiento del SIS, y a continuación cada dos años, eu-LISA deberá presentar al Parlamento Europeo y al Consejo un informe sobre el funcionamiento técnico del SIS Central y la infraestructura de comunicación, incluida su seguridad, el intercambio bilateral y multilateral de información complementaria entre los Estados miembros. Además, eu-LISA elaborará estadísticas diarias, mensuales y anuales que muestren el número de registros por categoría de descripción, el número de respuestas positivas anuales por categoría de descripción, el número de ocasiones en que se ha consultado el SIS, y el número de ocasiones en que se ha accedido al sistema para introducir, actualizar o suprimir una descripción, en total y para cada Estado miembro.

Transcurridos tres años desde la entrada en funcionamiento del SIS, y a continuación cada cuatro años, la Comisión elaborará una evaluación del SIS Central y del intercambio bilateral y multilateral de información complementaria entre los Estados miembros. Esta evaluación incluirá un examen de los resultados obtenidos en relación con los objetivos, evaluará si los principios básicos siguen siendo válidos, la aplicación del presente Reglamento con respecto al SIS Central, la seguridad del SIS Central, así como cualquier consecuencia de las futuras operaciones. La Comisión remitirá la evaluación al Parlamento Europeo y al Consejo.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo

1. Contribuir al mantenimiento de un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la UE.

2. Reforzar la lucha contra la delincuencia internacional, el terrorismo y otras amenazas para la seguridad.

3. Ampliar el ámbito de aplicación del SIS introduciendo nuevos elementos en las descripciones a efectos de la denegación de entrada y estancia.

4. Reforzar la eficacia de los controles fronterizos.

5. Aumentar la eficiencia del trabajo de los guardias de fronteras y las autoridades de inmigración.

6. Lograr un mayor nivel de eficacia y armonización de los procedimientos nacionales y garantizar la aplicabilidad de la prohibición de entrada en el espacio Schengen.

7. Contribuir a la lucha contra la migración irregular.

1.5.2. Valor añadido de la intervención de la UE

El SIS es la principal base de datos de seguridad en Europa. En ausencia de controles en las fronteras interiores, la lucha eficaz contra la delincuencia y el terrorismo ha adquirido una dimensión europea. Así pues, el SIS es indispensable para apoyar los controles en las fronteras exteriores y el control de los migrantes irregulares detectados en el territorio nacional. Los objetivos de la presente propuesta se refieren

a mejoras técnicas para aumentar la eficiencia y la eficacia del sistema y armonizar su utilización en los Estados miembros participantes. La naturaleza transnacional de estos objetivos, junto con los retos que plantea garantizar un intercambio de información eficaz para contrarrestar las amenazas cada vez más diversificadas, implica que la UE esté en la mejor posición para proponer soluciones a dichos problemas. Los objetivos de mejora de la eficacia y uso armonizado del SIS, y en particular el aumento del volumen, la calidad y la rapidez del intercambio de información a través de un sistema de información centralizado a gran escala gestionado por una agencia reguladora (eu-LISA) no puede ser alcanzado por los Estados miembros por sí solos y requiere una intervención a nivel de la UE. Si las presentes cuestiones no se abordan, el SIS continuará operando de acuerdo con las normas aplicables en la actualidad, perdiendo por tanto la oportunidad de maximizar la eficiencia y el valor añadido de la UE identificado a través de la evaluación del SIS y su utilización por parte de los Estados miembros.

