COMISIÓN
EUROPEA

Bruselas, 21.12.2016
COM(2016) 883 final

2016/0409 (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 la cooperación policial y judicial en materia penal, por el que se modifica el Reglamento (UE) n.º 515/2014 y se deroga el Reglamento (CE) n.º 1986/2006, la Decisión 2007/533/JAI del Consejo, y la Decisión 2010/261/UE de la Comisión

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 que plantean 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, las guardias 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 evaluó exhaustivamente el 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 interoperables, 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

[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 …

complementa la propuesta para la gestión de las fronteras y las disposiciones contenidas en 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.

La presente propuesta forma parte de un primer paquete de propuestas[6] destinadas a mejorar el funcionamiento y utilización del SIS en el ámbito de la cooperación policial y judicial en materia penal. La propuesta aplica:

---

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 (UE) 2018/xxx [inspecciones fronterizas] y Reglamento (UE) 2018/xxx [retorno de residentes ilegales nacionales de terceros países].

(1) el anuncio de la Comisión sobre la mejora del valor añadido del SIS con fines policiales[7] para responder a las nuevas amenazas;

(2) 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;

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

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

(3) 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 el ámbito de los controles fronterizos, 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].

El actual marco jurídico del SIS de segunda generación (relativo a su utilización para las necesidades de la cooperación policial y judicial en materia penal) se basa en un antiguo instrumento del tercer pilar, la Decisión 2007/533/JAI del Consejo[11], así como en un antiguo instrumento del primer pilar, el Reglamento (CE) n.º 1986/2006[12]. La presente propuesta consolida el contenido de los instrumentos existentes y añade nuevas disposiciones a fin de:

- armonizar mejor los procedimientos nacionales de utilización del SIS, en particular por lo que respecta a los delitos relacionados con el terrorismo y a los niños que corren riesgo de ser víctimas de sustracción parental de menores;
- ampliar el ámbito del SIS introduciendo nuevos elementos de identificación biométrica en las descripciones existentes;

---

7 Véase la Comunicación Aplicación de la Agenda Europea de Seguridad para luchar contra el terrorismo y allanar el camino hacia una Unión de seguridad genuina y efectiva, p. 4, COM(2016) 230 final de 20.4.2016.

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.

11 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.

12 Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al acceso al Sistema de Información de Schengen de segunda generación (SIS II) por los servicios de los Estados miembros competentes para la expedición de los certificados de matriculación de vehículos, DO L 381 de 28.12.2006, p. 1.

- introducir modificaciones técnicas para mejorar la seguridad y ayudar a reducir la carga administrativa, disponiendo la realización de copias nacionales obligatorias y estableciendo normas técnicas comunes para su aplicación;
- abordar el uso completo de todas las facetas del SIS, no abarcando solo los sistemas central y nacionales, sino garantizando también que los usuarios finales reciban toda la información necesaria para llevar a cabo sus tareas y cumplir todas las normas de seguridad cuando traten datos del SIS.

• Coherencia con otras políticas de la Unión así como con los instrumentos jurídicos existentes y futuros

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

(1) **la seguridad interior,** tal y como se destacó en la Agenda Europea de Seguridad[13] y en el trabajo de la Comisión hacia una Unión de la Seguridad real y efectiva[14] para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y otros delitos graves y permitir a los cuerpos de seguridad tratar los datos personales de personas sospechosas de estar implicadas en actos de terrorismo o delitos graves;

(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.

La presente propuesta también está estrechamente relacionada con la legislación vigente de la Unión, a saber:

(3) la **Guardia Europea de Fronteras y Costas** en lo que respecta a su acceso al SIS a efectos de la propuesta de Sistema Europeo de Información y Autorización de Viajes (SEIAV)[15], así como a facilitar una interfaz técnica de acceso al SIS a los equipos de la Guardia, a los equipos de personal implicados en tareas relacionadas con el retorno y a los miembros del equipo de apoyo a la gestión de la migración, con arreglo a su mandato, que tienen derecho de acceso y búsqueda de los datos introducidos en el SIS;

(4) **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;

(5) **Prüm**, en la medida en que las novedades de la presente propuesta, que permiten la identificación de personas a partir de sus impresiones dactilares (así como de imágenes faciales y perfiles de ADN) complementa las actuales disposiciones de Prüm[16] sobre acceso mutuo transfronterizo en línea a las bases de datos nacionales de ADN y a los sistemas automatizados de identificación de impresiones dactilares.

---

13 COM(2015) 185 final.

14 COM(2016) 230 final.

15 COM(2016) 731 final.

16 Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO L 210 de 6.8.2008, p. 1; y Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO L 210 de 6.8.2008, p. 12.

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

(6) la **gestión de las fronteras exteriores.** La propuesta complementa el nuevo principio, previsto en el Código de fronteras Schengen, de controles sistemáticos mediante la consulta de bases de datos de todos los viajeros, incluidos los ciudadanos de la UE, en el momento de su entrada y salida de la zona Schengen, como respuesta al fenómeno de los combatientes terroristas extranjeros;

(7) 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.

(8) 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 que desean viajar a la UE.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La presente propuesta se articula en torno al artículo 82, apartado 1, letra d), el artículo 85, apartado 1, el artículo 87, apartado 2, letra a), y el artículo 88, apartado 2, letra a), del Tratado de Funcionamiento de la Unión Europea como base jurídica para las disposiciones relativas a la cooperación policial y judicial en materia penal.

• Geometría variable

La presente propuesta desarrolla las disposiciones del acervo de Schengen relativas a la cooperación policial y judicial en materia penal. 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: de conformidad con el artículo 5 del Protocolo sobre el acervo de Schengen integrado en el marco de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y con el artículo 8, apartado 2, de 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 de participar en algunas de las disposiciones del acervo de Schengen[17], el Reino Unido está vinculado por el presente Reglamento.

Irlanda: de conformidad con el artículo 5 del Protocolo sobre el acervo de Schengen integrado en el marco de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y con el artículo 6, apartado 2, de la Decisión 2002/192/CE del Consejo, de 28 de febrero de 2002, sobre la solicitud de Irlanda de participar

[17] DO L 131 de 1.6.2000, p. 43.

en algunas de las disposiciones del acervo de Schengen, Irlanda está vinculada por el presente Reglamento[18].

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[19], 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.

El considerable nivel de intercambio de información entre los Estados miembros a través del SIS 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.

[18] DO L 64 de 7.3.2002, p. 20.

[19] 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.

- **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 con la cooperación policial y judicial en materia penal.

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. Teniendo en cuenta las necesidades operativas, la propuesta reduce el plazo de conservación de las descripciones de objetos y las adecúa a las descripciones relativas a personas (puesto que muchas veces están relacionadas con datos personales, tales como documentos de identificación personal o números de matrícula). La experiencia policial demuestra que los bienes robados puedan recuperarse en un período relativamente corto, lo que hace que el plazo de 10 años para las descripciones de objetos resulte innecesariamente largo.

Las descripciones del SIS contienen únicamente los datos necesarios para identificar y localizar a una persona u objeto y para la adopción de medidas. Todos los demás detalles adicionales se facilitan 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 adoptará la forma de Reglamento y sustituirá a la Decisión 2007/533/JAI del Consejo, aunque manteniendo gran parte del contenido de la misma. 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[20] (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.

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, 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.

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 para abordar la perspectiva de funcionamiento y utilización del SIS en todas sus fases a través de la regulación de su utilización por los usuarios finales y el establecimiento de normas de seguridad aplicables también a las solicitudes de usuarios finales, reforzar el sistema con fines de lucha contra el terrorismo facilitando la adopción de nuevas medidas, aclarar la situación de los niños que corren el riesgo de ser secuestrados por sus progenitores, así como ampliar los identificadores biométricos disponibles 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[21]) han constituido la base de las medidas contenidas en la presente propuesta.

---

[20] 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.

[21] 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.

- **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 67 de la Decisión 2007/533/JAI del Consejo. 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.

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 tres estudios, cuyos resultados se han integrado en el desarrollo de la presente propuesta:

- Evaluación técnica del SIS (Kurt Salmon)[22]

  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.

[22] Informe final de la Comisión Europea - Evaluación técnica del SIS II.

- Evaluación del impacto de las tecnologías de la información y la comunicación en posibles mejoras en la arquitectura del SIS II (Kurt Salmon)[23]

  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)[24]

  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).

- **Evaluación de impacto**

La Comisión no realizó una evaluación de impacto.

Las tres evaluaciones independientes antes mencionadas (en «Obtención y uso de asesoramiento especializado») 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[25] el 29 de enero de 2015. La Comisión adoptó también un catálogo de mejores prácticas y recomendaciones[26]. 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.

---

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

24 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)

25 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.

26 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.

El mecanismo de evaluación de Schengen, establecido en el Reglamento (UE) n.º 1053/2013[27] 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 han cometido un delito grave y cuya identidad se desconoce, así como los menores desaparecidos. 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.

- **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, incluida la reducción de los períodos de conservación de las descripciones de objetos, 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. Será posible realizar una

[27] 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.

identificación más fiable de las personas usando datos biométricos de las personas desaparecidas que requieren protección y garantizando que los datos personales sean exactos y estén adecuadamente protegidos. 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[28], 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 los artículos 26, 32, 34 y 36. En el futuro deberá ser posible hacer búsquedas de estos datos (impresiones dactilares y palmares) con las impresiones dactilares encontradas en el lugar del delito, siempre que se trate de un delito grave o de terrorismo y que se pueda afirmar con un alto grado de probabilidad que pertenecen al autor. Además, la propuesta prevé la conservación de las impresiones dactilares de las denominadas «personas desconocidas buscadas» (las condiciones se describen detalladamente en la sección 5, subsección «Fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN»). 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.

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 el ámbito de las inspecciones fronterizas) 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.

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

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 período 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). La Comisión fue informada por eu-LISA 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[29]. 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[30] 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 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.

---

29 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.

30 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.

Además, la presente propuesta de Reglamento prevé, en el artículo 71, 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 disposiciones específicas de la propuesta**

Disposiciones comunes a la presente propuesta y a la propuesta de Reglamento relativo al establecimiento, funcionamiento y utilización del SIS en el ámbito de las inspecciones fronterizas:

- 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 período de conservación (artículos 43, 46, 48, 50 y 51)
- Normas generales sobre tratamiento y protección de datos (artículos 53-70)
- Seguimiento y estadísticas (artículo 71)

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, 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 búsqueda en una base de datos nacional policial o de inmigración, realicen paralelamente la búsqueda 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 búsqueda paralela deberá ser conforme con el artículo 4 de la Directiva (UE) 2016/680[31].

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 56). 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 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 71). 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 búsquedas 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 búsqueda sea obligatoria si la identidad de la persona no puede determinarse de otra forma. Por otra parte, los cambios introducidos en el artículo 22 y los nuevos artículos 40, 41 y 42 permitirán el uso de imágenes faciales, impresiones palmares y perfiles de ADN para identificar a una persona, además del uso de impresiones dactilares. Actualmente, las imágenes faciales solo pueden utilizarse para

[31] 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.

confirmar la identidad de una persona a raíz de una consulta alfanumérica, y no como base para una búsqueda. 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. Existen dos usos principales de las impresiones palmares:

i) A efectos de 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, Italia comunicó un éxito considerable en la identificación de 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 italianas permitió la posterior identificación.

ii) Las impresiones latentes procedentes del lugar del delito, donde a menudo el sospechoso deja rastros que se deduce que corresponden a la palma de la mano. Solo a través de la toma rutinaria de impresiones palmares en circunstancias legalmente admitidas el sospechoso podrá ser identificado. Las impresiones palmares suelen contener también detalles de la base del dedo que faltan en la impresiones dactilares rodadas y planas, pues estas tienden a concentrarse en las puntas de los dedos y las articulaciones superiores de los dedos.

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.

En los casos en que las impresiones dactilares o palmares no estén disponibles, el artículo 22, apartado 1, letra b), permite el uso de perfiles de ADN de personas desaparecidas que deban ser puestas bajo protección, en particular niños. Esta funcionalidad se utilizará únicamente cuando se carezca de impresiones dactilares y solo será accesible para usuarios autorizados. Por consiguiente, esta disposición permite la utilización de los perfiles de ADN obtenidos a partir de los padres o hermanos de la persona desaparecida para que las autoridades nacionales puedan identificarla y localizarla. Los Estados miembros ya intercambian esta información entre sí a nivel operativo, a través del intercambio de información complementaria. La presente propuesta constituye un marco reglamentario relativo a esta práctica, incluyéndola en la base jurídica sustantiva de funcionamiento y uso del SIS y aplicando procedimientos claros sobre las condiciones en las que podrán utilizarse esos perfiles.

Las modificaciones propuestas permitirán asimismo emitir descripciones sobre personas desconocidas buscadas en relación con un delito, sobre la base de impresiones dactilares o palmares (artículos 40-42). Estas descripciones pueden crearse, por ejemplo, cuando se hallen impresiones dactilares o palmares latentes en el lugar de un delito grave y existan razones fundadas para sospechar que las impresiones dactilares pertenecen al autor del delito. Por ejemplo, cuando se encuentran impresiones dactilares en un arma utilizada en la comisión del delito o cualquier otro objeto utilizado por el autor en aquel momento. Esta nueva categoría de descripción complementa las disposiciones de Prüm que permiten la interconectividad de los sistemas penales nacionales de identificación de impresiones dactilares. A través de dicho

mecanismo, un Estado miembro puede presentar una solicitud para determinar si el autor de un delito cuyas impresiones se han hallado es conocido en cualquier otro Estado miembro (generalmente a efectos de investigación). Una persona puede ser identificada a través del mecanismo de Prüm solamente si sus impresiones dactilares han sido tomadas en otro Estado miembro a efectos penales. Por tanto, no se puede identificar a quienes cometen un primer delito. El desarrollo de esta propuesta, es decir, el almacenamiento de las impresiones dactilares de personas desconocidas buscadas, permitirá introducir en el SIS las impresiones dactilares de un autor desconocido con el fin de que pueda ser identificado como persona buscada si la localiza en otro Estado miembro. La utilización de esta función presupone que los Estados miembros realizaron una consulta previa de todas las fuentes nacionales e internacionales disponibles, pero no pudieron determinar la identidad del sujeto en cuestión. En la propuesta se incluyen salvaguardias suficientes para garantizar que, dentro de esta categoría, el SIS solo almacene impresiones dactilares de personas de las que se tengan sospechas fundadas de que han cometido un delito grave o un delito de terrorismo. Por tanto, la utilización de este nuevo tipo de categoría de descripción solo puede autorizarse cuando el autor desconocido de un delito constituye un gran riesgo para la seguridad pública que justifica la comparación de tales impresiones con las impresiones dactilares de los viajeros, por ejemplo, para evitar que una persona abandone el espacio sin controles en las fronteras interiores.

