UNIÓN EUROPEA

EL PARLAMENTO EUROPEO **EL CONSEJO**

Bruselas, 8 de octubre de 2018
(OR. en)

2016/0409 (COD) **PE-CONS 36/18**

SIRIS 71
ENFOPOL 337
COPEN 222
SCHENGEN 30
COMIX 335
CODEC 1126

ACTOS LEGISLATIVOS Y OTROS INSTRUMENTOS

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

REGLAMENTO (UE) 2018/…
DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de …

relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y 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[1],

[1] Posición del Parlamento Europeo de 24 de octubre de 2018 [(DO …) (pendiente de publicación en el Diario Oficial)] y Decisión del Consejo de ….

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 contribuyen al mantenimiento de un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, al apoyar la cooperación operativa entre las autoridades nacionales competentes, en particular guardias de fronteras, servicios policiales, autoridades aduaneras, autoridades de inmigración y autoridades responsables de la prevención, la detección, la investigación o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

(2) Inicialmente, el SIS fue creado de conformidad con las disposiciones del título IV del Convenio 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[1] (en lo sucesivo, «Convenio de aplicación del Acuerdo de Schengen»), firmado el 19 de junio de 1990. El SIS de segunda generación (SIS II), cuyo desarrollo se había encomendado a la Comisión con arreglo al Reglamento (CE) n.º 2424/2001 del Consejo[2] y a la Decisión 2001/886/JAI del Consejo[3]. Posteriormente, fue establecido mediante el Reglamento (CE) n.º 1987/2006 del Parlamento Europeo y del Consejo[4], y la Decisión 2007/533/JAI del Consejo[5]. El SIS II sustituyó al SIS, tal como se había creado en virtud del Convenio de aplicación del Acuerdo de Schengen.

---

1 DO L 239 de 22.9.2000, p. 19.

2 Reglamento (CE) n.º 2424/2001 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. 4).

3 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).

4 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).

5 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).

(3) Tres años después de la entrada en funcionamiento del SIS II, la Comisión evaluó el sistema con arreglo a lo dispuesto en el Reglamento (CE) n.º 1987/2006 y en la Decisión 2007/533/JAI. El 21 de diciembre de 2016, la Comisión presentó al Parlamento Europeo y al Consejo el informe sobre la evaluación del Sistema de Información 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, al que acompañaba un documento de trabajo de los servicios de la Comisión. Las recomendaciones que figuran en dichos documentos deben reflejarse, en su caso, en el presente Reglamento.

(4) El presente Reglamento constituye la base jurídica para el SIS en las materias que entran en el ámbito de aplicación de la tercera parte, título V, capítulos 4 y 5, del Tratado de Funcionamiento de la Unión Europea (TFUE). El Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo[1+] constituye la base jurídica para el SIS en las materias que entran en el ámbito de aplicación de la tercera parte, título V, capítulo 2, del TFUE.

---

[1] Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo, de …, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 1987/2006 (DO L …).

[+] DO: insértese en el texto el número de serie y complétese en la nota a pie de página la referencia de publicación del Reglamento que figura en el documento PE-CONS 35/18.

(5) El hecho de que la base jurídica para el 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. Debe contar con una red única de oficinas nacionales, denominadas oficinas Sirene, para garantizar el intercambio de información complementaria. En consecuencia, algunas disposiciones de dichos instrumentos deben ser idénticas.

(6) Es necesario especificar los objetivos del SIS, determinados elementos de su arquitectura técnica y su financiación, establecer normas relativas a su funcionamiento y utilización de extremo a extremo y determinar las responsabilidades. También es necesario determinar las categorías de datos que se vayan a introducir en el sistema, los fines para los que se vayan a introducir y tratar, y los criterios de introducción. Asimismo, es preciso regular la supresión de descripciones, las autoridades autorizadas para acceder a los datos y el uso de datos biométricos, y desarrollar otras normas sobre protección y tratamiento de datos.

(7) Las descripciones del SIS solo contienen la información necesaria para identificar a una persona u objeto y para precisar las medidas que deben tomarse. Por tanto, los Estados miembros deben intercambiar, cuando sea necesario, información complementaria relacionada con las descripciones.

(8) El SIS incluye un sistema central (SIS Central) y unos sistemas nacionales. Los sistemas nacionales pueden contener una copia completa o parcial de la base de datos del SIS, que puede ser compartida entre dos o más Estados miembros. Considerando que el SIS es el instrumento de intercambio de información más importante de Europa para garantizar la seguridad y una gestión eficaz de las fronteras, es necesario asegurar su funcionamiento ininterrumpido tanto a escala central como nacional. La disponibilidad del SIS debe ser objeto de una estrecha supervisión tanto a escala central como en los Estados miembros, y todo incidente de indisponibilidad para los usuarios finales debe ser registrado y comunicado a las partes interesadas nacionales y de la Unión. Cada Estado miembro debe crear una copia de seguridad para su sistema nacional. Además, los Estados miembros deben garantizar la conectividad ininterrumpida con el SIS Central mediante puntos de conexión duplicados y separados física y geográficamente. El SIS Central y la infraestructura de comunicación deben organizarse de tal manera que se garantice su funcionamiento las 24 horas del día y los 7 días de la semana. Por este motivo, la Agencia de la Unión Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (en lo sucesivo, «eu-Lisa»), establecida en virtud del Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo[1+], debe implantar soluciones técnicas que refuercen la disponibilidad ininterrumpida del SIS, a reserva de una evaluación de impacto y un análisis coste-beneficio independientes.