Solo en 2015, las autoridades nacionales consultaron el SIS casi 2 900 millones de veces e intercambiaron más de 1,8 millones de unidades de información complementaria: una clara demostración de la contribución fundamental del sistema a los controles en las fronteras exteriores. Este alto nivel de intercambio de información entre los Estados miembros no podría haberse alcanzado a través de soluciones descentralizadas, y habría sido imposible alcanzar estos resultados a nivel nacional. Asimismo, el SIS ha demostrado ser el instrumento más eficaz de intercambio de información a efectos de lucha antiterrorista y proporciona un valor añadido de la UE que permite a los servicios de seguridad nacionales cooperar de forma rápida, segura y eficaz. Las nuevas propuestas facilitarán en mayor medida el intercambio de información y la cooperación entre las autoridades de control fronterizo de los Estados miembros de la UE. Por otra parte, en el marco de sus competencias, se concederá a Europol y a la Guardia Europea de Fronteras y Costas pleno acceso al sistema como un signo claro del valor añadido de la participación de la UE.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

Las principales enseñanzas extraídas del desarrollo del Sistema de Información de Schengen de segunda generación fueron las siguientes:

1. La fase de desarrollo deberá comenzar únicamente cuando los requisitos técnicos y operativos se hayan definido en su totalidad. El desarrollo no se iniciará hasta que se hayan adoptado definitivamente los instrumentos jurídicos subyacentes que establezcan su finalidad, alcance, funciones y detalles técnicos.

2. La Comisión realizó (y sigue realizando) consultas continuas con las partes interesadas pertinentes, en particular los delegados del Comité SISVIS en virtud del procedimiento de comitología. Este Comité incluye representantes de los Estados miembros tanto en aspectos operativos de SIRENE (cooperación transfronteriza en relación con el SIS) como en aspectos técnicos de desarrollo y mantenimiento del SIS y de la aplicación SIRENE. Las modificaciones propuestas por el presente Reglamento se debatieron de manera muy transparente y exhaustiva en reuniones y talleres específicos. Asimismo, internamente, la Comisión creó un grupo director interservicios con la Secretaría General y las Direcciones Generales de Migración y Asuntos de Interior, Justicia y Consumidores, Recursos Humanos y Seguridad, e Informática. Este grupo director supervisó el proceso de evaluación y ofreció las orientaciones necesarias.

3. La Comisión también solicitó asesoramiento externo a través de tres estudios, cuyos resultados se han integrado en el desarrollo de la presente propuesta:

- Evaluación técnica del SIS (Kurt Salmon) - la evaluación determinó cuestiones clave relativas al SIS y las necesidades futuras que deben tenerse en cuenta; reveló la existencia de problemas por lo que se refiere a la maximización de la continuidad de las actividades y a garantizar que la arquitectura global pueda adaptarse a las crecientes necesidades de capacidad.

- Evaluación de impacto TIC de las posibles mejoras en la arquitectura del SIS II (Kurt Salmon) - el estudio evaluó los costes corrientes del funcionamiento del SIS a nivel nacional y tres posibles hipótesis técnicas para la mejora del sistema. Todas las hipótesis incluyen una serie de propuestas centradas en mejoras al sistema central y la arquitectura general.

- Estudio sobre la viabilidad y las implicaciones de establecer, en el marco del SIS, un sistema a escala de la UE para el intercambio de datos sobre las decisiones de retorno y el seguimiento del cumplimiento de las mismas (PwC) - este estudio evaluó la viabilidad técnica y operativa y de las repercusiones de los cambios propuestos al SIS con el fin de aumentar su uso para el retorno de los migrantes irregulares e impedir su reentrada.

1.5.4. Compatibilidad y posibles sinergias con otros instrumentos adecuados

La presente propuesta debe considerarse como la ejecución de las medidas incluidas en la Comunicación de 6 de abril de 2016 sobre el tema «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad»[84], que destaca la necesidad de la Unión Europea de reforzar y mejorar sus sistemas de tecnologías de la información, su arquitectura de datos e intercambio de información en el ámbito policial, de lucha contra el terrorismo y de gestión de fronteras.

Por otra parte, la propuesta es coherente con diversas políticas de la Unión en este ámbito:

a) la seguridad interior en relación con la función del SIS para prevenir la entrada de nacionales de terceros países que suponen una amenaza para la seguridad;

b) la protección de datos en la medida en que la presente propuesta debe garantizar la protección del derecho fundamental al respeto de la intimidad de los individuos cuyos datos son tratados en el SIS.