Esta disposición no permite a los usuarios finales añadir impresiones dactilares en esta categoría si su relación con el infractor no puede establecerse. Otra condición será que la identidad de la persona no pueda establecerse utilizando otras bases de datos nacionales, europeas o internacionales que almacenan impresiones dactilares. Una vez almacenadas en el SIS, estas impresiones dactilares se utilizarán para identificar a las personas cuya identidad no pueda determinarse por otros medios. Si este control concluye en una posible coincidencia, el Estado miembro deberá proceder a controles adicionales de sus impresiones dactilares, en su caso con la participación de expertos en impresiones dactilares, a fin de determinar si se trata de la persona a quien corresponden las impresiones dactilares almacenadas en el SIS, y debe establecer la identidad de la persona. Los procedimientos están sujetos a la legislación nacional. Una identificación en el SIS como «persona desconocida buscada» posiblemente resultará en una detención.

Acceso al SIS

En este apartado se describen los elementos nuevos en términos de derechos de acceso al SIS por lo que respecta a las autoridades nacionales competentes y las agencias de la UE (usuarios institucionales).

Autoridades nacionales - autoridades de inmigración

Para garantizar el uso más eficaz del SIS, la propuesta permite el acceso al mismo a las autoridades nacionales responsables de examinar las condiciones y tomar las decisiones relativas a la entrada, la estancia y el retorno de nacionales de terceros países en el territorio de los Estados miembros. Esta adición permite la consulta del SIS en relación con los migrantes irregulares que no han sido controlados en las fronteras. Esta propuesta garantiza que se dispense el mismo trato a los nacionales de terceros países que cruzan las fronteras exteriores en pasos fronterizos regulares (y que, por tanto, son objeto de controles aplicables a los nacionales de terceros países) así como a los nacionales de terceros países que llegan de forma irregular al espacio Schengen.

Además, la propuesta garantiza que las autoridades responsables de la matriculación de vehículos (artículo 44), embarcaciones y aeronaves tendrán un acceso limitado al sistema para

llevar a cabo sus tareas, a condición de que se trate de servicios oficiales. Esto contribuirá a evitar la matriculación de los mencionados medios de transporte si han sido robados y están siendo buscados en otro Estado miembro. La iniciativa no es nueva en relación con los servicios encargados de la matriculación de vehículos, pues su acceso al SIS ya se contemplaba en el artículo 102 *bis* del Convenio de Schengen y en el Reglamento (CE) n.º 1986/2006[32]. Siguiendo la misma lógica, la propuesta prevé el acceso de las autoridades responsables de la matriculación de embarcaciones y aeronaves a las descripciones del SIS relativas a embarcaciones y aeronaves.

Usuarios institucionales

Europol (artículo 46), Eurojust (artículo 47) y la Agencia Europea de la Guardia de Fronteras y Costas, así como sus equipos, el personal responsable de tareas relacionadas con el retorno y los miembros del equipo de apoyo a la gestión de la migración (artículos 48 y 49) tienen acceso al SIS y a los datos del SIS que necesitan. Se introducen salvaguardias adecuadas para garantizar una adecuada protección de los datos del sistema (incluidas también las disposiciones del artículo 50, que establece que estos organismos solo podrán acceder a los datos que necesitan para llevar a cabo sus tareas).

En el caso de Europol, las modificaciones previstas en la propuesta amplían su acceso al SIS a las descripciones de personas desaparecidas, asegurando que pueda hacer el mejor uso del sistema al realizar sus tareas y añaden nuevas disposiciones que garantizan que la Agencia Europea de la Guardia de Fronteras y Costas y sus equipos puedan acceder al sistema al realizar las distintas operaciones con arreglo a su mandato de asistir a los Estados miembros. En el contexto de los trabajos del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad y con vistas a seguir reforzando el intercambio de información en materia de terrorismo, la Comisión evaluará si Europol debería recibir una notificación automática del SIS cuando se cree una descripción relacionada con una actividad terrorista.

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)[33], la unidad central de la Agencia Europea de la Guardia de Fronteras y Costas efectuará búsquedas 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 del SEIAV también tendrá pleno acceso al SIS.

Cambios específicos en las descripciones

El artículo 26 establece que los Estados miembros suspenderán temporalmente las descripciones a efectos de una detención (en caso de una operación o investigación policial en curso), haciendo que solo puedan ser consultadas por las Oficinas SIRENE, pero no por los agentes sobre el terreno durante un período limitado. Esta disposición contribuirá a evitar que una operación policial confidencial cuyo objetivo es detener a un delincuente muy buscado se vea comprometida por un agente de policía que no esté al tanto del asunto.

---

[32] Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al acceso al Sistema de Información de Schengen de segunda generación (SIS II) por los servicios de los Estados miembros competentes para la expedición de los certificados de matriculación de vehículos, DO L 381 de 28.12.2006, p. 1.

[33] COM (2016) 731 final.

Los artículos 32 y 33 se refieren a las descripciones sobre personas desaparecidas. Los cambios al respecto permiten emitir descripciones preventivas cuando se estime que existe un riesgo elevado de sustracción parental, y establecen una categorización más detallada de las descripciones sobre personas desaparecidas. La sustracción parental suele producirse en circunstancias muy planificadas, con la intención de abandonar el Estado miembro en el que se establecieron los acuerdos de custodia. Las modificaciones de la propuesta pretenden subsanar una posible laguna en la legislación actual, ya que actualmente las descripciones sobre niños solo pueden emitirse una vez que estos han desaparecido. Ello permitirá a las autoridades de los Estados miembros indicar qué niños se enfrentan a un riesgo particular. Estos cambios harán que, cuando exista un alto riesgo de sustracción parental inminente, los guardias de fronteras y las policías sean conscientes del riesgo y estén en condiciones de examinar con más detalle las circunstancias en que viaja un niño en riesgo, procediendo a custodiarlo en caso necesario. La información adicional, en particular sobre la decisión de las autoridades judiciales competentes que solicitaron la descripción, se facilitará a través de las Oficinas SIRENE. El Manual SIRENE será revisado en consecuencia. Esta descripción requerirá una oportuna resolución de las autoridades judiciales concediendo la custodia solo a uno de los progenitores. Otro requisito será que exista un riesgo inminente de sustracción. La situación de las descripciones sobre menores desaparecidos se actualizará para reflejar automáticamente que estos han alcanzado la edad adulta, cuando proceda.

El artículo 34 permite añadir a la descripción los datos sobre vehículos cuando haya indicios claros de que están relacionados con la persona buscada.

El artículo 37 introduce una nueva forma de control, la «investigación», destinada en particular a apoyar medidas para combatir el terrorismo y los delitos graves. Permite a las autoridades detener e interrogar a la persona de que se trate. Es más rigurosa que el actual sistema de control discreto, pero no implica la búsqueda de la persona y no equivale a su detención. No obstante, puede aportar información suficiente para decidir sobre las medidas ulteriores. Se modifica asimismo el artículo 36 para reflejar este tipo de control adicional.

La propuesta establece que las descripciones del SIS deberán cubrir los documentos oficiales vírgenes y los documentos de identidad expedidos (artículos 36) y los vehículos, incluidas embarcaciones y aeronaves (artículos 32 y 34) cuando estén relacionados con las descripciones de personas emitidas con arreglo a dichos artículos. Se modifica el artículo 37 a fin de establecer las medidas que deberán adoptarse sobre la base de estas descripciones. El objetivo es puramente de investigación, ya que permitirá a las autoridades abordar situaciones en las que varias personas utilizan documentos auténticos, pero que se semejan, de los que no son los titulares legítimos.

El artículo 38 establece una lista ampliada de objetos para los que pueden emitirse descripciones, añadiendo documentos falsificados, vehículos con independencia del sistema de propulsión (es decir, eléctricos así como de gasolina o gasóleo, etc.), billetes falsificados, equipos informáticos, y componentes claramente identificables de vehículos y equipos industriales. Ya no contiene descripciones relativas a medios de pago, dado que la eficacia de dichas descripciones era muy baja y apenas daban respuestas positivas.

A fin de aclarar el proceso a seguir una vez encontrado un objeto descrito, el artículo 39 se modifica para aclarar que los objetos deben ser incautados, de conformidad con la legislación nacional, además de ponerse en contacto con la autoridad que haya introducido la descripción.

Protección de datos y seguridad

La 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 57).

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

El artículo 12 también incluye disposiciones en materia de búsqueda automatizada mediante escaneo de las matrículas de vehículos de motor, utilizando sistemas de reconocimiento automático de matrículas, lo que obliga a los Estados miembros a mantener un registro de tales consultas de conformidad con la legislación nacional.

El artículo 15, apartado 3, mantiene el artículo 15, apartado 3, de la Decisión 2007/533/JAI del Consejo 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 examinar si un asunto es suficientemente adecuado, pertinente e importante para decidir si el período de validez de la descripción debe prorrogarse. Como novedad, este artículo también obliga a los Estados miembros a crear una descripción con arreglo a los artículos 34, 36 y 38 (según proceda) en todas las circunstancias, con respecto a las personas u objetos relacionados con ellas cuyas actividades estén contempladas por 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

La 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;
- otras observaciones relacionadas con ella; el motivo de la inscripción;
- datos sobre el número de registro nacional y el lugar de registro de la persona;
- categorización del tipo de caso de persona desaparecida (solo descripciones con arreglo al artículo 32);
- detalles sobre la identidad o el documento de viaje de la persona;
- copia en color del documento de identidad o de viaje de la persona;
- perfiles de ADN (solo si no se dispone de impresiones dactilares adecuadas a efectos de identificación).

El artículo 59 amplía la lista de datos personales que pueden consignarse y tratarse en el SIS a fin de luchar contra la usurpación de identidad. Estos datos solo pueden ser consignados con el consentimiento de la víctima de dicha usurpación e incluirán también:

- 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. Se incorporan detalles de los documentos de identificación personal de los interesados y se permite la posibilidad de clasificar a los niños desaparecidos (menores no acompañados, sustracción parental, fugas, etc.). Esto es esencial para que los usuarios finales adopten sin demora las medidas necesarias para proteger a los niños. La mejora de la información permite una mejor identificación de la persona afectada y, por otra, que los usuarios finales adopten las 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[34].

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 53).

Conservación

El período máximo de conservación de la descripción de las personas se ampliará a cinco años, con excepción de las descripciones a efectos de controles discretos, específicos o de investigación, para las que el período de conservación seguirá siendo de un año. Los Estados miembros siempre podrán establecer plazos más cortos. La prórroga de la fecha de expiración sigue las prácticas nacionales de prorrogarla en caso de que una descripción todavía no haya cumplido su objetivo mientras que el interesado sigue en búsqueda. Además, fue necesario adaptar el SIS al período de conservación en el marco de otros instrumentos, como la Directiva sobre el retorno y Eurodac. En aras de la transparencia y la claridad, es necesario prever el mismo período de conservación de las descripciones relativas a personas, excepto las creadas a efectos de controles discretos, específicos o de investigación. La prórroga del período de conservación no compromete los derechos de los interesados, ya que una descripción no puede mantenerse más de lo necesario para su objetivo. Las normas sobre supresión de descripciones se establecen explícitamente en el artículo 52. El artículo 51 establece el plazo para la revisión de las descripciones e incluye, en particular, la reducción del período de conservación de las descripciones relativas a objetos. A falta de una necesidad operativa de conservar el período más largo para los objetos, este se reduce ahora a cinco años para adecuarlo al período de conservación de las descripciones relacionadas con la persona. La fecha de expiración para los documentos expedidos y los documentos vírgenes, sin embargo, seguirá siendo de 10 años porque el período de validez de los documentos es de 10 años.

Supresión

El artículo 52 establece las circunstancias en las que se suprimirán las descripciones, en aras de una mayor armonización de las prácticas nacionales en este ámbito; el artículo 51 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.

[34] 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.

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[35] y la Directiva 2016/680[36]. Además, el artículo 63 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 en dicho artículo, y debe ser una medida proporcionada y necesaria, conforme con la legislación nacional.

Intercambio de datos con Interpol sobre documentos perdidos, robados, invalidados y usurpados

El artículo 63 mantiene plenamente el artículo 55 de la Decisión 2007/533/JAI del Consejo, pues la mejor interoperabilidad entre la sección de documentos del SIS y la base de documentos perdidos y robados de Interpol será abordada en la Comunicación del Grupo de Expertos de Alto Nivel y en la segunda serie de propuestas sobre el SIS en junio de 2017.

Estadísticas

Con el fin de mantener una visión general del funcionamiento de los recursos en la práctica, el artículo 66 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 71 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.

---

[35] 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.

[36] 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.

El artículo 71, apartado 5, prevé que eu-LISA facilitará a los Estados miembros, la Comisión, Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas los 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 71, apartado 6, establece 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, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas acceda a los datos enumerados en el artículo 71, apartado 3, a fin de elaborar las estadísticas necesarias.

2016/0409 (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 la cooperación policial y judicial en materia penal, por el que se modifica el Reglamento (UE) n.º 515/2014 y se deroga el Reglamento (CE) n.º 1986/2006, la Decisión 2007/533/JAI del Consejo, y la Decisión 2010/261/UE de la Comisión

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 82, apartado 1, párrafo segundo, letra d), su artículo 85, apartado 1, su artículo 87, apartado 2, letra a), y su artículo 88, apartado 2, letra a),

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 otros cuerpos de seguridad, y autoridades judiciales en materia penal.