---

1 Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo, de …, relativo a la Agencia de la Unión Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (eu-LISA), y por el que se modifican el Reglamento (CE) n.º 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) n.º 1077/2011 (DO L …).

\+ DO: insértese en el texto el número de serie del Reglamento que figura en el documento PE-CONS 29/18 y complétese en la nota a pie de página la referencia de publicación.

(9) Es necesario disponer de un manual que establezca normas detalladas sobre el intercambio de información complementaria en relación con las medidas solicitadas en las descripciones (Manual Sirene). Las oficinas Sirene deben garantizar el intercambio de esa información de manera rápida y eficiente.

(10) Con el fin de garantizar la eficiencia del intercambio de información complementaria, en particular sobre las medidas que deban tomarse según lo especificado en las descripciones, procede reforzar el funcionamiento de las oficinas Sirene precisando las exigencias relativas a los recursos disponibles y la formación de los usuarios y el tiempo de respuesta a las consultas que reciban de otras oficinas Sirene.

(11) Los Estados miembros deben asegurarse de que el personal de sus oficinas Sirene tenga las capacidades lingüísticas y los conocimientos de las normas sustantivas y procesales aplicables necesarios para desempeñar sus funciones.

(12) Para poder aprovechar plenamente las funcionalidades del SIS, los Estados miembros deben garantizar que los usuarios finales y el personal de las oficinas Sirene reciban formación periódicamente, en particular sobre la seguridad de los datos, la protección de los datos y la calidad de los datos. Las oficinas Sirene deben participar en la elaboración de los programas de formación. En la medida de lo posible, las oficinas Sirene deben prever además la organización de intercambios de personal con otras oficinas Sirene, con una periodicidad anual como mínimo. Se anima a los Estados miembros a adoptar las medidas necesarias para evitar la pérdida de capacidades y experiencia a causa de la rotación del personal.

(13) Eu-LISA se ocupa de la gestión operativa de los componentes centrales del SIS. Con el fin de que eu-LISA pueda dedicar los recursos financieros y humanos necesarios al conjunto de los aspectos de la gestión operativa del SIS Central y de la infraestructura de comunicación, el presente Reglamento debe definir pormenorizadamente sus funciones, en particular por lo que se refiere a los aspectos técnicos del intercambio de información complementaria.

(14) Sin perjuicio de la responsabilidad de los Estados miembros en lo que respecta a la exactitud de los datos introducidos en el SIS y de la función de coordinación de la calidad que desempeñan las oficinas Sirene, eu-LISA debe encargarse de la mejora de la calidad de los datos mediante la creación a nivel central de una herramienta de supervisión de la calidad de los datos y debe presentar informes periódicos a la Comisión y a los Estados miembros. La Comisión debe informar al Parlamento Europeo y al Consejo acerca de los problemas detectados en relación con la calidad de los datos. Para seguir mejorando la calidad de los datos del SIS, eu-LISA también debe ofrecer formación sobre la utilización del SIS a los organismos nacionales de formación y, en la medida de lo posible, a las oficinas Sirene y a los usuarios finales.

(15) Con el fin de mejorar el seguimiento de la utilización del SIS y analizar las tendencias relativas a los delitos, eu-LISA debe estar facultada para desarrollar una capacidad de vanguardia que le permita elaborar, sin poner en peligro la integridad de los datos, informes estadísticos destinados a los Estados miembros, el Parlamento Europeo, el Consejo, la Comisión, Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas. Por tanto, debe crearse un repositorio central. Las estadísticas conservadas en el repositorio u obtenidas de este no deben contener datos personales. Los Estados Miembros deben comunicar estadísticas relativas al ejercicio del derecho de acceso, rectificación de datos inexactos y supresión de datos almacenados ilegalmente, en el marco de la cooperación entre las autoridades de control y el Supervisor Europeo de Protección de Datos con arreglo al presente Reglamento.

(16) Se deben introducir en el SIS nuevas 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 y detectar identidades múltiples, la descripción debe incluir, si se dispone de esta información, una referencia al documento de identificación personal de la persona en cuestión, o a su número, y una copia, a ser posible en color, de dicho documento.

(17) Cuando sea estrictamente necesario, las autoridades competentes deben poder introducir en el SIS información específica relativa a rasgos físicos particulares, objetivos e inalterables de una persona, como tatuajes, marcas o cicatrices.

(18) Cuando se disponga de ellos, todos los datos pertinentes, en particular el nombre de la persona en cuestión, deben introducirse cuando se cree una descripción, a fin de minimizar el riesgo de obtener falsos positivos, así como actividades operativas innecesarias.

(19) El SIS no debe almacenar ningún dato empleado para efectuar consultas, con excepción de los registros destinados a comprobar la legalidad de la consulta y del tratamiento de datos, realizar controles internos y garantizar el correcto funcionamiento de los sistemas nacionales, así como la integridad y seguridad de los datos.