La propuesta también es compatible con la legislación vigente de la Unión Europea, fundamentalmente:

a) una política de retorno de la UE eficaz que contribuya y potencie el sistema de la UE para detectar e impedir el regreso de nacionales de terceros países tras su retorno. Ello contribuiría a la reducción de incentivos para la migración a la UE de forma irregular, que es uno de los principales objetivos de la Agenda Europea de Migración[85]. b) **Guardia Europea de Fronteras y Costas[86]:** por lo que respecta a la

84 COM(2016) 205 final.

85 COM(2015) 240 final.

86 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.

posibilidad de que el personal de la Agencia que realice análisis de riesgo, así como los equipos de la Guardia Europea de Fronteras y Costas o los equipos de personal implicados en tareas relacionadas con el retorno y los miembros de los equipos de apoyo a la gestión de la migración, dentro de los límites de su mandato, tengan derecho a acceder y consultar los datos introducidos en el SIS.

c) **los controles en las fronteras exteriores** en la medida en que el presente Reglamento ayuda a los Estados miembros a controlar su parte de las fronteras exteriores de la UE y a crear confianza en la eficacia del sistema de gestión de las fronteras de la UE.

d) Europol, en la medida en que la presente propuesta le atribuye derechos adicionales de acceso y consulta de los datos introducidos en el SIS con arreglo a su mandato.

La propuesta también es compatible con la futura legislación de la Unión Europea, fundamentalmente:

a) el **Sistema de Entradas y Salidas**[87]**,** que propone una combinación de la imagen facial y las impresiones dactilares como identificadores biométricos para el funcionamiento del Sistema de Entradas y Salidas (SES); un enfoque que la presente propuesta pretende reflejar;

b) el SEIAV, que prevé una rigurosa evaluación de seguridad, incluyendo un control en el SIS de los nacionales de terceros países que deseen viajar a la UE y estén exentos de la obligación de visado.

87 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de la denegación de entrada de los nacionales de terceros países que cruzan las fronteras exteriores de los Estados miembros de la Unión Europea, se determinan las condiciones de acceso al SES con fines coercitivos y se modifican el Reglamento (CE) n.º 767/2008 y el Reglamento (UE) n.º 1077/2011, COM(2016) 194 final.

1.6. Duración e incidencia financiera

☐ Propuesta/iniciativa de **duración limitada**

– ☐ Propuesta/iniciativa vigente desde el [DD.MM]AAAA hasta el [DD.MM]AAAA

– ☐ Incidencia financiera desde AAAA hasta AAAA

☑Propuesta/iniciativa de **duración ilimitada**

– Aplicación con una fase de puesta en marcha entre 2018 y 2020,

– seguida del pleno funcionamiento.

1.7. Modos de gestión previstos[88]

☑**Gestión directa** a cargo de la Comisión

– ☑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;

– ☐ 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

La Comisión será responsable de la gestión y eu-LISA será responsable del desarrollo, funcionamiento y mantenimiento del sistema.

El SIS es un sistema de información único. Por consiguiente, los gastos previstos en dos de las propuestas (la actual y la propuesta de Reglamento relativo al establecimiento, funcionamiento y utilización del SIS en los ámbitos de la cooperación policial y judicial en materia penal) no deberían considerarse dos importes separados, sino uno solo. Las

[88] Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

repercusiones presupuestarias de los cambios requeridos para la aplicación de ambas propuestas se incluyen en una única ficha financiera legislativa.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

La Comisión, los Estados miembros y la Agencia revisarán periódicamente y supervisarán la utilización del SIS, con el fin de garantizar que sigue funcionando de manera eficaz y eficiente. La Comisión estará asistida por el Comité para establecer las medidas técnicas y operativas descritas en la presente propuesta.

Además, la presente propuesta de Reglamento prevé, en el artículo 54, apartados 7 y 8, un proceso de revisión y evaluación formal periódico.