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[37] (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[38] y la Decisión 2001/886/JAI del Consejo[39] y fue creado

[37] 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.

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

[39] 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.

por el Reglamento (CE) n.º 1987/2006[40] así como por la Decisión 2007/533/JAI del Consejo[41]. 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[42]. 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 de los capítulos 4 y 5 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 las inspecciones fronterizas[43] 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.

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

---

40 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.

41 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.

42 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....

43 Reglamento (UE) 2018/...

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 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[44] («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 los delitos, 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, para facilitar la identificación de personas y detectar las identidades múltiples, las categorías de datos relativos a las personas deben incluir una referencia al documento o número de identidad personal 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

[44] 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.

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 búsqueda en una base de datos nacional de policía o de inmigración consulten también el SIS en paralelo, con arreglo a lo dispuesto en el artículo 4 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[45]. 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 impresiones dactilares e imágenes faciales. La búsqueda 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) La introducción de un servicio automatizado de identificación de impresiones dactilares en el SIS complementa el mecanismo existente de Prüm sobre acceso mutuo transfronterizo en línea a las bases de datos nacionales de ADN y los sistemas automatizados de identificación de impresiones dactilares[46]. El mecanismo de Prüm permite la interconexión de los sistemas nacionales de identificación dactilar, gracias a lo cual un Estado miembro puede presentar una solicitud para determinar si el autor de un delito cuyas impresiones dactilares han sido halladas es conocido en cualquier otro Estado miembro. El mecanismo de Prüm verifica si la persona a quien corresponden las impresiones dactilares es conocida en un momento dado; por tanto, aunque posteriormente sea reconocida en algún Estado miembro, no será necesariamente detenida. La búsqueda de impresiones dactilares en el SIS permite una búsqueda activa del autor. Por tanto, conviene prever la posibilidad de cargar las impresiones dactilares de un autor desconocido en el SIS, a condición de que la persona a quien correspondan las impresiones pueda ser identificada con un alto grado de probabilidad como autor de un acto de terrorismo o de delincuencia grave. Este es el caso, en particular, cuando las impresiones dactilares se encuentran en un arma o en cualquier objeto utilizado para el delito. La mera presencia de las impresiones dactilares en el lugar del delito no debe considerarse como indicio de un alto grado de probabilidad de que sean las del

---

45 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.

46 Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (DO L 210 de 6.8.2008, p. 1). y la Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO L 210 de 6.8.2008, p. 12.

autor. Otro requisito previo para la creación de dicha descripción debe ser que la identidad del autor no pueda establecerse mediante otras bases de datos nacionales, europeas o internacionales. En caso de que este tipo de búsqueda de impresiones dactilares conduzca a una posible correspondencia, el Estado miembro deberá proceder a verificaciones adicionales con sus impresiones dactilares, en su caso con la participación de expertos en la materia, a fin de determinar si es el autor es la persona a quien corresponden las impresiones dactilares almacenadas en el SIS, y debe establecer la identidad de la persona. Los procedimientos deben estar sujetos a la legislación nacional. Una identificación como «persona desconocida buscada» en el SIS puede contribuir sustancialmente a la investigación y podrá desembocar en una detención siempre que se cumplan todas las condiciones para proceder a la detención.

19) Las impresiones dactilares encontradas en el lugar del delito deberán poder cotejarse con las almacenadas 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[47] y los «delitos de terrorismo» serán los tipificados en la legislación nacional a que se refiere la Decisión Marco 2002/475/JAI del Consejo[48].

20) Deberá ser posible añadir un perfil de ADN en los casos en que no se disponga de datos dactiloscópicos, que solo deberá ser accesible para usuarios autorizados. Los perfiles de ADN deben facilitar la identificación de personas desaparecidas que necesitan protección y especialmente de niños desaparecidos, en particular permitiendo el uso de los perfiles de ADN de sus padres o hermanos para permitir la identificación. Los datos relativos al ADN no deben contener referencias al origen racial.

21) El SIS deberá contener descripciones de personas buscadas para detenerlas a fin de entregarlas o extraditarlas. Además de las descripciones, procede disponer el intercambio de la información complementaria que sea necesaria para los procedimientos de entrega y extradición. En particular, los datos a que se refiere el artículo 8 de la 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, deben ser tratados en el SIS[49]. Por razones operativas, resulta oportuno que el Estado miembro emisor suspenda temporalmente una descripción de detención existente tras obtener autorización de la autoridad judicial y cuando la persona objeto de una orden de detención europea sea buscada activa e intensivamente y los usuarios finales que no participen en la operación de búsqueda puedan poner en peligro un resultado satisfactorio. La indisponibilidad temporal de este tipo de descripciones no debe superar las 48 horas

22) Deberá ser posible añadir en el SIS una traducción de los datos adicionales introducidos a efectos de una entrega con arreglo a la orden de detención europea o de una extradición.

---

47 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.

48 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.

49 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.

23) El SIS deberá contener descripciones de personas desaparecidas para garantizar su protección o prevenir amenazas a la seguridad pública. La emisión de una descripción en el SIS para niños en riesgo de sustracción (es decir, con el fin de evitar un perjuicio futuro que todavía no ha tenido lugar, como en el caso de los niños que sufren riesgo de sustracción parental) debe limitarse; por ello es conveniente prever salvaguardias estrictas y adecuadas. En el caso de los niños, estas descripciones y los procedimientos correspondientes deben servir el interés superior del niño, teniendo en cuenta el artículo 24 de la Carta de los Derechos Fundamentales de la Unión Europea y la Convención de las Naciones Unidas sobre los Derechos del Niño, de 20 de noviembre de 1989.

24) Deberán incluirse nuevas medidas para presuntos casos de terrorismo y delitos graves, que permitan retener e interrogar a una persona sospechosa de haber cometido un delito grave o cuando haya motivos para creer que tiene intención de cometerlo, con el fin de que el Estado miembro emisor pueda recabar información más detallada. Esta nueva medida no debe equivaler al registro o la detención de la persona. Sin embargo, deberá facilitar información suficiente para decidir la adopción de ulteriores medidas. Los delitos graves deben ser los enumerados en la Decisión Marco 2002/584/JAI del Consejo.

25) El SIS deberá incluir nuevas categorías de objetos de gran valor, como equipos electrónicos y técnicos, que puedan ser identificados y registrados con un único número.

26) Los Estados miembros deberán tener la posibilidad de añadir una indicación a una descripción a fin de que la medida que deba adoptarse en relación con la descripción no se aplique en su territorio. Cuando las descripciones se introduzcan para detener a una persona a efectos de su entrega, nada en la presente Decisión se interpretará como una excepción a la Decisión Marco 2002/584/JAI ni en el sentido de impedir la aplicación de lo dispuesto en ella. La decisión de añadir una indicación a una descripción deberá basarse únicamente en los motivos de denegación contenidos en la citada Decisión Marco.

27) Cuando se añada una indicación a una descripción y se descubra el paradero de la persona buscada para detenerla a efectos de entrega, siempre deberá comunicarse ese paradero a la autoridad judicial requirente, que podrá decidir emitir una orden europea de detención a la autoridad judicial competente, de conformidad con lo dispuesto en la Decisión Marco 2002/584/JAI.

28) 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 período de conservación ni a los derechos de acceso a las descripciones.

29) 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 período de conservación de las descripciones relativas a personas con los períodos de conservación previstos a efectos del retorno y la residencia ilegales. Además, los Estados miembros prorrogan regularmente la fecha de expiración de las descripciones relativas a personas en caso de que la medida requerida no pueda tomarse en el período original. Por tanto, el plazo de conservación de las descripciones de personas deberá ser como máximo de cinco años. Por regla general, las descripciones de personas deberán suprimirse automáticamente del SIS

tras un período de cinco años, salvo en el caso de las descripciones a efectos de controles discretos, específicos y de investigación, que deben suprimirse al cabo de un año. Las descripciones de objetos introducidas a efectos de controles discretos, específicos o de investigación deberán suprimirse automáticamente del SIS después de un año, pues siempre están relacionadas con personas. Las descripciones de objetos para su incautación o su utilización como pruebas en un procedimiento penal deberán suprimirse automáticamente del SIS tras un período de cinco años, pues una vez transcurrido dicho plazo la probabilidad de encontrarlos es muy baja y se reduce significativamente su valor económico. Las descripciones relativas a documentos de identidad expedidos o vírgenes deberán conservarse durante 10 años, puesto que el período de validez de los documentos es de 10 años en el momento de la emisión. Las decisiones de mantener descripciones de personas deberán basarse en una evaluación general del caso concreto. Los Estados miembros deberán revisar las descripciones de personas en el período de revisión establecido y elaborar estadísticas del número de descripciones cuyo período de conservación se haya prorrogado.

30) La introducción y prórroga de la fecha de expiración de una descripción del SIS deberán estar sujetas al necesario requisito de proporcionalidad, examinando si un caso concreto es adecuado, pertinente e importante como para introducir una descripción en el SIS. Los delitos contemplados en los artículos 1, 2, 3 y 4 de la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo[50] constituyen una amenaza muy grave para la seguridad pública y la integridad de la vida de las personas y para la sociedad, y estos delitos son extremadamente difíciles de prevenir, detectar e investigar en un espacio sin controles fronterizos internos en el que los posibles infractores circulan libremente. En caso de que una persona u objeto sean buscados en relación con estos delitos, siempre es necesario crear la correspondiente descripción en el SIS sobre personas buscadas a efectos de un proceso penal, sobre personas u objetos que deban ser sometidos a controles discretos, específicos y de investigación, así como sobre objetos para su incautación, ya que ningún otro medio resultará tan eficaz a dicho efecto.

31) Es necesario aclarar los aspectos relativos a la supresión de las descripciones. Una descripción deberá conservarse únicamente durante el tiempo necesario para alcanzar el objetivo con que se introdujo. Habida cuenta de las prácticas divergentes de los Estados miembros en lo que respecta a la definición del momento en que una descripción cumple su objetivo, procede establecer criterios detallados a fin de determinar, para cada tipo de descripción, el momento en que ha de ser suprimida del SIS.

32) 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, así como a nivel nacional, para garantizar la seguridad de los datos durante todas las fases de su funcionamiento y utilización. Las autoridades que intervengan en el tratamiento de datos deberán estar sujetas a los requisitos de seguridad del presente Reglamento y a un procedimiento uniforme de notificación de incidentes.

33) 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. No obstante, procede fortalecer la cooperación entre la Unión Europea

[50] 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.

e Interpol fomentando un intercambio eficaz de datos de pasaportes. Cuando se transmitan datos personales del SIS a Interpol, deberán someterse a un nivel adecuado de protección, garantizado por un acuerdo que estipule unas salvaguardias y unas condiciones estrictas.

34) Es conveniente conceder el acceso al SIS a las autoridades responsables de la matriculación de vehículos, embarcaciones y aeronaves con el fin de permitirles comprobar si el medio de transporte ya es objeto de búsqueda en un Estado miembro para su incautación o control. Deberá facilitarse el acceso directo a las autoridades que son servicios públicos. Este acceso deberá limitarse a las descripciones relativas al respectivo medio de transporte y su documento de registro o número de matrícula. En consecuencia, las disposiciones del Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo[51] deben incluirse en el presente Reglamento y dicho Reglamento debe derogarse.

35) Para el tratamiento de datos por parte de las autoridades nacionales competentes a efectos de prevención, investigación, detección de delitos graves o delitos de terrorismo, enjuiciamiento de delitos o ejecución de sanciones penales, inclusive la protección contra amenazas para la seguridad pública, deberán aplicarse las disposiciones nacionales de transposición de la Directiva (UE) 2016/680. Las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[52] y de la Directiva (UE) 2016/680 deben concretarse en el presente Reglamento cuando sea necesario.

36) En virtud del presente Reglamento, el Reglamento (UE) 2016/679 deberá aplicarse al tratamiento de datos personales por las autoridades nacionales cuando la Directiva (UE) 2016/680 no sea aplicable. El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo[53] debe 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.

37) 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 (Europol)[54].

---

51 Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al acceso al Sistema de Información de Schengen de segunda generación (SIS II) por los servicios de los Estados miembros competentes para la expedición de los certificados de matriculación de vehículos, DO L 381 de 28.12.2006, p. 1.

52 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 la que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, DO L 119 de 4.5.2016, p. 1.

53 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.

54 Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la Agencia de la Unión Europea de cooperación en funciones coercitivas (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JAI y 2009/968/JAI, DO L 135 de 25.5.2016, p. 53.

38) Las disposiciones de la Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002[55], por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, relativas a la protección de datos se aplican al tratamiento de los datos del SIS por parte de Eurojust, incluidas la competencia de la Autoridad Común de Control, creada en virtud de dicha Decisión, para controlar las actividades de Eurojust y la responsabilidad por todo tratamiento ilegal de datos personales por Eurojust. En caso de que una búsqueda realizada por Eurojust en el SIS revele la existencia de una descripción emitida por un Estado miembro, Eurojust no puede adoptar las medidas necesarias. Por consiguiente, deberá informar de ello al Estado miembro para que este pueda hacer un seguimiento del asunto.

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

40) 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 cooperar entre sí para abordar las cuestiones de seguridad desde una perspectiva común.

41) 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.

42) Las autoridades 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 debe ser realizada por las autoridades de supervisión o las autoridades nacionales de supervisión deben ordenar directamente la auditoría a un auditor independiente para 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 lo 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.