(20) El SIS debe permitir tratar datos biométricos para ayudar a la identificación fiable de las personas en cuestión. La introducción en el SIS de fotografías, imágenes faciales o datos dactiloscópicos y la utilización de esos datos deben limitarse a lo necesario para lograr los objetivos perseguidos, debe estar autorizada por el Derecho de la Unión, respetar los derechos fundamentales, en particular el interés superior del menor, y debe ser conforme con el Derecho de la Unión en materia de protección de datos, en particular las disposiciones aplicables en materia de protección de datos previstas en el presente Reglamento. Desde la misma perspectiva y a fin de evitar los inconvenientes de una identificación incorrecta, el SIS también debe permitir el tratamiento de datos sobre personas cuya identidad haya sido usurpada, con las garantías adecuadas, con el consentimiento de la persona en cuestión para cada categoría de datos, y en especial para las impresiones palmares, y con una limitación estricta de los fines para los que dichos datos personales pueden ser tratados legalmente.

(21) Los Estados miembros deben adoptar las disposiciones técnicas necesarias para que, cada vez que los usuarios finales sean facultados para realizar una consulta en una base de datos nacional de uso policial o de inmigración, puedan consultar también el SIS en paralelo, a reserva de los principios establecidos en el artículo 4 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[1] y en el artículo 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[2]. De este modo se garantiza que el SIS funcione como la principal medida compensatoria en el espacio sin controles en las fronteras interiores y sirva para afrontar mejor la dimensión transfronteriza de la delincuencia y la movilidad de los delincuentes.

(22) El presente Reglamento debe establecer las condiciones para el uso de datos dactiloscópicos, fotografías e imágenes faciales a efectos de identificación y comprobación. Las imágenes faciales y las fotografías a efectos de identificación solo deben utilizarse en un principio en el contexto de los pasos fronterizos oficiales. Previamente a dicha utilización, se necesitará un informe de la Comisión que confirme que la tecnología necesaria está disponible, es fiable y está lista para su uso.

---

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

[2] 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).

(23) 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 a los sistemas automatizados de identificación de impresiones dactilares, tal como establecen las Decisiones 2008/615/JAI[1] y 2008/616/JAI[2] del Consejo. La consulta de datos dactiloscópicos en el SIS permite una búsqueda activa del autor de un delito. Por tanto, conviene prever la posibilidad de cargar los datos dactiloscópicos de un autor desconocido en el SIS, a condición de que la persona a quien correspondan esos datos dactiloscópicos pueda ser identificada con un muy alto grado de probabilidad como autor de un delito grave o un acto de terrorismo. Este es el caso, en particular, cuando se encuentran datos dactiloscópicos en un arma o en cualquier objeto utilizado para la comisión del delito. La mera presencia de los datos dactiloscópicos en el lugar del delito no debe considerarse como indicio de un muy alto grado de probabilidad de que dichos datos dactiloscópicos sean los del autor. Otro requisito previo para la creación de dicha descripción debe ser la imposibilidad de establecer la identidad del sospechoso a partir de datos procedentes de cualquier otra base de datos nacional, de la Unión o internacional pertinente. En caso de que una consulta de datos dactiloscópicos conduzca a una posible coincidencia, el Estado miembro debe proceder a verificaciones adicionales con la participación de expertos en la materia, a fin de determinar si el sospechoso es la persona a quien corresponden las impresiones dactilares almacenadas en el SIS, y debe establecer la identidad de la persona. El procedimiento debe estar sujeto al Derecho nacional. Tal identificación podría contribuir sustancialmente a la investigación y desembocar en una detención siempre que se cumplan todas las condiciones para proceder a la detención.

---

1 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).

2 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).

(24) Los conjuntos completos o incompletos de impresiones dactilares o palmares encontradas en el lugar de un delito deben poder cotejarse con los datos dactiloscópicos almacenados en el SIS, si puede acreditarse con un alto grado de probabilidad que pertenecen al autor de un delito grave o un delito de terrorismo, siempre que se haga también un cotejo de forma simultánea en las bases de datos nacionales pertinentes de impresiones dactilares. Se debe prestar particular atención al establecimiento de normas de calidad aplicables al almacenamiento de datos biométricos, en particular de datos dactiloscópicos latentes.

(25) Cuando la identidad de una persona no se pueda acreditar por ningún otro medio, se deben utilizar los datos dactiloscópicos para intentar identificarla. La identificación de una persona mediante datos dactiloscópicos debe estar autorizada en todos los casos.

(26) En casos claramente definidos en que no se disponga de datos dactiloscópicos, ha de ser posible añadir a la descripción un perfil de ADN. Únicamente los usuarios autorizados deben tener acceso a ese perfil de ADN. Los perfiles de ADN deberían facilitar la identificación de personas desaparecidas que necesitan protección y especialmente de menores desaparecidos, en particular si se permite el uso de los perfiles de ADN de sus ascendientes o descendientes directos o hermanos para permitir la identificación. Los datos de ADN han de contener únicamente la información mínima necesaria para la identificación de la persona desaparecida.

(27) En el SIS solo deben consultarse perfiles de ADN cuando la identificación sea necesaria y proporcionada a efectos de lo dispuesto en el presente Reglamento. No se deben consultar ni tratar perfiles de ADN para fines distintos de aquellos para los que fueron introducidos en el SIS. Deben aplicarse las normas sobre seguridad y protección de datos establecidas en el presente Reglamento. Se deben tomar, si fuera necesario, medidas adicionales cuando se utilicen perfiles de ADN con el fin de evitar todo riesgo de falsas coincidencias, piratería informática o intercambio no autorizado con terceros.