Cada dos años, eu-LISA deberá informar al Parlamento Europeo y al Consejo sobre el funcionamiento técnico del SIS, incluida la seguridad, la infraestructura de comunicación que lo sostiene y el intercambio bilateral y multilateral de información complementaria entre los Estados miembros.

Además, cada cuatro años, la Comisión deberá realizar, y transmitir al Parlamento y al Consejo, una evaluación global del SIS y el intercambio de información entre los Estados miembros. Esta evaluación:

a) examinará los resultados comparándolos con los objetivos;

b) evaluará si la lógica en que se basa el sistema sigue siendo válida;

c) estudiará la forma en que el Reglamento se aplica al sistema central;

d) evaluará la seguridad del sistema central;

e) estudiará las implicaciones para el futuro funcionamiento del sistema.

2.2. Asimismo, eu-LISA deberá facilitar estadísticas diarias, mensuales y anuales sobre la utilización del SIS, efectuando un seguimiento continuo del sistema y su funcionamiento en función de los objetivos. Sistema de gestión y control

2.2.1. Riesgo(s) identificado(s)

Los riesgos identificados son los siguientes:

1. Posibles dificultades de eu-LISA para gestionar las iniciativas presentadas en la presente propuesta en paralelo con otras en curso (por ejemplo, la implantación del SAID en el SIS) y las futuras iniciativas (por ejemplo, el Sistema de Entradas y Salidas, el SEIAV y la actualización de EURODAC). Este riesgo podría mitigarse garantizando que eu-LISA disponga de suficiente personal y recursos para desempeñar estas funciones y la gestión en curso del contratista del mantenimiento en estado de funcionamiento.

2. Dificultades para los Estados miembros:

2.1 Estas dificultades son esencialmente de naturaleza financiera. Por ejemplo, las propuestas legislativas incluyen el desarrollo obligatorio de una copia nacional parcial en cada N.SIS. Los Estados miembros que no han hayan desarrollado ya una deberán hacer la inversión. Del mismo modo, la aplicación nacional del documento de control de interfaces debe realizarse en su totalidad. Aquellos Estados miembros que aún no lo hayan hecho deberán preverlo en los presupuestos de los ministerios correspondientes. Este riesgo podría mitigarse mediante la provisión de financiación de la UE a los Estados miembros, por ejemplo del componente de Fronteras del Fondo de Seguridad Interior (FSI).

2.2 Los sistemas nacionales deben ser acordes con los requisitos del sistema central y los debates con los Estados miembros al respecto pueden generar retrasos en el desarrollo. Este riesgo podría mitigarse a través de la colaboración desde un primer momento con los Estados miembros sobre esta cuestión para garantizar que puedan tomarse medidas en el momento oportuno.

2.2.2. Información relativa al sistema de control interno establecido

Las responsabilidades relativas a los elementos centrales del SIS son ejercidas por eu-LISA. Con el fin de permitir una mejor supervisión del uso del SIS para analizar las tendencias relativas a la presión migratoria, la gestión de las fronteras y las infracciones penales, la Agencia deberá poder desarrollar una capacidad de vanguardia para la elaboración de informes estadísticos destinados a los Estados miembros y a la Comisión.

Las cuentas de eu-LISA se someterán a la aprobación del Tribunal de Cuentas y al procedimiento de aprobación de la gestión. El Servicio de Auditoría Interna de la Comisión llevará a cabo auditorías en cooperación con el auditor interno de la Agencia.

2.2.3. Estimación de los costes y beneficios de los controles y evaluación del nivel de riesgo de error esperado

N.d.

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, cuyo contenido es el siguiente:

1. Para luchar contra el fraude, la corrupción y otras actividades ilegales, se aplicará el Reglamento (CE) n.º 1073/1999.

2. La Agencia se adherirá al Acuerdo Interinstitucional relativo a las investigaciones internas de la Oficina Europea de Lucha contra el Fraude (OLAF) y adoptará sin demora las disposiciones adecuadas aplicables a los empleados de la Agencia.