43) El Reglamento (UE) 2016/794 (Reglamento Europol) establece 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. La ampliación de los derechos de acceso de Europol a las descripciones del SIS sobre personas desaparecidas debería seguir mejorando la capacidad de Europol para facilitar a los servicios policiales nacionales una asistencia operativa y productos analíticos relativos a la trata de seres humanos y la explotación sexual de los niños, incluidos los delitos en internet. Esto contribuiría a mejorar la prevención de estos delitos, la protección de las víctimas potenciales y la investigación de la autoría. El Centro Europeo de Ciberdelincuencia de Europol también se beneficiaría del nuevo acceso de Europol a las descripciones en

[55] Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO L 63 de 6.3.2002, p. 1.

el SIS de personas desaparecidas, como en los casos de los delincuentes sexuales viajeros y el abuso sexual de menores en línea, casos en que los autores sostienen a menudo que tienen o pueden tener acceso a niños que pueden haber sido registrados como desaparecidos. Además, dado que el Centro Europeo sobre Tráfico Ilícito de Migrantes de Europol desempeña un importante papel estratégico para luchar contra la facilitación de la migración irregular, deberá tener acceso a las descripciones de personas a las que se deniegue la entrada o la estancia en el territorio de un Estado miembro, ya sea por motivos delictivos o por el incumplimiento de las condiciones de los visados y de estancia.

44) 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 deben intercambiar información sobre actividades relacionadas con el terrorismo con Europol en paralelo 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.

45) Además, es necesario establecer normas claras para Europol sobre el tratamiento y la transferencia de los datos del SIS para 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 registros realizados 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 concernido para permitir un seguimiento del asunto.

46) A efectos del presente Reglamento, el Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo[56] 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 del personal implicado 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 dichas agencias. El objetivo del despliegue de los equipos de la Guardia Europea de Fronteras y Costas, de los equipos implicados en tareas relacionadas con el retorno y del equipo de apoyo a la gestión de la migración es prever el refuerzo operativo y técnico a petición de los Estados miembros, especialmente de aquellos que se enfrentan a retos migratorios desproporcionados. El cumplimiento de las tareas asignadas a los equipos de la Guardia Europea de Fronteras y Costas, de los equipos

[56] Reglamento (UE) n.º 2016/1624 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2016, relativo a la Guardia Europea de Fronteras y Costas y por el que se modifica el Reglamento (UE) n.º 2016/399 del Parlamento Europeo y del Consejo y por el que se deroga 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.

de personal implicados en tareas relacionadas con el retorno y del equipo 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 que se conecte el SIS Central. En caso de que las búsquedas 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 puede llevar a cabo la acción 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.

47) Conforme a la propuesta presentada por la Comisión con respecto a un Reglamento del Parlamento Europeo y del Consejo por el que se crea un Sistema Europeo de Información y Autorización de Viajes (SEIAV)[57], la unidad central 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 personas y sobre documentos de identidad personal vírgenes y expedidos.

48) 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 búsqueda de datos, la calidad de los datos y las normas sobre consulta relativas a los identificadores biométricos, las normas sobre compatibilidad y prioridad de las descripciones, la inclusión de indicaciones, las conexiones entre descripciones, la especificación de nuevas categorías de objetos dentro de la categoría de equipos técnicos y electrónicos, 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 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.

49) Con el fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deberán atribuirse competencias de ejecución a la Comisión. Dichas competencias deberán ejercerse de conformidad con el Reglamento (UE) n.º 182/2011[58]. El procedimiento para la adopción de medidas de ejecución en virtud del presente Reglamento y del Reglamento (UE) 2018/xxx (inspecciones fronterizas) deberá ser el mismo.

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

---

57 COM (2016) 731 final.

58 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, DO L 55 de 28.2.2011, p. 13.

51) 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.

52) 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. En particular, el presente Reglamento aspira a garantizar un entorno seguro para todas las personas que residen en el territorio de la Unión Europea y una protección especial para los niños que pueden ser víctimas de tráfico o sustracción parental, respetando plenamente la protección de los datos de carácter personal.

53) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la adopción del presente Reglamento y no 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 período de seis meses a partir de que el Consejo haya tomado una medida sobre el presente Reglamento, si lo incorpora a su legislación nacional.

54) El Reino Unido participa en el presente Reglamento de conformidad con el artículo 5 del Protocolo sobre el acervo de Schengen integrado en el marco de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y con el artículo 8, apartado 2, de 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 de participar en algunas de las disposiciones del acervo de Schengen[59].

55) Irlanda participa en el presente Reglamento de conformidad con el artículo 5 del Protocolo sobre el acervo de Schengen integrado en el marco de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y con el artículo 6, apartado 2, de 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[60].

56) 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[61], que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE del Consejo[62], relativa a determinadas normas de desarrollo de dicho Acuerdo.

57) 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

[59] DO L 131 de 1.6.2000, p. 43.
[60] DO L 64 de 7.3.2002, p. 20.
[61] DO L 176 de 10.7.1999, p. 36.
[62] DO L 176 de 10.7.1999, p. 31.

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[63] y 2004/860/CE del Consejo[64].

58) Por lo que se refiere a Liechtenstein, la presente Decisión 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[65], 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[66] y el artículo 3 de la Decisión 2011/350/UE del Consejo[67].

59) 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[68].

60) 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.

61) El presente Reglamento deberá aplicarse a Irlanda en las fechas determinadas de conformidad con los procedimientos establecidos en los instrumentos pertinentes relativos a la aplicación del acervo de Schengen a dicho Estado.

---

63 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.

64 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.

65 DO L 160 de 18.6.2011, p. 21.

66 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.

67 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.

68 DO L 166 de 1.7.2010, p. 17.

62) Los costes estimados de la actualización del SIS y de los sistemas nacionales y de la aplicación de las nuevas funcionalidades previstas en el presente Reglamento son inferiores a los importes restantes en la línea presupuestaria para la iniciativa «fronteras inteligentes» en el Reglamento (UE) n.º 515/2014 del Parlamento Europeo y del Consejo[69]. 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.

63) Por consiguiente, procede derogar la Decisión 2007/533/JAI del Consejo y la Decisión 2010/261/UE de la Comisión[70].

64) 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 ...

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 de los capítulos 4 y 5 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 personas y objetos introducidas en el SIS, así como de intercambio de información complementaria y datos adicionales a efectos de la cooperación policial y judicial en materia penal.

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.

---

69 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.

70 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.

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 los artículos 22 y 40, introducidos en el SIS que permiten a las autoridades competentes identificar a una persona o un objeto 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) «datos personales»: toda información sobre una persona física identificada o identificable («interesado»);

(e) «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;

(f) «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;

(g) «respuesta positiva» en el SIS significa que:

(1) un usuario realiza una búsqueda,

(2) la búsqueda 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 búsqueda, y

(4) se requiere la adopción de nuevas medidas;

h) «indicación»: suspensión de la validez de una descripción a nivel nacional que puede añadirse a las descripciones a efectos de una detención, a las descripciones sobre personas desaparecidas y a las descripciones a efectos de controles discretos, específicos y de investigación, cuando un Estado miembro considere que hacer efectiva una descripción introducida es incompatible con su Derecho nacional, con sus obligaciones internacionales o con intereses nacionales esenciales. Cuando se añada una indicación a una descripción, la medida que deba adoptarse basada en la descripción no deberá ejecutarse en el territorio de dicho Estado miembro;

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

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

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

l) «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;

m) «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[71];

n) «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[72].

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;

[71] 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.

[72] 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.

(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, sobre los objetos y los datos enumerados en el artículo 20, apartado 3, letras a) a v), del presente Reglamento relativas a las descripciones sobre personas. 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[73] («la Agencia»). La CS-SIS o la CS-SIS de seguridad podrán contener una copia 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.

[73] 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.

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 53, 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 61, 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 72, 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 adoptarse a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, 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 66, 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 43.

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, los datos utilizados para realizar una consulta, una referencia a los 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 los artículos 40, 41 y 42, 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 desde 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.

7. Cuando los Estados miembros lleven a cabo búsquedas automatizadas escaneadas de las matrículas de vehículos de motor utilizando sistemas de reconocimiento automático de matrículas, deberán mantener un registro de búsqueda de conformidad con la legislación nacional. El contenido de este registro deberá establecerse a través de medidas de ejecución de conformidad con el procedimiento de examen a que se refiere el artículo 72, apartado 2. En caso de respuesta positiva con los datos almacenados en el SIS o con los de una copia nacional o copia técnica de los datos del SIS, se efectuará una búsqueda completa en el SIS con el fin de comprobar la respuesta positiva. Las disposiciones de los apartados 1 a 6 del presente artículo se aplicarán a esta búsqueda completa.

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 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 a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2.

6. La gestión operativa del SIS Central consistirá en todas las funciones necesarias para mantenerlo en funcionamiento ininterrumpido 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 64, 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 40, 41 y 42, 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 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

CATEGORÍAS DE DATOS E INTRODUCCIÓN DE INDICACIONES

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 los artículos 26, 32, 34, 36 y 38.
2. Las categorías de datos serán las siguientes:
   (a) información sobre las personas objeto de una descripción;
   (b) información sobre los objetos citados en los artículos 32, 36 y 38.
3. La información sobre las personas descritas solo contendrá los datos siguientes:
   (c) apellido(s);
   (d) nombre(s);
   (e) nombre(s) de nacimiento;
   (f) nombres usados con anterioridad y alias;
   (g) rasgos físicos particulares, objetivos e inalterables;
   (h) lugar de nacimiento;
   (i) fecha de nacimiento;
   (j) sexo;
   (k) nacionalidad(es);

(l) 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;

(m) motivo de la descripción;

(n) autoridad que emite la descripción;

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

(p) medidas que deben adoptarse;

(q) conexión o conexiones con otras descripciones introducidas en el SIS de conformidad con el artículo 53;

(r) tipo de delito para el que se emitió la descripción;

(s) número de registro de la persona en el registro nacional;

(t) categorización del tipo de persona desaparecida (solo para las descripciones emitidas con arreglo al artículo 32);

(u) categoría del documento de identidad;

(v) país de expedición del documento de identidad;

(w) número del documento de identidad;

(x) fecha de expedición del documento de identidad;

(y) fotografías e imágenes faciales;

(z) perfiles de ADN pertinentes contemplados en el artículo 22, apartado 1, letra b), del presente Reglamento;

(aa) datos dactiloscópicos;

(bb) fotocopia en color del documento de identidad.

4. Las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en los apartados 2 y 3 deberán establecerse y desarrollarse a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2.

5. Las normas técnicas necesarias para la búsqueda de los datos mencionados en el apartado 3 deberán establecerse y desarrollarse con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2. Estas normas técnicas serán iguales para las búsquedas en la CS-SIS, en las copias nacionales y en las copias técnicas, según lo mencionado en el artículo 53, apartado 2, 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 72, apartado 2.

Artículo 21
Proporcionalidad

1. Antes de emitir una descripción y al prorrogar el período 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. Cuando una persona o un objeto sea buscado por un Estado miembro en relación con un delito que entre en el ámbito de aplicación de los artículos 1 a 4 de la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo, el Estado miembro deberá, en cualquier caso, crear la descripción correspondiente, en virtud del artículo 34, 36 o 38, según corresponda.

Artículo 22
Normas específicas para la introducción de fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN

1. La introducción en el SIS de los datos a que se refiere el artículo 20, apartado 3, letras w), x) e y), estará sujeta a las siguientes disposiciones:

   (a) Las fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN solo se introducirán tras ser sometidos a un control de calidad para determinar que cumplen unas normas de calidad mínima de los datos.

   (b) Un perfil de ADN solo podrá añadirse a las descripciones previstas en el artículo 32, apartado 2, letras a) y c), cuando no se disponga de fotografías, imágenes faciales o datos dactiloscópicos pertinentes para la identificación. Los perfiles de ADN de personas que sean descendientes o ascendientes directos o hermanos de la persona objeto de la descripción podrán añadirse a la descripción siempre que dichas personas den su consentimiento explícito. El origen racial de la persona no deberá incluirse en el perfil de ADN.

2. Se establecerán normas de calidad para el almacenamiento de los datos mencionados en el apartado 1, letra a), del presente artículo y en el artículo 40. 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 72, apartado 2.

Artículo 23
Requisitos para la introducción de una descripción

1. No podrá introducirse una descripción sobre una persona sin los datos a que se refieren el artículo 20, apartado 3, letras a), g), k), m) y n) y, cuando proceda, letra p), excepto en las situaciones contempladas en el artículo 40.

2. Además, cuando estén disponibles, se introducirán todos los demás datos a los que se refiere el artículo 20, apartado 3.

Artículo 24
Disposiciones generales sobre la introducción de indicaciones

1. Si un Estado miembro considera que hacer efectiva una descripción introducida de conformidad con los artículos 26, 32 y 36 es incompatible con su legislación nacional, sus obligaciones internacionales o sus intereses nacionales esenciales, podrá posteriormente exigir que se añada una indicación a una descripción, a fin de que la medida que deba adoptarse en relación con la descripción no se ejecute en su territorio. La indicación la añadirá la Oficina SIRENE del Estado miembro emisor.

2. A fin de que los Estados miembros puedan pedir que se añada una indicación a una descripción introducida con arreglo al artículo 26, se notificará automáticamente a todos los Estados miembros toda nueva descripción de esta categoría mediante el intercambio de información complementaria.

3. Si, en casos particularmente urgentes y graves, el Estado miembro emisor solicita la ejecución de la medida, el Estado miembro que ejecute la descripción examinará si puede o no permitir que la indicación añadida a instancia suya se retirada. En caso afirmativo, adoptará las medidas necesarias para garantizar que se adopte inmediatamente la medida requerida.

Artículo 25
Introducción de indicaciones relativas a descripciones para detenciones a efectos de entrega

1. Cuando la Decisión Marco 2002/584/JAI sea aplicable, solo se podrá añadir a una indicación destinada a impedir una detención a efectos de entrega en caso de que la autoridad judicial competente con arreglo a la legislación nacional para la ejecución de una orden de detención europea haya denegado su ejecución acogiéndose a un motivo de no ejecución y cuando se haya pedido añadir la indicación.

2. No obstante, previa solicitud de una autoridad judicial competente con arreglo a la legislación nacional, bien sobre la base de un requerimiento general, bien en un caso específico, también podrá solicitarse que se añada una indicación a una descripción para detención a efectos de entrega cuando sea obvio que tendrá que denegarse la ejecución de la orden europea de detención.