(28) El SIS debe contener descripciones sobre personas a las que se busca para detenerlas y entregarlas o extraditarlas. Además de las descripciones, procede facilitar el intercambio, a través de las oficinas Sirene, de la información complementaria que sea necesaria para los procedimientos de entrega y extradición. En particular, deben ser tratados en el SIS los datos a que se refiere el artículo 8 de la Decisión Marco 2002/584/JAI del Consejo[1]. Por razones operativas, resulta oportuno que el Estado miembro emisor, tras obtener autorización de la autoridad judicial, pueda suspender temporalmente la disponibilidad de una descripción existente a efectos de detención cuando la persona que sea objeto de una orden de detención europea esté siendo buscada activa e intensivamente y los usuarios finales que no participen en la operación de búsqueda puedan poner en peligro el resultado de esta. La indisponibilidad temporal de este tipo de descripciones no debe superar, en principio, las 48 horas.

(29) Debe ser posible añadir en el SIS una traducción de los datos adicionales introducidos a efectos de una entrega al amparo de la orden de detención europea o a efectos de una extradición.

---

[1] 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).

(30) El SIS debe contener descripciones sobre personas desaparecidas o sobre personas vulnerables a quienes se deba impedir viajar para garantizar su protección o prevenir amenazas contra la seguridad o el orden públicos. En el caso de los menores, estas descripciones y los procedimientos correspondientes deben servir al interés superior del menor, de conformidad con el artículo 24 de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 3 de la Convención de las Naciones Unidas sobre los Derechos del Niño, de 20 de noviembre de 1989. Las autoridades competentes, incluidas las autoridades judiciales, que vayan a tomar medidas o decisiones a raíz de una descripción sobre un menor deben hacerlo en cooperación con las autoridades de protección de menores. Cuando proceda, debe informarse a la línea directa nacional sobre menores desaparecidos.

(31) Las descripciones sobre personas desaparecidas que necesiten recibir protección deben ser introducidas a petición de la autoridad competente. Para cualquier menor que haya desaparecido de algún centro de acogida de los Estados miembros se debe introducir una descripción en el SIS como persona desaparecida.

(32) Las descripciones sobre menores en riesgo de sustracción parental deben introducirse en el SIS a petición de las autoridades competentes, especialmente de las autoridades judiciales que tengan competencia en asuntos de responsabilidad parental con arreglo al Derecho nacional. Solamente deben introducirse en el SIS descripciones sobre menores en riesgo de sustracción parental cuando dicho riesgo sea concreto y evidente y en limitadas situaciones. Por lo tanto, es necesario prever salvaguardias estrictas y adecuadas. Al evaluar si existe un riesgo concreto y evidente de traslado ilegal e inminente de un menor fuera de un Estado miembro, la autoridad competente debe tener en cuenta las circunstancias personales del menor y el entorno al que está expuesto.

(33) El presente Reglamento ha de establecer una nueva categoría de descripciones para determinadas categorías de personas vulnerables a quienes se debe impedir viajar. Debe considerarse vulnerables a las personas que, debido a su edad, discapacidad o circunstancias familiares, necesitan protección.

(34) Han de introducirse en el SIS descripciones sobre menores a quienes se deba impedir viajar por su propia protección cuando haya un riesgo concreto y evidente de que abandonen el territorio de un Estado miembro o sean trasladados fuera de él. Han de introducirse dichas descripciones cuando el viaje ponga a los menores en peligro de ser objeto de trata de seres humanos o matrimonio forzado, mutilación genital femenina u otras formas de violencia de género; de ser víctimas de delitos de terrorismo o de verse involucrados en ellos, o de ser reclutados o alistados en grupos armados u obligados a participar activamente en hostilidades.

(35) Han de introducirse descripciones sobre adultos vulnerables a quienes se deba impedir viajar por su propia protección cuando el viaje los ponga en peligro de ser objeto de trata de seres humanos o violencia de género.

(36) Con el fin de garantizar unas salvaguardias estrictas y adecuadas y cuando así lo requiera el Derecho nacional, las descripciones sobre menores u otras personas vulnerables a quienes se deba impedir viajar han de introducirse en el SIS tras la decisión de una autoridad judicial o la decisión de una autoridad competente confirmada por una autoridad judicial.

(37) Debe añadirse una nueva medida para permitir dar el alto e interrogar a una persona para que el Estado miembro emisor pueda obtener información. Dicha medida debe aplicarse en los casos en los que, a partir de un indicio claro, se sospeche que una persona ha cometido o tiene previsto cometer cualquiera de los delitos a que se refiere el artículo 2, apartados 1 y 2, de la Decisión Marco 2002/584/JAI, cuando se necesite más información para la ejecución de una pena de privación de libertad o una orden de detención contra una persona declarada culpable de cualesquiera de los delitos a que se refiere el artículo 2, apartados 1 y 2, de la Decisión Marco 2002/584/JAI, o cuando haya motivos para creer que dicha persona cometerá alguno de tales delitos. Esta medida debe entenderse también sin perjuicio de los mecanismos existentes de asistencia judicial. Gracias a ella ha de obtenerse información suficiente para decidir la adopción de ulteriores medidas. Esta nueva medida no debe equivaler al registro o la detención de la persona. Se deben salvaguardar los derechos procesales de los sospechosos y acusados con arreglo al Derecho nacional y de la Unión, en particular, el derecho a la asistencia de letrado de conformidad con la Directiva 2013/48/UE del Parlamento Europeo y el Consejo[1].