3. Las decisiones de financiación y los acuerdos e instrumentos de aplicación resultantes establecerán expresamente que el Tribunal de Cuentas y la OLAF podrán, en caso necesario, efectuar controles in situ de los beneficiarios de los créditos de la Agencia, así como de los agentes responsables de la asignación de dichos créditos.

De conformidad con estas disposiciones, 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 en lo que respecta a las condiciones de las investigaciones internas relacionadas con la prevención del fraude, la corrupción y cualquier otra actividad ilegal que vaya en detrimento de los intereses de la Unión.

Se aplicará la estrategia de prevención y detección del fraude de la DG HOME.

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)

- Líneas presupuestarias existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	[Rúbrica 3 – Seguridad y Ciudadanía	CD/CND[89].	de países AELC[90]	de países candidatos [91]	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
	18.0208 – Sistema de Información de Schengen	CD	NO	NO	SÍ	NO
	18.020101 – Apoyo a la gestión de las fronteras y política común de visados para facilitar los viajes legítimos	CD	NO	NO	SÍ	NO
	18.0207 - 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

89 CD = créditos disociados / CND = créditos no disociados.

90 AELC: Asociación Europea de Libre Comercio.

91 Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

Rúbrica del marco financiero plurianual	3	Seguridad y Ciudadanía

DG HOME			Año **2018**	Año **2019**	Año **2020**	**TOTAL**
Créditos de operaciones						
18.0208 Sistema de Información de Schengen	Compromisos	1)	6,234	1,854	1,854	**9,942**
	Pagos	2)	6,234	1,854	1,854	**9,942**
18.020101 (Fronteras y Visados)	Compromisos	1)		18,405	18,405	**36,810**
	Pagos	2)		18,405	18,405	**36,810**
TOTAL de los créditos para la DG HOME	Compromisos	=1+1a +3	6,234	20,259	20,259	**46,752**
	Pagos	=2+2a +3	6,234	20,259	20,259	**46,752**

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	3	Seguridad y Ciudadanía

eu-LISA			Año **2018**	Año **2019**	Año **2020**	**TOTAL**
Créditos de operaciones						
Título 1: Gastos de personal	Compromisos	1)	0,210	0,210	0,210	**0,630**
	Pagos	2)	0,210	0,210	0,210	**0,630**
Título 2: Infraestructura y gastos de funcionamiento	Compromisos	1a)	0	0	0	**0**
	Pagos	2a)	0	0	0	**0**
Título 3: Gastos operativos	Compromisos	1a)	12,893	2,051	1,982	**16,926**
	Pagos	2a)	2,500	7,893	4,651	**15,044**
TOTAL de los créditos para ue-LISA	Compromisos	=1+1a +3	13,103	2,261	2,192	**17,556**
	Pagos	=2+2a +3	2,710	8,103	4,861	**15,674**

3.2.2. Incidencia estimada en los créditos de operaciones

TOTAL de los créditos de operaciones	Compromisos	4)								
	Pagos	5)								
TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		6)								

TOTAL de los créditos para la RÚBRICA <….> del marco financiero plurianual	Compromisos	=4+ 6								
	Pagos	=5+ 6								

Si la propuesta/iniciativa afecta a más de una rúbrica:

•TOTAL de los créditos de operaciones	Compromisos	4)							
	Pagos	5)							
•TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		6)							
TOTAL de los créditos para las RÚBRICAS 1 a 4 del marco financiero plurianual (Importe de referencia)	Compromisos	=4+ 6	19,337	22,520	22,451				**64,308**
	Pagos	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3. Incidencia estimada en los créditos de carácter administrativo

Rúbrica del marco financiero plurianual	**5**	«Gastos administrativos»

En millones EUR (al tercer decimal)

		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
DG: <…….>									
•Recursos humanos									
•Otros gastos administrativos									
TOTAL para la DG <….>	Créditos								

TOTAL de los créditos para la RÚBRICA 5 del marco financiero plurianual	(Total de los compromisos = total de los pagos)								