CAPÍTULO VI

DESCRIPCIONES RELATIVAS A PERSONAS BUSCADAS PARA SU DETENCIÓN A EFECTOS DE ENTREGA O EXTRADICIÓN

Artículo 26
Objetivos y condiciones de las descripciones

1. Los datos relativos a personas buscadas para su detención a efectos de entrega al amparo de una orden de detención europea o para su detención a efectos de extradición se introducirán a instancia de la autoridad judicial del Estado miembro emisor.

2. También se introducirán los datos relativos a personas buscadas para su detención a efectos de entrega sobre la base de una orden de detención emitida con arreglo a los acuerdos celebrados entre la Unión y terceros países en virtud del artículo 37 del Tratado de la Unión Europea a efectos de la entrega de personas sobre la base de una orden de detención, que prevén la transmisión de dicha orden de detención a través del SIS.

3. En el presente Reglamento se entenderá que las referencias a las disposiciones de la Decisión Marco 2002/584/JAI incluyen las disposiciones correspondientes de los acuerdos celebrados entre la Unión Europea y terceros países, sobre la base del artículo 37 del Tratado de la Unión Europea a efectos de la entrega de personas sobre la base de una orden de detención que prevean la transmisión de dicha orden de detención a través del SIS.

4. En el caso de una operación de búsqueda que esté activada y tras la autorización de la autoridad judicial competente del Estado miembro emisor, dicho Estado podrá suspender temporalmente una descripción a efectos de detención emitida con arreglo al artículo 26 del presente Reglamento, de tal modo que la descripción no podrá ser consultada por el usuario final y solo será accesible a las Oficinas SIRENE. Esta

funcionalidad solo se utilizará durante un período no superior a 48 horas. Sin embargo, en caso de que sea necesario desde el punto de vista operativo, podrá prorrogarse por períodos sucesivos de 48 horas. Los Estados miembros llevarán estadísticas del número de descripciones en que se haya utilizado esta funcionalidad.

Artículo 27

Datos adicionales sobre personas buscadas para su detención a efectos de entrega

1. En lo que se refiere a personas buscadas para su detención a efectos de entrega al amparo de una orden de detención europea, el Estado miembro emisor introducirá en el SIS una copia del original de la orden de detención europea.

2. El Estado miembro emisor podrá incluir una copia de la traducción de la orden de detención europea en una o más lenguas oficiales de la Unión Europea.

Artículo 28

Información complementaria sobre personas buscadas para su detención a efectos de entrega

El Estado miembro que haya introducido la descripción en el SIS para la detención a efectos de entrega comunicará la información a que se refiere el artículo 8, apartado 1, de la Decisión Marco 2002/584/JAI a los demás Estados miembros mediante el intercambio de información complementaria.

Artículo 29

Información complementaria sobre personas buscadas para su detención a efectos de extradición

1. El Estado miembro que haya introducido la descripción en el SIS a efectos de extradición comunicará los siguientes datos a los demás Estados miembros mediante el intercambio de información complementaria:

   (a) a) la autoridad que emitió la orden de detención;

   (b) b) la existencia de una orden de detención o de un documento que tenga el mismo efecto jurídico, o de una sentencia ejecutoria;

   (c) c) la naturaleza y la tipificación jurídica del delito;

   (d) d) la descripción de las circunstancias en que se cometió el delito, incluidos el momento, el lugar y el grado de participación de la persona mencionada;

   (e) e) en la medida de lo posible, las consecuencias del delito;

   (f) f) cualquier otra información útil o necesaria para la ejecución de la descripción.

2. Los datos mencionados en el apartado 1 no se comunicarán cuando los datos a que se refieren los artículos 27 o 28 ya se hayan facilitado y se considere que son suficientes para que el Estado miembro de que se trate ejecute la descripción.

Artículo 30
Conversión de las descripciones relativas a personas buscadas para su detención a efectos de entrega o extradición

Cuando no fuera posible proceder a la detención, bien por una decisión denegatoria del Estado miembro requerido, de conformidad con el procedimiento de introducción de indicaciones establecido en los artículos 24 o 25, bien porque, en el caso de una descripción para la detención a efectos de extradición, la investigación no hubiese concluido, el Estado miembro requerido deberá considerar la descripción como una descripción con vistas a la comunicación del paradero de la persona de que se trate.

Artículo 31
Ejecución de la medida requerida por la descripción relativa a una persona buscada para su detención a efectos de entrega o extradición

1. Las descripciones introducidas en el SIS con arreglo al artículo 26, junto con los datos adicionales a que se refiere el artículo 27, constituirán y tendrán los mismos efectos que una orden de detención europea dictada de conformidad con la Decisión Marco 2002/584/JAI, cuando esta sea aplicable.

2. En los casos en que no sea aplicable la Decisión Marco 2002/584/JAI, una descripción introducida en el SIS de conformidad con los artículos 26 y 29 surtirá los mismos efectos que una solicitud de detención provisional con arreglo al artículo 16 del Convenio Europeo de Extradición, de 13 de diciembre de 1957, o al artículo 15 del Tratado Benelux de extradición y asistencia judicial en materia penal, de 27 de junio de 1962.

CAPÍTULO VII

DESCRIPCIONES RELATIVAS A PERSONAS DESAPARECIDAS

Artículo 32
Objetivos y condiciones de las descripciones

1. Los datos relativos a personas desaparecidas u otras personas que deban ser puestas bajo protección, o cuyo paradero sea preciso determinar, se introducirán en el SIS a petición de la autoridad competente del Estado miembro que emita la descripción.

2. Podrán introducirse datos sobre las siguientes categorías de personas desaparecidas:

   (a) personas desaparecidas que deban ser puestas bajo protección:

      i) para su propia protección;

      ii) para prevenir amenazas;

   (b) personas desaparecidas que no sea necesario poner bajo protección.

   (c) niños en riesgo de sustracción de conformidad con el apartado 4.

3. El apartado 2, letra a), se aplicará en particular a los menores y a las personas que deban ser internadas por resolución de una autoridad competente.

4. La descripción relativa a un menor al que se hace referencia en el apartado 2, letra c), se introducirá a instancia de la autoridad judicial competente del Estado miembro que sea competente en asuntos de responsabilidad parental de conformidad con el

Reglamento n.º 2201/2003[74] cuando exista un riesgo concreto y evidente de que el menor podría ser trasladado inminentemente de forma ilegal desde el Estado miembro al que pertenezca la autoridad judicial competente. En los Estados miembros que son partes en el Convenio de La Haya, de 19 de octubre de 1996, relativo a la competencia judicial, la ley aplicable, el reconocimiento, la ejecución y la cooperación en materia de responsabilidad parental y medidas de protección de los niños, y en los que el Reglamento n.º 2201/2003 no sea aplicable, las disposiciones del Convenio de La Haya serán aplicables.

5. Los Estados miembros velarán por que los datos introducidos en el SIS indiquen a cuál de las categorías previstas en el apartado 2 pertenece la persona desaparecida. Además, los Estados miembros también velarán por que los datos introducidos en el SIS indiquen de qué tipo de persona vulnerable se trata. Las normas relativas a la categorización de los tipos de casos y la introducción de estos datos deberán establecerse y desarrollarse a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2.

6. Cuatro meses antes de que un niño que sea objeto de una descripción prevista en el presente artículo alcance la edad adulta, la CS-SIS notificará automáticamente al Estado miembro emisor el motivo por el que la descripción y las medidas han de actualizarse o que la descripción debe suprimirse.

7. Cuando haya indicios claros de que vehículos, embarcaciones o aeronaves están relacionadas con una persona que sea objeto de una descripción con arreglo al apartado 2, podrán emitirse descripciones relativas a dichos vehículos, embarcaciones y aeronaves para localizar a la persona. En estos casos, podrá establecerse una conexión entre la descripción de la persona desaparecida y la descripción del objeto con arreglo a lo dispuesto en el artículo 60. Las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos a que se refiere el presente apartado serán establecidas y desarrolladas a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2.

Artículo 33
Ejecución de medidas basadas en una descripción

1. Cuando se localice a una persona mencionada en el artículo 32, las autoridades competentes, sin perjuicio de lo dispuesto en el apartado 2, comunicarán su paradero al Estado miembro emisor. En el caso de la desaparición de niños o de niños que deban ser puestos bajo protección, el Estado miembro de ejecución consultará inmediatamente al Estado miembro emisor, a fin de llegar a un acuerdo lo antes posible acerca de las medidas que deban adoptarse para salvaguardar el interés superior del menor. Las autoridades competentes podrán, en los casos contemplados en el artículo 32, apartado 2, letras a) y c), trasladar a la persona a un lugar seguro para impedir que continúe su viaje, si así lo autoriza la legislación nacional.

2. Toda comunicación, con excepción de la que tenga lugar entre autoridades competentes, de datos relativos a una persona desaparecida que haya sido localizada y sea mayor de edad, estará subordinada al consentimiento de esta. No obstante, las

[74] Reglamento (CE) n.º 2201/2003 del Consejo, de 27 de noviembre de 2003, relativo a la competencia, el reconocimiento y la ejecución de resoluciones judiciales en materia matrimonial y de responsabilidad parental, por el que se deroga el Reglamento (CE) n.º 1347/2000, DO L 338 de 23.12.2003, p. 1.

autoridades competentes podrán comunicar el hecho de que se ha borrado la descripción debido a que la localización de la persona desaparecida ha sido comunicada a la persona que comunicó la desaparición.

CAPÍTULO VIII

DESCRIPCIONES RELATIVAS A PERSONAS BUSCADAS A EFECTOS DE UN PROCEDIMIENTO JUDICIAL

Artículo 34
Objetivos y condiciones para emitir una descripción

1. A efectos de la comunicación del lugar de residencia o del domicilio de las personas, los Estados miembros, previa solicitud de la autoridad competente, introducirán en el SIS los datos relativos a:

   (a) testigos;

   (b) personas citadas o buscadas para que comparezcan ante las autoridades judiciales en el marco de un proceso penal para responder de los hechos que se les imputan;

   (c) personas a las que se deba notificar una sentencia penal u otros documentos relacionados con procesos penales con el fin de responder de los hechos que se les imputan;

   (d) personas a las que se deba notificar un requerimiento para que comparezcan a fin de que cumplan una pena privativa de libertad.

2. Cuando haya indicios claros de que vehículos, embarcaciones o aeronaves estén relacionados con una persona objeto de una descripción con arreglo al apartado 1, podrán emitirse descripciones relativas a dichos vehículos, embarcaciones y aeronaves para localizar a la persona. En tales casos, deberá establecerse una conexión entre las descripciones relativas a la persona y al objeto con arreglo a lo dispuesto en el artículo 60. Las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos a que se refiere el presente apartado serán establecidas y desarrolladas a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2.

Artículo 35
Ejecución de la acción basada en una descripción

La información solicitada se comunicará al Estado miembro emisor mediante el intercambio de información complementaria.

CAPÍTULO IX

DESCRIPCIONES RELATIVAS A PERSONAS Y OBJETOS A EFECTOS DE CONTROLES DISCRETOS, ESPECÍFICOS O DE INVESTIGACIÓN

Artículo 36
Objetivos y condiciones de las descripciones

1. Los datos relativos a personas o vehículos, embarcaciones, aeronaves y contenedores serán introducidos, de conformidad con la legislación nacional del Estado miembro emisor, a efectos de controles discretos, específicos o de investigación de conformidad con el artículo 37, apartado 4.

2. La descripción podrá emitirse para el enjuiciamiento de delitos, la ejecución de una condena penal y la prevención de amenazas para la seguridad pública:

   (a) cuando haya indicios claros de que una persona pretende cometer o está cometiendo un delito grave, en particular alguno de los mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI;

   (b) cuando la información mencionada en el artículo 37, apartado 1, sea necesaria para la ejecución de una condena penal de una persona condenada por un delito grave, en particular alguno de los mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI; o

   (c) cuando la apreciación general de una persona, en particular sobre la base de hechos delictivos anteriores, permita suponer que también podría cometer delitos graves en el futuro, en particular alguno de los mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI.

3. Además, podrá emitirse una descripción de conformidad con la legislación nacional a instancia de las autoridades competentes para la seguridad del Estado, cuando haya indicios concretos de que la información mencionada en el artículo 37, apartado 1, es necesaria con objeto de evitar una amenaza grave por parte del interesado u otras amenazas graves para la seguridad nacional interior o exterior. El Estado miembro que emita una descripción con arreglo al presente apartado informará de ello a los demás Estados miembros. Cada Estado miembro determinará a qué autoridades se transmitirá esta información.

4. Cuando haya indicios claros de que vehículos, embarcaciones, aeronaves y contenedores están relacionados con los delitos graves a que se refiere el apartado 2 o con las amenazas graves a que se refiere el apartado 3, podrán emitirse descripciones relativas a dichos vehículos, embarcaciones, aeronaves y contenedores.

5. Cuando haya indicios claros de que documentos oficiales vírgenes o documentos de identidad expedidos están relacionados con los delitos graves a que se refiere el apartado 2 o con las amenazas graves contempladas en el apartado 3, podrán emitirse descripciones relativas a dichos documentos, con independencia de la identidad del poseedor original del documento de identidad, si lo hubiera. Las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos a que se refiere el presente apartado serán establecidas y desarrolladas a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2.

Artículo 37
Ejecución de medidas basadas en una descripción

1. En el marco de controles discretos, específicos o de investigación, la totalidad o parte de los datos siguientes deberán ser recopilados y remitidos a la autoridad que emitió la descripción, con motivo de controles fronterizos, controles de policía y de aduanas u otras actividades policiales realizadas en un Estado miembro:

   (a) el hecho de que se ha localizado a la persona o el vehículo, embarcación, aeronave, contenedor, documento oficial virgen o documento de identidad objeto de la descripción;

   (b) el lugar, la hora y la razón del control;

   (c) el itinerario y el destino del viaje;

   (d) las personas que acompañaban a la persona en cuestión o los ocupantes del vehículo, embarcación o aeronave, o que acompañaban al titular del documento oficial virgen o del documento de identidad que pueda suponerse razonablemente que tienen relación con las persona en cuestión;

   (e) la identidad revelada y la descripción de la persona que utilizaba el documento oficial virgen o el documento de identidad objeto de la descripción;

   (f) el vehículo, embarcación, aeronave o contenedor utilizado;

   (g) los objetos transportados, incluidos los documentos de viaje;

   (h) las circunstancias en las que se localizó a la persona o el vehículo, embarcación, aeronave, contenedor, documento oficial virgen o documento de identidad expedido.