(38) En el caso de descripciones sobre objetos para su incautación o utilización como pruebas en un proceso penal, la incautación de los objetos en cuestión debe llevarse a cabo de conformidad con la normativa nacional que determine en qué casos y en qué condiciones se puede proceder a la incautación de un objeto, en particular si este está en manos de su legítimo propietario.

[1] Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad (DO L 294 de 6.11.2013, p. 1).

(39) El SIS debe incluir nuevas categorías de objetos de gran valor, como artículos de tecnología de la información, que puedan ser identificados y registrados con un único número identificativo.

(40) En cuanto a las descripciones introducidas en el SIS sobre documentos a efectos de incautación o utilización como prueba en procesos penales, se entenderá que el término «falso» se refiere tanto a los documentos falsificados como a los falsos.

(41) Los Estados miembros deben 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. Por lo que respecta a las descripciones introducidas a efectos de la detención y entrega de una persona, lo dispuesto en el presente Reglamento no puede interpretarse como una excepción a la Decisión Marco 2002/584/JAI ni en el sentido de que impida la aplicación de lo dispuesto en ella. La decisión de añadir una indicación a una descripción para la no ejecución de una orden de detención europea debe basarse únicamente en los motivos de denegación previstos en la citada Decisión Marco.

(42) Cuando se haya añadido una indicación a una descripción y se descubra el paradero de la persona en búsqueda a efectos de detención y entrega, siempre se debe comunicar ese paradero a la autoridad judicial emisora, que podrá decidir transmitir una orden de detención europea a la autoridad judicial competente de conformidad con lo dispuesto en la Decisión Marco 2002/584/JAI.

(43) Debe existir la posibilidad de que los Estados miembros establezcan conexiones entre las descripciones en el SIS. La creación de conexiones entre dos o más descripciones no debe afectar a las medidas que deban tomarse, al plazo de revisión de las descripciones ni a los derechos de acceso a las descripciones.

(44) Las descripciones no deben conservarse en el SIS por más tiempo del necesario para cumplir el fin específico para el que fueron introducidas. Los plazos de revisión de las distintas categorías de descripción deben ser adecuados a la luz de la finalidad de esta. Las descripciones sobre objetos que estén vinculadas a una descripción sobre una persona solo deben conservarse mientras se conserve la descripción sobre la persona. Las decisiones de conservar descripciones sobre personas deben basarse en una evaluación global de cada caso concreto. Los Estados miembros deben volver a examinar las descripciones sobre personas y objetos en los plazos de revisión establecidos y deben elaborar estadísticas del número de descripciones cuyo período de conservación se haya prorrogado.

(45) La introducción de una descripción en el SIS y la prórroga de su fecha de expiración deben estar sujetas al requisito de proporcionalidad, lo que significa que se debe determinar en cada situación concreta si se trata de un caso adecuado, pertinente y suficientemente importante como para justificar la introducción de una descripción en el SIS. Cuando se trate de delitos de terrorismo, el caso debe ser considerado adecuado, pertinente y suficientemente importante como para justificar una descripción en el SIS. Los Estados miembros deben poder abstenerse excepcionalmente, por motivos de seguridad pública o nacional, de introducir una descripción en el SIS cuando sea probable que obstaculice indagaciones, investigaciones o procedimientos administrativos o judiciales.

(46) Es necesario establecer normas sobre la supresión de las descripciones. Una descripción debe 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 determinación del momento en que una descripción ha cumplido su objetivo, procede establecer criterios detallados a fin de determinar, para cada categoría de descripción, el momento en que ha de ser suprimida.

(47) La integridad de los datos del SIS reviste una importancia primordial. Por tanto, deben fijarse salvaguardias adecuadas para tratar los datos del SIS a escala central y a escala nacional, a fin de garantizar la seguridad de los datos de extremo a extremo. Las autoridades que intervienen en el tratamiento de los datos deben estar sujetas a los requisitos de seguridad del presente Reglamento y se les debe aplicar un procedimiento uniforme de notificación de incidentes. Su personal debe estar debidamente formado y estar al tanto de las infracciones y sanciones a este respecto.

(48) Los datos tratados en el SIS y la información complementaria conexa intercambiada con arreglo al presente Reglamento no se deben transmitir ni poner a disposición de terceros países ni de organizaciones internacionales.

(49) Es conveniente conceder acceso al SIS a los servicios responsables de la matriculación de vehículos, embarcaciones y aeronaves con el fin de permitirles comprobar si el medio de transporte en cuestión es objeto de búsqueda en los Estados miembros para su incautación. También es conveniente conceder acceso al SIS a los servicios responsables de registrar armas de fuego, con el fin de permitirles comprobar si el arma en cuestión ya es objeto de búsqueda en los Estados miembros para su incautación o si existe una descripción sobre la persona que solicita el registro.

(50) Debe facilitarse el acceso directo al SIS únicamente a los servicios públicos competentes. Dicho acceso debe limitarse a las descripciones relativas a los respectivos medios de transporte y sus documentos de registro o números de matrícula, o a las armas de fuego y las personas que solicitan su registro. Los servicios mencionados deben informar de cualquier respuesta positiva en el SIS a las autoridades policiales, las cuales deben tomar las medidas oportunas en relación con esa descripción concreta del SIS y notificar la respuesta positiva al Estado miembro emisor a través de las oficinas Sirene.