En millones EUR (al tercer decimal)

		Año **N**[92]	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 5 del marco financiero plurianual	Compromisos								
	Pagos								

92 El año N es el año de comienzo de la ejecución de la propuesta/iniciativa.

3.2.3.1. Incidencia estimada en los créditos de operaciones de eu-LISA

– ☐ 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:

Indíquense los objetivos y los resultados			Año **2018**		Año **2019**		Año **2020**		Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)								**TOTAL**	
	RESULTADOS																	
⇩	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 total	Coste total
OBJETIVO ESPECÍFICO N.º 1[94] Desarrollo del sistema central																		
- Contratista			1	5,013														5,013
- Programas			1	4,050														4,050
- Equipos			1	3,692														3,692
Subtotal del objetivo específico n.º 1				12,755														12,755
OBJETIVO ESPECÍFICO N.º 2 Mantenimiento del sistema central																		
-Contratista			1	0	1	0,365	1	0,365										0,730
Programas			1	0	1	0,810	1	0,810										1,620
Equipos			1	0	1	0,738	1	0,738										1,476

93 Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carretera construidos, etc.).

94 Tal como se describe en el punto 1.4.2. «Objetivo(s) específico(s)…».

Subtotal del objetivo específico n.º 2				1,913		1,913										3,826
OBJETIVO ESPECÍFICO N.° 3 Reuniones/Formación																
Actividades de formación	1	0,138	1	0,138	1	0,069										0,345
Subtotal del objetivo específico n.º 3		0,138		0,138		0,069										0,345
COSTE TOTAL		12,893		2,051		1,982										16,926

Créditos de compromiso en millones EUR (al tercer decimal)

3.2.3.2. Incidencia estimada sobre 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:

Indíquense los objetivos y los resultados ⇩			Año **2018**		Año **2019**		Año **2020**		Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)						**TOTAL**			
	RESULTADOS																	
	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 total	Coste total
OBJETIVO ESPECÍFICO N.° 1[96] Desarrollo del sistema nacional			1		1	1,221	1	1,221										2,442
OBJETIVO ESPECÍFICO N.° 2 Infraestructuras			1		1	17,184	1	17,184										34,368
COSTE TOTAL						18,405		18,405										36,810

95 Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carretera construidos, etc.).

96 Tal como se describe en el punto 1.4.2. «Objetivo(s) específico(s)…».

3.2.3.3. Incidencia estimada en los recursos humanos de eu-LISA - Resumen

– ☐ 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 **2018**	Año **2019**	Año **2020**	**TOTAL**
Funcionarios (categoría AD)				
Funcionarios (categoría AST)				
Agentes contractuales	0,210	0,210	0,210	0,630
Personal temporal				
Expertos nacionales en comisión de servicios				
TOTAL	**0,210**	**0,210**	**0,210**	**0,630**

La contratación está prevista para enero de 2018. Todo el personal deberá estar disponible desde principios de 2018 con el fin de permitir la puesta en marcha a tiempo para asegurar la entrada en funcionamiento del SIS refundido en 2020. Los tres nuevos agentes contractuales (AC) se precisan para cubrir necesidades tanto para la ejecución del proyecto como para el apoyo operativo y el mantenimiento después del inicio de la producción. Estos recursos se destinarán a:

- Apoyar la ejecución del proyecto como miembros del equipo del proyecto, incluyendo actividades tales como: la definición de requisitos y especificaciones técnicas, la cooperación y el apoyo a los Estados miembros durante la ejecución; actualizaciones del documento de control de interfaces (DCI), seguimiento de las entregas contractuales, entrega de documentación y actualizaciones, etc.
- Apoyar las actividades de transición para poner el sistema en funcionamiento en cooperación con el contratista [seguimiento de las actualizaciones, actualización del proceso operativo, actividades de formación (incluidas las actividades de formación en los Estados miembros), etc.].
- Apoyar de las actividades a más largo plazo, definir especificaciones, preparativos contractuales en caso de reconfiguración del sistema (por ejemplo, debido al reconocimiento de imagen) o en caso de que el nuevo contrato de mantenimiento en estado de funcionamiento del nuevo SIS II deba modificarse para incluir nuevos cambios (desde el punto de vista técnico o presupuestario).
- Aplicar el segundo nivel de apoyo tras la entrada en funcionamiento, durante el mantenimiento continuo y las operaciones.