2. La información a que se refiere el apartado 1 se comunicará mediante el intercambio de información complementaria.

3. En función de las circunstancias operativas y de conformidad con la legislación nacional, un control discreto comprenderá un control rutinario de una persona o un objeto con vistas a recabar la mayor información posible descrita en el apartado 1 sin poner en peligro la naturaleza discreta del control.

4. En función de las circunstancias operativas, y de conformidad con la legislación nacional, la investigación comprenderá un control y un interrogatorio de la persona más exhaustivos. Cuando la legislación de un Estado miembro no autorice las investigaciones, estas deberán sustituirse por controles discretos en dicho Estado miembro.

5. Durante los controles específicos, las personas, vehículos, embarcaciones, aeronaves, contenedores y objetos transportados podrán ser registrados con arreglo a la legislación nacional, para cumplir la finalidad contemplada en el artículo 36. Las búsquedas se llevarán a cabo de acuerdo con la legislación nacional. Cuando los controles específicos no estén autorizados en virtud de la legislación de un Estado miembro, se sustituirán por controles discretos en dicho Estado miembro.

CAPÍTULO X

DESCRIPCIONES DE OBJETOS PARA SU INCAUTACIÓN O UTILIZACIÓN COMO PRUEBA EN UN PROCESO PENAL

Artículo 38
Objetivos y condiciones para emitir descripciones

1. Los datos relativos a objetos buscados con vistas a su incautación, a efectos policiales o como pruebas en un proceso penal se introducirán en el SIS.

2. Se introducirán las siguientes categorías de objetos fácilmente identificables:

   a) vehículos de motor, definidos por la legislación nacional, independientemente de su sistema de propulsión;

   b) remolques de un peso en vacío superior a 750 kg;

   c) caravanas;

   d) equipos industriales;

   e) embarcaciones;

   f) motores de embarcaciones;

   g) contenedores;

   h) aeronaves;

   i) armas de fuego;

   j) documentos oficiales vírgenes que hayan sido robados, sustraídos o extraviados;

   k) documentos de identidad expedidos, tales como pasaportes, tarjetas de identidad, permisos de conducción, permisos de residencia y documentos de viaje expedidos que hayan sido robados, sustraídos, extraviados o anulados, o que pretendan pasar por uno de estos documentos, pero que sean falsificaciones;

   l) certificados de matriculación de vehículos y placas de matrícula de vehículos que hayan sido robados, sustraídos, extraviados, o anulados o que pretendan pasar por uno de estos documentos o placas, pero que sean falsificaciones;

   m) billetes de banco (billetes registrados) y billetes falsificados;

   n) equipos técnicos, artículos de tecnología de la información y otros objetos de alto valor fácilmente identificables;

   o) componentes identificables de vehículos de motor;

   p) componentes identificables de equipos industriales.

3. La definición de nuevas subcategorías de objetos con arreglo al apartado 2, letra n), y de las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos enumerados en el apartado 2 se establecerán y desarrollarán a través de medidas de ejecución con arreglo al procedimiento de examen a que se refiere el artículo 72, apartado 2.

Artículo 39
Adopción de medidas basadas en una descripción

1. Cuando como resultado de una búsqueda se compruebe la existencia de una descripción relativa a un objeto que haya sido localizado, la autoridad que haya efectuado el hallazgo incautará el objeto de conformidad con la legislación nacional y se pondrá en contacto con la autoridad emisora para decidir las medidas necesarias. A tal fin, también podrán transmitirse datos personales de conformidad con el presente Reglamento.
2. La información a que se refiere el apartado 1 se comunicará a través del intercambio de información complementaria.
3. El Estado miembro que haya localizado el objeto deberá adoptar las medidas solicitadas de conformidad con su legislación nacional.

CAPÍTULO XI

DESCRIPCIONES RELATIVAS A PERSONAS DESCONOCIDAS BUSCADAS PARA SU IDENTIFICACIÓN EN VIRTUD DE LA LEGISLACIÓN NACIONAL Y BÚSQUEDA CON DATOS BIOMÉTRICOS

Artículo 40
Descripciones relativas a personas desconocidas buscadas a efectos de su detención con arreglo a la legislación nacional

En el SIS podrán introducirse datos dactiloscópicos no relacionados con personas que sean objeto de descripciones. Estos datos serán grupos completos o incompletos de impresiones dactilares o impresiones palmares descubiertas en los lugares de delitos investigados, de delitos graves y de delitos de terrorismo cuando pueda demostrarse con un alto grado de probabilidad que pertenecen al autor del delito. Los datos dactiloscópicos de esta categoría se almacenarán como correspondientes a «persona sospechosa o persona desconocida buscada», siempre que las autoridades competentes no puedan determinar la identidad de la persona utilizando cualquier otra base de datos nacional, europea o internacional.

Artículo 41
Adopción de medidas basadas en una descripción

En caso de una respuesta positiva o de una correspondencia potencial con los datos almacenados con arreglo al artículo 40, la identidad de la persona se establecerá de conformidad con la legislación nacional, junto con la comprobación de que los datos dactiloscópicos almacenados en el SIS pertenecen a dicha persona. Los Estados miembros lo comunicarán utilizando información complementaria a fin de facilitar un rápido examen del asunto.

Artículo 42

Normas específicas para la verificación o la búsqueda con fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN

1. En el SIS se consultarán fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN con objeto de verificar la identidad de una persona que haya sido localizada a resultas 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 consultarán a efectos de identificación si la identidad de la persona no puede determinarse por otros medios.

3. Los datos dactiloscópicos almacenados en el SIS en relación con descripciones emitidas de conformidad con el artículo 26, el artículo 34, apartado 1, letras b) y d), y el artículo 36 podrán también consultarse utilizando conjuntos completos o incompletos de impresiones dactilares o impresiones palmares hallados 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 dispongan de la posibilidad de 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 en los que se utilicen sistemas de autoservicio y sistemas automatizados de control de fronteras.

CAPÍTULO XII

DERECHO DE ACCESO A LAS DESCRIPCIONES Y PERÍODO DE CONSERVACIÓN DE ESTAS

Artículo 43

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 en materia de:

   a) control de fronteras, de conformidad con el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre un código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen);

   b) 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.

2. 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 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 introducidos en el SIS y a consultarlos directamente, podrán ser ejercidos por las autoridades competentes de la ejecución de las tareas a que se refiere el apartado 1, letra c), en la realización de dichas tareas. El acceso 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 53, apartado 8.

Artículo 44
Autoridades responsables de la matriculación de vehículos

1. Los servicios de los Estados miembros competentes para la expedición de los certificados de matriculación de vehículos con arreglo a la Directiva 1999/37/CE del Consejo[75] tendrán acceso a los siguientes datos introducidos en el SIS de conformidad con el artículo 38, apartado 2, letras a), b), c) y l) de dicho Reglamento con el único fin de comprobar si los vehículos presentados para su matriculación han sido robados, sustraídos o extraviados o son requeridos como pruebas en un proceso penal:

   a) datos sobre vehículos de motor, tal y como se definen en la legislación nacional, independientemente del sistema de propulsión;

   b) datos sobre remolques de un peso en vacío superior a 750 kg y caravanas;

   c) datos sobre certificados de matriculación de vehículos y placas de matriculación de vehículos que hayan sido robados, sustraídos, extraviados o anulados.

   El acceso a dichos datos por parte de los servicios competentes para la expedición de certificados de matriculación de vehículos estará regulado por la legislación nacional de dicho Estado miembro.

2. Cuando los servicios a los que se refiere el apartado 1 sean servicios públicos, tendrán derecho a acceder directamente a los datos introducidos en el SIS.

3. Cuando los servicios a los que se refiere el apartado 1 no sean servicios públicos, tendrán acceso a los datos incluidos en el SIS solo a través de una de las autoridades a que se refiere el artículo 43 del presente Reglamento. Tal autoridad tendrá derecho a acceder a los datos directamente y transmitirlos al servicio interesado. El Estado miembro de que se trate velará por que el servicio en cuestión y sus empleados respeten todas las limitaciones de utilización de los datos que la autoridad les comunique.

4. El artículo 39 del presente Reglamento no se aplicará al acceso obtenido de conformidad con el presente artículo. La comunicación a las autoridades policiales o

[75] Directiva 1999/37 del Consejo, de 29 de abril de 1999, relativo a los documentos de matriculación de los vehículos, DO L 138 de 1.6.1999, p. 57.

judiciales por parte de los servicios a que se refiere el apartado 1 de información obtenido mediante el acceso al SIS que suscite la sospecha de la comisión de un delito se regirá por la legislación nacional.

Artículo 45
Autoridades de registro de buques y aeronaves

1. Los servicios de los Estados miembros competentes para la expedición de certificados de matriculación o de la gestión del tráfico de embarcaciones, incluidos los motores de embarcaciones, y de aeronaves, tendrán acceso a los siguientes datos introducidos en el SIS de conformidad con lo dispuesto en el artículo 38, apartado 2, del presente Reglamento con el único fin de comprobar si las embarcaciones, incluidos los motores de embarcaciones, las aeronaves o los contenedores presentados para su matriculación o sujetos a la gestión del tráfico han sido robados, sustraídos o extraviados o son requeridos como pruebas en un proceso penal:

   a) datos sobre embarcaciones;

   b) datos sobre motores de embarcaciones;

   c) datos sobre aeronaves.

   Sin perjuicio de lo dispuesto en el apartado 2, el acceso a estos datos por parte de dichos servicios estará regulado por la legislación de cada Estado miembro. El acceso a los datos indicados en las letras a) a c) se limitará a la competencia específica de los servicios de que se trate.

2. Los servicios a los que se refiere el apartado 1 que sean servicios públicos tendrán derecho a acceder directamente a los datos incluidos en el SIS.

3. Los servicios a los que se refiere el apartado 1 que no sean servicios públicos tendrán acceso a los datos incluidos en el SIS solo a través de una de las autoridades a que se refiere el artículo 43 del presente Reglamento. Esta autoridad tendrá derecho a acceder a los datos directamente y transmitirlos al servicio interesado. El Estado miembro de que se trate velará por que el servicio en cuestión y sus empleados respeten todas las limitaciones de utilización de los datos que la autoridad les comunique.

4. El artículo 39 del presente Reglamento no se aplicará al acceso obtenido de conformidad con el presente artículo. La comunicación a las autoridades policiales o judiciales por parte de los servicios a que se refiere el apartado 1 de información obtenida mediante el acceso al SIS que suscite la sospecha de la comisión de un delito se regirá por la legislación nacional.

Artículo 46
Acceso a los datos del SIS por parte de Europol

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 búsqueda 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, su tratamiento por parte de Europol 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 pedir más información al Estado miembro en cuestión con arreglo a lo dispuesto en el Reglamento (UE) 2016/794.

5. Europol deberá:

   a) sin perjuicio de lo dispuesto en los apartados 3, 4 y 6, no conectar las partes del SIS a las que acceda ni transferir los datos contenidos en las mismas a ningún sistema informático para el tratamiento y la recopilación de datos gestionado por Europol o que se halle en sus locales, ni descargar ni copiar de otra 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 realizadas por 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 dicha copia sea necesaria para que los miembros del personal de Europol debidamente autorizados efectúen una búsqueda directa. Las disposiciones del presente Reglamento se aplicarán a esas copias. La copia técnica se utilizará con fines de almacenamiento de datos del SIS, mientras dichos datos son consultados. Una vez que 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 las descripciones y datos adicionales emitidos por Estados miembros u por la CS-SIS en 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 período máximo de 48 horas. Dicho período podrá prorrogarse en 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 mencionadas en los apartados 2 a 7 se apliquen adecuadamente.

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

Artículo 47
Acceso a los datos del SIS por parte de Eurojust

1. Con arreglo a su mandato, los miembros nacionales de Eurojust y sus asistentes tendrán derecho a acceder a los datos introducidos en el SIS y a consultarlos con arreglo a los artículos 26, 32, 34, 38 y 40.

2. En caso de que una búsqueda efectuada por un miembro nacional de Eurojust revele la existencia de una descripción en el SIS, informará al Estado miembro emisor.

3. Nada en el presente artículo deberá interpretarse en el sentido de que afecte a las disposiciones de la Decisión 2002/187/JAI relativas a la protección de datos y a la responsabilidad por el tratamiento no autorizado o incorrecto de esos datos por parte de los miembros nacionales de Eurojust o de sus asistentes, ni a las facultades de la Autoridad Común de Control establecida de conformidad con dicha Decisión.

4. Cada acceso y cada consulta que efectúe un miembro nacional de Eurojust o un asistente quedará registrada de conformidad con lo dispuesto en el artículo 12, así como toda utilización que hayan hecho de los datos a los que han tenido acceso.

5. Ninguna parte del SIS se conectará a ningún sistema informático de recopilación y tratamiento de datos gestionado o alojado por Eurojust y los datos contenidos en el SIS a que los miembros nacionales o sus asistentes tengan acceso no se transferirán a dicho sistema informático. Ninguna parte del SIS será descargada. El registro del acceso y las búsquedas no deberán interpretarse como descarga ilegal ni copia de datos del SIS.

6. El acceso a los datos introducidos en el SIS se limitará a los miembros nacionales y sus asistentes y no se extenderá al personal de Eurojust.

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

Artículo 48

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 los miembros del equipo 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 buscar 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 49, apartado 1.