(51) Sin perjuicio de normas más específicas recogidas en el presente Reglamento, las disposiciones legales, reglamentarias y administrativas nacionales adoptadas en virtud de la Directiva (UE) 2016/680 deben aplicarse al tratamiento de datos personales, incluidas su recogida y comunicación, con arreglo al presente Reglamento por parte de las autoridades nacionales competentes a efectos de prevención, detección, investigación o enjuiciamiento de delitos de terrorismo u otros delitos graves o de la ejecución de sanciones penales. En el caso de las autoridades nacionales competentes responsables de la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo u otros delitos graves o de la ejecución de sanciones penales, el acceso a los datos introducidos en el SIS y el derecho a consultarlos deben estar sujetos a todas las disposiciones pertinentes del presente Reglamento y de la Directiva (UE) 2016/680, tal como se hayan incorporado al Derecho nacional, en particular por lo que respecta a la supervisión por las autoridades de control mencionadas en la Directiva (UE) 2016/680.

(52) Sin perjuicio de normas más específicas recogidas en el presente Reglamento para el tratamiento de datos personales, el Reglamento (UE) 2016/679 debe aplicarse al tratamiento de datos personales efectuado por los Estados miembros con arreglo al presente Reglamento, a menos que dicho tratamiento sea llevado a cabo por las autoridades nacionales competentes a efectos de prevención, investigación, detección o enjuiciamiento de delitos de terrorismo u otros delitos graves.

(53) El Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo[1+] debe aplicarse al tratamiento de datos personales por las instituciones y los órganos de la Unión en el ejercicio de sus competencias con arreglo al presente Reglamento.

(54) El Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo[2] debe aplicarse al tratamiento de datos personales por Europol con arreglo al presente Reglamento.

(55) En caso de que una consulta realizada en el SIS por miembros nacionales de Eurojust o sus asistentes revele la existencia de una descripción introducida por un Estado miembro, Eurojust no puede adoptar la medida que se pide. Por consiguiente, debe informar de ello al Estado miembro afectado para que este pueda hacer un seguimiento del asunto.

---

1 Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo, de …, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L …).

\+ DO: insértese en el texto el número de serie del Reglamento que figura en el documento PE-CONS 31/18 y complétese en la nota a pie de página la referencia de publicación.

2 Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).

(56) A la hora de utilizar el SIS, las autoridades competentes deben velar por que se respeten la dignidad e integridad de la persona cuyos datos están siendo tratados. El tratamiento de datos personales a los efectos del presente Reglamento no debe dar lugar a discriminación contra las personas por motivos tales como el sexo, el origen racial o étnico, la religión o las creencias, la discapacidad, la edad o la orientación sexual.

(57) En lo que respecta a la confidencialidad, las disposiciones pertinentes del Estatuto de los funcionarios de la Unión Europea y el Régimen aplicable a los otros agentes de la Unión, establecido en el Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo[1] (en lo sucesivo, «Estatuto de los funcionarios») deben aplicarse a los funcionarios y otros agentes que trabajen en ámbitos relacionados con el SIS.

(58) Tanto los Estados miembros como eu-LISA deben disponer de planes de seguridad para facilitar la aplicación de las obligaciones en materia de seguridad y deben cooperar entre sí para abordar las cuestiones de seguridad desde una perspectiva común.

[1] DO L 56 de 4.3.1968, p. 1.

(59) Las autoridades nacionales de control independientes a las que se refieren el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 (en lo sucesivo, «autoridades de control») deben supervisar la legalidad del tratamiento de datos personales por los Estados miembros en el marco del presente Reglamento, incluido el intercambio de información complementaria. A tal efecto, se debe dotar de recursos suficientes a las autoridades de control. Deben regularse los derechos de los interesados con respecto al acceso, la rectificación y la supresión de sus datos personales almacenados en el SIS y cualquier recurso ulterior ante los órganos jurisdiccionales nacionales, así como el reconocimiento mutuo de las resoluciones judiciales. También resulta adecuado solicitar estadísticas anuales a los Estados miembros.

(60) Las autoridades de control deben velar por que, al menos cada cuatro años, se lleve a cabo una auditoría de las operaciones de tratamiento de datos en los sistemas nacionales de sus respectivos Estados miembros de acuerdo con las normas internacionales de auditoría. La auditoría debe ser realizada por las autoridades de control o bien encargada directamente por estas a un auditor independiente especializado en protección de datos. El auditor independiente debe quedar bajo la supervisión y la responsabilidad de las autoridades de control correspondientes que, por lo tanto, deben dirigir ellas mismas instrucciones al auditor, definir con claridad su objetivo, alcance y metodología, y ejercer una función de orientación y control respecto a la auditoría y sus resultados finales.

(61) El Supervisor Europeo de Protección de Datos debe supervisar las actividades de las instituciones y órganos de la Unión en lo que se refiere al tratamiento de datos personales al amparo del presente Reglamento. El Supervisor Europeo de Protección de Datos y las autoridades de control deben cooperar en la supervisión del SIS.

(62) Se deben asignar al Supervisor Europeo de Protección de Datos recursos suficientes para el desempeño de las funciones que le encomienda el presente Reglamento, incluido el asesoramiento de personas con conocimientos técnicos sobre datos biométricos.