Cabe señalar que los tres nuevos recursos (ETC AC) vendrá a sumarse a las capacidades del equipo interno, que se utilizarán también para las actividades operativas, de seguimiento financiero y contractuales y del proyecto. La utilización de un puesto de AC proporcionará una duración adecuada y continuidad a los contratos, a fin de garantizar la continuidad de la actividad y la utilización de las mismas personas especializadas para las actividades de apoyo operativo después de la conclusión del proyecto. Además, las actividades de apoyo operativo requieren accesos al entorno de producción que no pueden asignarse a los contratistas o al personal externo.

3.2.3.4. Necesidades estimadas de recursos humanos

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos.

– ☐ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en unidades de equivalente a jornada completa

		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
•Empleos de plantilla (funcionarios y personal temporal)								
XX 01 01 01 (Sede y Oficinas de Representación de la Comisión)								
XX 01 01 02 (Delegaciones)								
XX 01 05 01 (Investigación indirecta)								
10 01 05 01 (Investigación directa)								
• Personal externo (en equivalentes de tiempo completo, ETC)[97]								
XX 01 02 01 (AC, ENCS, INT de la dotación global)								
XX 01 02 02 (AC, LA, END, INT y JED en las Delegaciones)								
XX 01 04 **yy** [98]	- en la sede							
	- en las Delegaciones							
XX 01 05 02 (AC, ENCS, INT; investigación indirecta)								
10 01 05 02 (AC, INT, ENCS; investigación directa)								
Otras líneas presupuestarias								

97 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.

98 Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

(especifíquense)							
TOTAL							

XX 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:

Funcionarios y agentes temporales	
Personal externo	

3.2.4. 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.

Se ha previsto una reprogramación del resto del paquete «fronteras inteligentes» del Fondo de Seguridad Interior para aplicar las funcionalidades y los cambios previstos en las dos propuestas. El Reglamento de Fronteras FSI es el instrumento financiero en el que se ha incluido el presupuesto de ejecución del paquete de medidas sobre «fronteras inteligentes». En el artículo 5 se establece que se ejecutarán 791 millones EUR a través de un programa encaminado a la creación de sistemas de tecnología de la información en apoyo de la gestión de los flujos migratorios en las fronteras exteriores en las condiciones establecidas en el artículo 15. De los citados 791 millones EUR, 480 millones están reservados para el desarrollo del Sistema de Entradas y Salidas, y 210 para el desarrollo del Sistema Europeo de Información y Autorización de Viajes (SEIAV). El resto, 100,828 millones EUR, se utilizarán en parte para financiar los costes de los cambios previstos en las dos propuestas.

– ☐ La propuesta/iniciativa requiere la aplicación del instrumento de flexibilidad o la revisión del marco financiero plurianual.

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas y los importes correspondientes.

3.2.5. Contribuciones de terceros

– ☑La propuesta/iniciativa no prevé la cofinanciación por terceros.

– La propuesta/iniciativa prevé la cofinanciación que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			Total
Especifíquese el organismo de cofinanciación								

TOTAL de los créditos cofinanciados								

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 ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[99]						
		2018	2019	2020	2021	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo 6313 — Contribución de los países asociados a Schengen (CH, NO, LI, IS).		p.m.	p.m.	p.m.	p.m.			

En el caso de los ingresos diversos «asignados», especifíquese la(s) línea(s) presupuestaria(s) de gasto en la(s) que repercutan.

18.02.08 (Sistema de Información de Schengen), 18.02.07 (eu-LISA)

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.

[99] 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.