3. En caso de que una búsqueda por parte de un miembro de los equipos de la Guardia Europea de Fronteras y Costas implicado en tareas relacionadas con el retorno o por un miembro del equipo de apoyo a la gestión de la migración revele la existencia de una descripción en el SIS, el Estado miembro emisor deberá ser informado al respecto. 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 en virtud de 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 un miembro del equipo de apoyo a la gestión de la migración será registrada 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 a los equipos de personal implicados en tareas relacionadas con el retorno o a un miembro del equipo de apoyo a la gestión de la migración y no se extenderá a los demás miembros del equipo.

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

Artículo 49

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

1. A efectos del artículo 48, apartado 1, y del apartado 2 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.

2. 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 artículos 26, 32, 34, 36 y 38, apartado 2, letras j) y k).

3. Cuando una verificación realizada por la Agencia Europea de la Guardia de Fronteras y Costas revele la existencia de una descripción en el SIS, será aplicable el procedimiento enunciado en el artículo 22 del Reglamento por el que se crea un Sistema Europeo de información y Autorización de Viajes (SEIAV).

4. 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.

5. 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 de los datos a los que se haya accedido.

6. 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. Ninguna parte del SIS será descargada. El registro de los accesos y consultas no se considerará descarga o copia de datos del SIS.

7. Las medidas para garantizar la seguridad y la confidencialidad contempladas en los artículos 10 y 11 deberán ser adoptadas y aplicadas por la Agencia Europea de la Guardia de Fronteras y Costas.

Artículo 50
Alcance del acceso

Los usuarios, incluidos Europol, los miembros nacionales de Eurojust y sus asistentes, así como la Agencia Europea de la Guardia de Fronteras y Costas, podrán acceder únicamente a los datos que precisen para el cumplimiento de sus funciones.

Artículo 51
Período de conservación de las descripciones

1. Las descripciones 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 el plazo de cinco años a partir de la introducción de una descripción en el SIS el Estado miembro emisor examinará la necesidad de mantenerla. Las descripciones a efectos del artículo 36 del presente Reglamento, se conservarán durante un período máximo de un año.

3. Las descripciones relativas a documentos oficiales vírgenes y a documentos de identidad introducidos con arreglo al artículo 38 se conservarán por un período máximo de 10 años. Podrán establecerse períodos de conservación más breves para las categorías de descripciones de objetos a través de medidas de ejecución adoptadas de conformidad con el procedimiento de examen contemplado en el artículo 72, apartado 2.

4. En su caso, cada Estado miembro fijará unos plazos de examen más cortos con arreglo a su legislación nacional.

5. 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 ha de ser suprimida del SIS, deberá notificarlo a la autoridad que ha creado la descripción para que esta plantee la cuestión a autoridad. La autoridad dispondrá de un plazo de 30 días naturales desde la recepción de esta notificación para indicar que la notificación ha sido o será suprimida o deberá motivar la conservación de la descripción. Si el plazo de 30 días expira sin dicha 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.

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

7. Las descripciones se borrarán automáticamente una vez transcurrido el período de revisión a que se refiere el apartado 2, salvo en caso de que el Estado miembro emisor haya comunicado a la CS-SIS la prórroga de la descripción con arreglo al apartado 6. La CS-SIS informará automáticamente a los Estados miembros de la supresión programada de datos del sistema, con un preaviso de cuatro meses.

8. Los Estados miembros llevarán estadísticas del número de descripciones cuyo período de conservación se haya prorrogado con arreglo al apartado 6.

CAPÍTULO XIII

SUPRESIÓN DE DESCRIPCIONES

Artículo 52
Supresión de descripciones

1. Las descripciones para la detención a efectos de entrega o extradición en virtud del artículo 26 se suprimirán una vez la persona haya sido entregada o extraditada a las autoridades competentes del Estado miembro emisor. Podrán también suprimirse cuando la resolución judicial en la que se basó la descripción haya sido revocada por la autoridad judicial competente con arreglo a la legislación nacional.

2. Las descripciones de personas desaparecidas se suprimirán de conformidad con las siguientes normas:

   (a) En lo relativo a los menores desaparecidos, con arreglo al artículo 32, deberá suprimirse la descripción:

   – en caso de resolución del asunto, por ejemplo, cuando el menor haya sido repatriado o las autoridades competentes del Estado miembro de ejecución adopten una resolución sobre su custodia;

   – cuando la descripción expire de conformidad con el artículo 51;

   – cuando la autoridad competente del Estado miembro emisor adopte una decisión; o

   – cuando se localice al menor.

   b) En lo relativo a los adultos desaparecidos contemplados en el artículo 32 con respecto a los cuales no se exijan medidas de protección, deberá suprimirse la descripción:

   – cuando se haya ejecutado la medida que debe adoptarse (paradero determinado por el Estado miembro de ejecución);

   – cuando expire la descripción de conformidad con el artículo 51; o

   – cuando la autoridad competente del Estado miembro emisor adopte una decisión.

   c) En lo relativo a adultos desaparecidos con respecto a los cuales se exijan medidas de protección, de conformidad con el artículo 32, deberá suprimirse la descripción:

   – cuando se haya ejecutado la medida que debe adoptarse (persona puesta bajo protección);

   – cuando expire la descripción de conformidad con el artículo 51; o

   – cuando la autoridad competente del Estado miembro emisor adopte una decisión.

Con arreglo a la legislación nacional, cuando una persona haya sido internada por resolución de una autoridad competente, la descripción podrá mantenerse hasta que la persona haya sido repatriada.

3. Las descripciones sobre personas buscadas a efectos de un procedimiento judicial se suprimirán con arreglo a las siguientes normas:

Con respecto a las descripciones sobre personas buscadas a efectos de un procedimiento judicial con arreglo al artículo 34, deberá suprimirse la descripción:

a) cuando se haya comunicado el paradero de la persona a la autoridad competente del Estado miembro emisor. Si la información enviada no puede dar lugar a la adopción de medidas, la Oficina SIRENE del Estado miembro emisor se pondrá en contacto con la Oficina SIRENE del Estado miembro de ejecución para resolver el problema;

b) cuando expire la descripción de conformidad con el artículo 51; o

c) cuando la autoridad competente del Estado miembro emisor adopte una decisión.

Si se ha obtenido una respuesta positiva en un Estado miembro y los detalles relativos a la dirección se enviaron al Estado miembro emisor y una respuesta positiva posterior en dicho Estado miembro revela los mismos datos, la respuesta positiva se registrará en el Estado miembro de ejecución, pero ni los detalles relativos a la dirección ni la información complementaria se reenviará al Estado miembro emisor. En tales casos, el Estado miembro de ejecución comunicará al Estado miembro emisor las respuestas positivas repetidas, y el Estado miembro emisor considerará la necesidad de mantener la descripción.

4. Las descripciones sobre controles discretos, específicos y de investigación se suprimirán con arreglo a las siguientes normas:

En lo que respecta a descripciones sobre controles discretos, específicos y de investigación, de conformidad con el artículo 36, deberá suprimirse la descripción:

(a) cuando esta expire de conformidad con el artículo 51;

(b) cuando la autoridad competente del Estado miembro emisor así lo decida.

5. Las descripciones de objetos para su incautación o utilización como pruebas se suprimirán con arreglo a las siguientes normas:

Con respecto a la supresión de descripciones de objetos para su incautación o utilización como pruebas en un proceso penal con arreglo al artículo 38, deberá suprimirse la descripción:

(a) cuando se haya incautado el objeto o se haya ejecutado la medida equivalente una vez que se haya producido el necesario intercambio de información complementaria de seguimiento entre las Oficinas SIRENE o que el objeto haya pasado a ser objeto de otro procedimiento administrativo o judicial;

(b) cuando expire la descripción; o

(c) cuando la autoridad competente del Estado miembro emisor así lo decida.

6. Las descripciones relativas a personas desconocidas buscadas en virtud del artículo 40 se suprimirán cuando:

7. a) se haya identificado a la persona; o

8. b) expire la descripción.

CAPÍTULO XIV

NORMAS GENERALES DE TRATAMIENTO DE DATOS

Artículo 53
Tratamiento de datos del SIS

1. Los Estados miembros podrán tratar los datos contemplados en el artículo 20 únicamente para los fines enunciados para cada una de las categorías de descripciones mencionadas en los artículos 26, 32, 34, 36, 38 y 40.

2. Los datos solo podrán ser copiados con fines técnicos, siempre que dicha copia sea necesaria para la consulta directa por las autoridades mencionadas en el artículo 43. Las disposiciones del presente Reglamento se aplicarán a esas copias. Un Estado miembro no deberá copiar las descripciones y datos adicionales introducidos por otro Estado miembro desde su N.SIS o del 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 por un período máximo de 48 horas. Este período de conservación podrá prorrogarse en caso de emergencia hasta que haya finalizado la misma.

4. 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.

5. 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 43 y al personal debidamente autorizado.

6. Por lo que respecta a las descripciones previstas en los artículos 26, 32, 34, 36, 38 y 40 del presente Reglamento, todo tratamiento de la información contenida en las mismas para fines distintos de aquellos para los que se introdujo en el SIS deberá estar relacionada con un caso concreto y justificarse por la necesidad de prevenir una amenaza grave e inminente para el orden y la seguridad públicos, por razones graves de seguridad del Estado o con vistas a prevenir un delito grave. Deberá obtenerse la autorización previa del Estado miembro emisor con este fin.

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

8. Cada Estado miembro enviará a la Agencia, una lista de las autoridades competentes que estén autorizadas a consultar directamente los datos contenidos en el SIS en virtud del 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 54
Datos del SIS y ficheros nacionales

1. El artículo 53, apartado 2, se entenderá sin perjuicio del derecho de un Estado miembro a conservar en los ficheros nacionales datos del SIS en relación con los cuales se haya tomado una medida en su territorio. Dichos datos se conservarán en los ficheros nacionales durante un período máximo de tres años, salvo si la legislación nacional contiene disposiciones específicas que prevean un período de conservación más largo.

2. El artículo 53, 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 introducida en el SIS por ese Estado miembro.

Artículo 55
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 56
Calidad de los datos tratados en el SIS

1. El Estado miembro emisor será responsable de la exactitud y actualidad de los datos y 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 salieron a la luz en primer lugar 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 59.

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 57
Incidentes relativos a la seguridad

1. Cualquier acontecimiento que repercuta o pueda repercutir en la seguridad del SIS y pueda causar daños o pérdidas de datos al SIS será considerado un incidente relativo a la seguridad, especialmente cuando se haya podido acceder a los datos o cuando 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 a la autoridad nacional de supervisión 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 facilitados por la Agencia.

Artículo 58
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 56, 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 59
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

   c) apellido(s) de soltera

   d) nombres y apellidos anteriores y los 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) fotografías e imágenes faciales

   j) impresiones dactilares

   k) nacionalidad o nacionalidades

   l) categoría de documento personal de identidad

   m) país de expedición del documento personal de identidad

   n) número(s) del documento personal 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 la introducción, actualización y supresión de los datos enumerados en el apartado 3 se establecerán a través de las medidas de aplicación establecidas y desarrolladas de conformidad con el procedimiento de examen contemplado en el artículo 72, 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 60
Conexiones entre descripciones

1. Un Estado miembro podrá crear una conexión entre las descripciones que introduzca 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 a partir de cada descripción conectada, ni al período 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 la conexión 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 parte de 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 sobre conexiones entre descripciones deberán establecerse y desarrollarse de conformidad con el procedimiento de examen contemplado en el artículo 72, apartado 2.

Artículo 61
Finalidad y período 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 para 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 la descripción correspondiente del SIS.

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 período durante el que podrán conservarse dichos datos en esos ficheros se regirá por la legislación nacional.

Artículo 62
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.

Artículo 63
Intercambio con Interpol de información sobre pasaportes robados, sustraídos, extraviados o anulados

1. No obstante lo dispuesto en el artículo 62, los datos relativos al número de pasaporte, el país de expedición y el tipo de pasaporte robado, sustraído, extraviado o anulado introducidos en el SIS podrán intercambiarse con los miembros de Interpol mediante el establecimiento de una conexión entre el SIS y la base de datos de Interpol sobre documentos de viaje robados o desaparecidos, previa celebración de un acuerdo entre Interpol y la Unión Europea. En el acuerdo se establecerá que la transmisión de los datos introducidos por un Estado miembro estará supeditada al consentimiento de dicho Estado miembro.

2. El acuerdo a que se refiere el apartado 1 dispondrá que solo puedan acceder a los datos intercambiados los miembros de Interpol de aquellos países que garanticen un nivel adecuado de protección de los datos personales. Antes de celebrar dicho acuerdo, el Consejo pedirá el dictamen de la Comisión sobre la idoneidad del nivel de protección de los datos personales y de respeto de los derechos y libertades fundamentales en lo que atañe al tratamiento automatizado de datos personales por parte de Interpol y de los países que hayan destinado miembros a dicha organización.

3. El acuerdo a que se refiere el apartado 1 también permitirá que los Estados miembros accedan a través del SIS a los datos de la base de datos de Interpol sobre documentos de viaje robados o desaparecidos, de conformidad con las disposiciones pertinentes de la Decisión relativa a las descripciones sobre pasaportes robados, sustraídos, extraviados y anulados introducidas en el SIS.

CAPÍTULO XV

PROTECCIÓN DE DATOS

Artículo 64
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 siempre que las disposiciones nacionales de transposición de la Directiva (UE) 2016/680 no se apliquen.

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 65

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 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 o 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. Toda persona tendrá derecho a que se rectifiquen los datos erróneos o a que se borren los datos ilegalmente almacenados relativos a ella.

6. 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.

7. Se informará al interesado de las medidas adoptadas a raíz del ejercicio de su derecho de rectificación y supresión lo antes posible y, en cualquier caso, antes de que hayan transcurrido tres meses desde la fecha en que solicitó la rectificación o la supresión, o antes si la legislación nacional así lo dispone.

Artículo 66

Vías de recurso

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 70.

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 borrado de datos introducidos ilegalmente presentadas al responsable del tratamiento de los 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 borrado de datos introducidos ilegalmente presentadas a la autoridad nacional de supervisión;

   (e) el número de casos dirimidos en los órganos jurisdiccionales;

   (f) el número de casos en los que el órgano jurisdiccional se haya pronunciado en 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 69.