(63) El Reglamento (UE) 2016/794 dispone que Europol apoye y refuerce las acciones llevadas a cabo por las autoridades nacionales competentes y su cooperación en la lucha contra el terrorismo y los delitos graves, y elabore análisis y evaluaciones de amenazas. La ampliación de los derechos de acceso de Europol a las descripciones sobre personas desaparecidas debería seguir mejorando la capacidad de Europol para facilitar a las autoridades policiales nacionales una amplila asistencia operativa y productos analíticos relativos a la trata de seres humanos y la explotación sexual de menores, incluidos los delitos en Internet. Con ello se contribuiría a mejorar la prevención de estos delitos, la protección de las víctimas potenciales y la investigación de la autoría. El Centro Europeo de Lucha contra la Ciberdelincuencia de Europol también se beneficiaría del nuevo acceso de Europol a las descripciones sobre personas desaparecidas, en particular en casos de turismo sexual y de abuso sexual de menores en Internet, ya que en este contexto los autores de esos delitos sostienen a menudo que tienen, o pueden tener, acceso a menores que pueden haber sido registrados como desaparecidos.

(64) Con el fin de colmar las lagunas existentes en lo que respecta al intercambio de información relacionada con el terrorismo, en particular sobre los combatientes terroristas extranjeros (por la crucial importancia que reviste el seguimiento de sus movimientos), se anima a los Estados miembros a intercambiar con Europol información sobre las actividades relacionadas con el terrorismo. Dicho intercambio de información debe llevarse a cabo mediante el intercambio de información complementaria con Europol sobre las descripciones correspondientes. Con este fin, Europol debe establecer una conexión con la infraestructura de comunicación.

(65) Además, es necesario establecer normas claras aplicables a Europol en lo que se refiere al tratamiento y la descarga de datos del SIS a fin de permitirle el más amplio uso del SIS, siempre que se cumplan las normas de protección de datos con arreglo a lo dispuesto en el presente Reglamento y en el Reglamento (UE) 2016/794. En caso de que las consultas realizadas por Europol en el SIS revelen la existencia de una descripción introducida por un Estado miembro, Europol no puede tomar las medidas que se piden. Por consiguiente, debe informar al Estado miembro afectado mediante el intercambio de información complementaria con la oficina Sirene correspondiente, a fin de que dicho Estado miembro pueda realizar el seguimiento del asunto.

(66) El Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo[1] establece, a los efectos de su objeto, que el Estado miembro de acogida debe autorizar a los miembros de los equipos mencionados en el artículo 2, punto 8, de dicho Reglamento desplegados por la Agencia Europea de la Guardia de Fronteras y Costas a consultar las bases de datos de la Unión, cuando dicha consulta sea necesaria para cumplir objetivos operativos sobre controles en las fronteras, vigilancia fronteriza y retorno especificados en el plan operativo. Otras agencias competentes de la Unión, especialmente la Oficina Europea de Apoyo al Asilo y Europol, pueden también desplegar expertos no pertenecientes al personal de dichas agencias de la Unión en el marco de los equipos de apoyo a la gestión de la migración.El objetivo del despliegue de los equipos a que se refiere el artículo 2, puntos 8 y 9, de dicho Reglamento es proporcionar un refuerzo operativo y técnico a los Estados miembros solicitantes, especialmente a aquellos que se enfrentan a desafíos de migración desproporcionados. Para el cumplimiento de las tareas asignadas, los equipos a que se refiere el artículo 2, puntos 8 y 9, de dicho Reglamento necesitan acceso al SIS a través de una interfaz técnica de la Agencia Europea de la Guardia de Fronteras y Costas conectada al SIS Central. En caso de que las consultas efectuadas en el SIS por los equipos a que se refiere el artículo 2, puntos 8 y 9, del Reglamento (UE) 2016/1624 o los equipos de personal revelen la existencia de una descripción introducida por un Estado miembro, el miembro del personal o el equipo no puede tomar las medidas que se piden, a menos que esté autorizado para ello por el Estado miembro de acogida. Por consiguiente, se debe informar al Estado miembro de acogida para posibilitarle el seguimiento del asunto. El Estado miembro de acogida debe notificar la respuesta positiva al Estado miembro emisor mediante el intercambio de información complementaria.

[1] 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).

(67) Debido a su naturaleza técnica, nivel de detalle y carácter variable frecuente, determinados aspectos del SIS no pueden ser regulados exhaustivamente por el presente Reglamento. Entre esos aspectos figuran, por ejemplo, las normas técnicas sobre introducción, actualización, supresión y consulta de datos y sobre la calidad de los datos y las normas relativas a los datos biométricos, las normas sobre compatibilidad y orden de prioridad de las descripciones, sobre conexiones entre descripciones, sobre el establecimiento de la fecha de expiración de las descripciones dentro del plazo máximo y sobre el intercambio de información complementaria. En consecuencia, deben conferirse a la Comisión competencias de ejecución en estas materias. Las normas técnicas sobre la consulta de descripciones deben tener en cuenta la necesidad de que las aplicaciones nacionales funcionen con fluidez.

(68) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[1]. El procedimiento para la adopción de actos de ejecución en virtud del presente Reglamento y del Reglamento (UE) 2018/…[+] debe ser el mismo.

(69) A fin de garantizar la transparencia, eu-LISA debe elaborar, dos años después de la entrada en funcionamiento del SIS con arreglo al presente Reglamento, un informe sobre el funcionamiento técnico del SIS Central y de la infraestructura de comunicación, incluida su seguridad, y sobre el intercambio bilateral y multilateral de información complementaria. La Comisión debe emitir una evaluación general cada cuatro años.

---

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

[+] DO: insértese el número de serie del Reglamento que figura en el documento PE-CONS 35/18.