Artículo 67
Supervisión del N.SIS

1. Cada Estado miembro velará por que las autoridades nacionales de supervisión 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 velará 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 68
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 69
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 información pertinente, se asistirán mutuamente en la realización de auditorías e inspecciones, examinarán las dificultades de interpretación o aplicación del presente Reglamento y de otros actos jurídicos aplicables de la Unión, estudiarán los problemas puestos de manifiesto en el ejercicio de la supervisión independiente o en el ejercicio de los derechos de los interesados, elaborarán propuestas armonizadas de soluciones conjuntas a cualquier problema y promoverán la sensibilización respecto de los derechos 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 las 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 y en función de las necesidades.

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

CAPÍTULO XVI

RESPONSABILIDAD

Artículo 70
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 XVII

DISPOSICIONES FINALES

Artículo 71
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 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 por categoría de descripción y el número de ocasiones en que se haya realizado una búsqueda del SIS y el número de ocasiones en que se haya accedido al SIS para introducir, actualizar o suprimir una descripción, en total y para cada Estado miembro. Las estadísticas no contendrán datos personales. El informe estadístico anual se publicará. La Agencia facilitará asimismo estadísticas anuales sobre el uso de la funcionalidad consistente en que temporalmente no pueda consultarse una descripción emitida con arreglo al artículo 26 del presente Reglamento, en total y para cada Estado miembro, incluidas las posibles prórrogas del período de conservación de 48 horas.

4. Los Estados miembros, así como Europol, Eurojust 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 3, 7 y 8. Esta información incluirá estadísticas separadas sobre el número de búsquedas realizadas (o en nombre de) los servicios de los Estados miembros responsables de la expedición de certificados de matriculación de vehículos y los servicios de los Estados miembros competentes para la expedición de los certificados de matriculación o la gestión del tráfico de embarcaciones (incluidos los motores de embarcaciones), aeronaves y contenedores. Las estadísticas también indicarán el número de respuestas positivas por categoría de descripción.

5. La Agencia facilitará a los Estados miembros, la Comisión, Europol, Eurojust 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 periódicamente o extraordinarios, 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, Eurojust 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 adoptarse 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 72, 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 72
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 73
Modificaciones del Reglamento (UE) n.º 515/2014

El Reglamento (UE) n.º 515/2014[76] 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 mejora 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 en el ámbito de las inspecciones fronterizas y en el Reglamento (DO ...)*».

Artículo 74
Derogación

A partir de la fecha de aplicación del presente Reglamento, quedarán derogados los actos siguientes:

Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al acceso al Sistema de Información de Schengen de segunda generación (SIS II) por los servicios de los Estados miembros competentes para la expedición de los certificados de matriculación de vehículos;

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);

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[77].

[76] 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.

[77] 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.

Artículo 75
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*

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 la cooperación policial y judicial en materia penal, por la que se modifica el Reglamento (UE) n.º 515/2014 y se deroga el Reglamento (CE) n.º 1986/2006, la Decisión 2007/533/JAI del Consejo y la Decisión 2010/261/UE de la Comisión.

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA[78]

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[79]**

☑ 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 - «Entorpecer las actividades de la delincuencia organizada»

Objetivo A - «Una fuerte respuesta de la UE para combatir el terrorismo y prevenir la radicalización»

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. Por ejemplo, en la «Agenda Europea de Seguridad»[80], la Comisión anunció su intención de evaluar el SIS en 2015-2016 y evaluar si existen nuevas necesidades operativas que requieran cambios legislativos. Por otra parte, la Agenda de Seguridad subrayó que el SIS constituye el núcleo del intercambio de información policial y deberían reforzarse. Más recientemente, en su Comunicación «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad»[81], la Comisión manifestó que las funcionalidades adicionales del sistema serán consideradas sobre la base del informe de evaluación general con vistas a presentar las propuestas de revisión de la base jurídica del SIS. Finalmente, el 20 de abril de 2016, en su Comunicación «Aplicación de la Agenda Europea de Seguridad para luchar contra el terrorismo y allanar el camino hacia una Unión de la

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

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

80 COM(2015) 185 final.

81 COM(2016) 205 final.

Seguridad real y efectiva»[82], la Comisión propuso una serie de cambios al SIS con el fin de mejorar su valor añadido a efectos de las actividades policiales.

La evaluación general realizada por la Comisión confirmó que el SIS constituye un éxito operativo. Sin embargo, pese a sus múltiples éxitos, la evaluación también hizo una serie de recomendaciones con el objetivo de mejorar la eficacia y la eficiencia técnica y operativa del sistema.

Sobre la base de las recomendaciones del informe de evaluación general y plenamente en consonancia con los objetivos de la Comisión establecidos en la mencionada Comunicación y en el Plan estratégico 2016-2020 de la DG Migración y Asuntos de Interior[83], la propuesta aspira a aplicar:

- la iniciativa anunciada por la Comisión para mejorar el valor añadido del SIS con fines policiales a fin de responder a las nuevas amenazas;
- las recomendaciones de cambios técnicos y de procedimiento resultantes de una evaluación general del SIS;
- las peticiones de mejoras técnicas por parte de los usuarios finales;
- los resultados provisionales del Grupo de Expertos de Alto Nivel sobre Sistemas de Información y la Interoperabilidad y en lo que se refiere a la calidad de los datos.

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 2.1 - Una fuerte respuesta de la UE para combatir el terrorismo y prevenir la radicalización.

Objetivo específico 2.2 - Entorpecer las actividades de la delincuencia transfronteriza grave y organizada.

Actividad(es) GPA/PPA afectada(s)

Capítulo 18 02 - Seguridad interior

[82] COM(2016) 230 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.

El objetivo principal de la propuesta de modificaciones técnicas y jurídicas en el SIS es hacer el sistema más eficaz desde el punto de vista operativo. La evaluación general del SIS, realizada por la DG HOME en 2015-2016, recomendó mejoras técnicas del sistema y la armonización de los procedimientos nacionales en el ámbito de la cooperación policial.

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 los agentes de policía 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 períodos de no funcionamiento pueden tener una incidencia significativa en el trabajo de las policías. Por otra parte, la presente propuesta introduce cambios técnicos que harán que el sistema sea más eficiente y sencillo.

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.

La propuesta introduce nuevos identificadores biométricos: impresiones palmares, imágenes faciales y perfiles de ADN en casos determinados y limitados. Esto, unido a las modificaciones previstas de los artículos 32 y 33 (descripciones de personas desaparecidas) para permitir la introducción de descripciones con una finalidad preventiva y la clasificación de los casos de personas desaparecidas, permitirá, en primer lugar, reforzar considerablemente la protección de los menores no acompañados y, por otro, hacer posible su identificación sobre la base de su perfil de ADN o del de sus padres o hermanos (con autorización).

Las autoridades de los Estados miembros también podrán emitir descripciones relativas a personas desconocidas buscadas en relación con un delito, únicamente sobre la base de impresiones dactilares o palmares latentes o procedentes del lugar del delito. Esto no es posible en el actual marco jurídico y técnico y, por tanto, representa un importante avance.

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 de la 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 sistema mediante la introducción de nuevos elementos en las categorías existentes de descripciones y 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. Además, la Agencia también ofrecerá estadísticas anuales sobre la utilización consistente en que temporalmente no pueda consultarse una descripción emitida con arreglo al artículo 26 del presente Reglamento, en total y para cada Estado miembro, incluidas las posibles prórrogas del período de conservación de 48 horas.

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.

Objetivo específico 1 - Entorpecer las actividades de la delincuencia organizada.

Indicador - Utilización de los mecanismos de intercambio de información de la UE. Esto puede medirse a través de un aumento del número de respuestas positivas en el SIS. Los indicadores son los informes estadísticos, publicados por eu-LISA y los Estados miembros, que permitirán a la Comisión evaluar el uso de las nuevas funcionalidades del sistema.

Objetivo específico 2 - Una fuerte respuesta de la UE para combatir el terrorismo y prevenir la radicalización.

Indicador - Incremento del número de descripciones y respuestas positivas, particularmente por lo que respecta al artículo 36, apartado 3, de la propuesta sobre descripciones relativas a personas y objetos a efectos de controles discretos, específicos o de investigación.

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. Armonizar mejor los procedimientos nacionales para la utilización del SIS.

3. Ampliar la lista de los usuarios institucionales con acceso a los datos del SIS ofreciendo pleno acceso al sistema de Europol y a la nueva Guardia Europea de Fronteras y Costas.

4. Aportar nuevos elementos a las descripciones del SIS y nuevas funcionalidades con el fin de ampliar el ámbito de aplicación del sistema, permitirle abordar el actual entorno de seguridad, y mejorar la cooperación entre las autoridades policiales y de seguridad y reducir la carga administrativa.

5. Abordar la utilización del SIS en todas sus fases de funcionamiento, de forma que no solo abarque los sistemas central y nacionales, sino también garantizar que los usuarios finales reciban toda la información necesaria para el desempeño de sus funciones.

6. Reforzar la continuidad de las actividades y garantizar el funcionamiento ininterrumpido del SIS a nivel central y nacional.

7. Reforzar la lucha contra la delincuencia internacional, el terrorismo y la ciberdelincuencia como ámbitos interrelacionados con una marcada dimensión transfronteriza.

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. Los objetivos de la 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 competentes de los Estados miembros accedieron al sistema casi 2 900 millones de veces, lo que constituye una clara demostración de la contribución fundamental del sistema a la cooperación policial en el espacio Schengen. Este alto nivel de intercambio de información entre los Estados miembros no podría haberse alcanzado a través de soluciones nacionales descentralizadas, y habría sido imposible alcanzar estos resultados a nivel de los Estados miembros.

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, confidencial y eficaz. Las nuevas propuestas facilitarán en mayor medida el intercambio de información y la cooperación entre los Estados miembros de la UE. Por otra parte, en el marco de sus competencias, se concederá a Europol y a la nueva Agencia de 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

1. La fase de desarrollo deberá comenzar únicamente cuando los requisitos del sistema y de los usuarios finales 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. 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 dos estudios, cuyos resultados se han integrado en el desarrollo de la presente propuesta:

- Evaluación técnica del SIS, que 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 del impacto de las tecnologías de la información y la comunicación en las posibles mejoras en la arquitectura del SIS II, que evaluó los costes corrientes de 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.

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.

[84] COM(2016) 205 final.

Por otra parte, la propuesta es coherente y complementa diversas políticas de la Unión estrechamente vinculadas, en particular:

a) la seguridad interior, como se destaca en la Agenda Europea de Seguridad[85], con el fin de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves, permitiendo a los cuerpos de seguridad tratar los datos personales de los sospechosos de estar implicados en actos de terrorismo o delitos graves;

b) la protección de datos en la medida en que la presente propuesta debe garantizar la protección de los derechos fundamentales en aras del 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) la Guardia Europea de Fronteras y Costas[86] por lo que se refiere, en primer lugar, a la posibilidad de que el personal de la Agencia efectúe análisis de riesgos y, en segundo lugar, su acceso al SIS para los fines del SEIAV propuesto. La propuesta también tiene por objeto garantizar la interfaz técnica de acceso al SIS a los equipos de la Guardia Europea de Fronteras y Costas, los equipos de personal implicados en tareas relacionadas con el retorno y los miembros del equipo de apoyo a la gestión de la migración, con arreglo a su mandato, que tienen derecho de acceso y búsqueda de datos introducidos en el SIS;

b) Europol, en la medida en que esta propuesta le atribuye derechos adicionales de acceso y búsqueda de los datos introducidos en el SIS con arreglo a su mandato;

c) Prüm[87], en la medida en que la evolución de esta propuesta para permitir la identificación de personas a partir de sus impresiones dactilares (así como imágenes faciales y perfiles de ADN) complementa las actuales disposiciones sobre acceso mutuo transfronterizo en línea a las bases de datos nacionales de ADN y los sistemas automatizados de identificación de impresiones dactilares.

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

a) la gestión de las fronteras exteriores. La propuesta complementa el nuevo principio previsto en el Código de fronteras Schengen de realización de controles sistemáticos mediante la consulta de bases de datos de todos los viajeros, incluidos los ciudadanos de la UE, tanto a la entrada como a la salida de la zona Schengen, establecidos como respuesta al fenómeno de los combatientes terroristas extranjeros;

85 COM(2015) 185 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.

87 Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO L 210 de 6.8.2008, p. 1, y Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO L 210 de 6.8.2008, p. 12.

b) Sistema de Entradas y Salidas (SES)[88] en la medida en que la presente propuesta pretende reflejar el uso propuesto de una combinación de imágenes faciales y las huellas dactilares como identificadores biométricos para el funcionamiento del SES;

c) el SEIAV en la medida en que la presente propuesta tiene en cuenta la propuesta de 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 Unión Europea.

[88] 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, 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**

- Período preparatorio: 2017

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

– seguida del pleno funcionamiento.

1.7. Modos de gestión previstos[89]

☑**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 el ámbito de las inspecciones fronterizas) no

89 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

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 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 71, 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.

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. Sistema de gestión y de 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, eu-LISA 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 eu-LISA.

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[90].	de países AELC[91]	de países candidatos [92]	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

[90] CD = créditos disociados / CND = créditos no disociados.
[91] AELC: Asociación Europea de Libre Comercio.
[92] 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**

	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 DG <…….>	Créditos								

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

3.2.3. Incidencia estimada en los créditos de carácter administrativo

En millones EUR (al tercer decimal)

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**[93]	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								

93 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 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[94]	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[95] 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

94 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.).

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

3.2.3.2. Incidencia estimada sobre los créditos 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:

Créditos de compromiso en millones EUR (al tercer decimal)

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[96]	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[97] Desarrollo del sistema nacional																		
- 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.° 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

96 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.).

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

Equipos			1	0	1	0,738	1	0,738										1,476
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

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)[98]								
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** [99]	- 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 (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 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:

98 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.

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

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 relativos a la mejora de las funcionalidades del SIS II, 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[100]						
		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.

[100] 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.