(70) A fin de garantizar el correcto funcionamiento del SIS, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE por lo que respecta a nuevas subcategorías de objetos cuya búsqueda pueda solicitarse en las descripciones sobre objetos para su incautación o utilización como pruebas en un proceso penal, y a la determinación de las circunstancias en las que se debe permitir la utilización de fotografías e imágenes faciales a efectos de la identificación de personas en un contexto distinto al de los pasos fronterizos oficiales. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación[1]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(71) 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 ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a su naturaleza, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

[1] DO L 123 de 12.5.2016, p. 1.

(72) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea. Concretamente, el presente Reglamento respeta plenamente la protección de los datos personales de conformidad con el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, con el objetivo simultáneo de garantizar un entorno seguro para todas las personas que residen en el territorio de la Unión y una protección especial para los menores que pueden ser víctimas de trata o sustracción. En los casos relacionados con menores, la principal consideración debe ser el interés superior del menor.

(73) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no participa en la adopción del presente Reglamento y no queda vinculada por este ni sujeta a su aplicación. Dado que el presente Reglamento desarrolla el acervo de Schengen, Dinamarca decidirá, de conformidad con el artículo 4 de dicho Protocolo, dentro de 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.

(74) El Reino Unido participa en el presente Reglamento de conformidad con el artículo 5, apartado 1, del Protocolo n.º 19 sobre el acervo de Schengen integrado en el marco de la Unión Europea, anejo al TUE y al TFUE, y con el artículo 8, apartado 2, de la Decisión 2000/365/CE del Consejo[1].

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

(75) Irlanda participa en el presente Reglamento de conformidad con el artículo 5, apartado 1, del Protocolo n.º 19 anejo al TUE y al TFUE, y con el artículo 6, apartado 2, de la Decisión 2002/192/CE del Consejo[1].

(76) Por lo que respecta a Islandia y Noruega, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del Acuerdo celebrado por el Consejo de la Unión Europea, 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[2], que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE del Consejo[3].

---

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

2 DO L 176 de 10.7.1999, p. 36.

3 Decisión 1999/437/CE del Consejo, de 17 de mayo de 1999, relativa a determinadas normas de desarrollo 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 (DO L 176 de 10.7.1999, p. 31).

(77) Por lo que respecta a Suiza, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del Acuerdo firmado entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen[1], que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE, en relación con el artículo 3 de la Decisión 2008/149/JAI del Consejo[2].

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

[2] Decisión 2008/149/JAI del Consejo, de 28 de enero de 2008, relativa a la celebración, en nombre de la Unión Europea, del 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 (DO L 53 de 27.2.2008, p. 50).

(78) Por lo que respecta a Liechtenstein, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del Protocolo entre la Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein sobre la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen[1], que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE, en relación con el artículo 3 de la Decisión 2011/349/UE del Consejo[2].

---

1 DO L 160 de 18.6.2011, p. 21.

2 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 policial (DO L 160 de 18.6.2011, p. 1).

(79) Por lo que respecta a Bulgaria y Rumanía, el presente Reglamento constituye un acto que desarrolla el acervo de Schengen o está relacionado con él de otro modo en el sentido del artículo 4, apartado 2, del Acta de adhesión de 2005 y debe interpretarse conjuntamente con las Decisiones 2010/365/UE[1] y (UE) 2018/934[2] del Consejo.

(80) Por lo que respecta a Croacia, el presente Reglamento constituye un acto que desarrolla el acervo de Schengen o está relacionado con él de otro modo en el sentido del artículo 4, apartado 2, del Acta de adhesión de 2011, y debe interpretarse conjuntamente con la Decisión (UE) 2017/733 del Consejo[3].

(81) Por lo que respecta a Chipre, el presente Reglamento constituye un acto que desarrolla el acervo de Schengen o está relacionado con él de otro modo en el sentido del artículo 3, apartado 2, del Acta de adhesión de 2003.

(82) El presente Reglamento debe 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.

---

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

2 Decisión (UE) 2018/934 del Consejo, de 25 de junio de 2018, relativa a la puesta en aplicación de las disposiciones restantes del acervo de Schengen relacionadas con el Sistema de Información de Schengen en la República de Bulgaria y en Rumanía (DO L 165 de 2.7.2018, p. 37).

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

(83) El presente Reglamento introduce una serie de mejoras en el SIS que aumentarán su eficacia, reforzarán la protección de datos y ampliarán los derechos de acceso. Algunas de estas mejoras no requieren avances técnicos complejos, mientras que otras precisan modificaciones técnicas de diversa magnitud. Con objeto de permitir que las mejoras en el sistema estén disponibles para los usuarios finales lo antes posible, el presente Reglamento introduce modificaciones en la Decisión 2007/533/JAI en varias fases. Algunas de las mejoras introducidas en el sistema deben aplicarse con carácter inmediato a partir de la entrada en vigor del presente Reglamento y otras deben aplicarse uno o dos años después de su entrada en vigor. El presente Reglamento debe aplicarse en su integridad en un plazo de tres años a partir de su entrada en vigor. A fin de evitar retrasos en la ejecución del presente Reglamento, debe hacerse un atento seguimiento de las diversas fases de su aplicación.

(84) El Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo[1], la Decisión 2007/533/JAI y la Decisión 2010/261/UE de la Comisión[2] deben quedar derogados con efectos a partir de la fecha de aplicación completa del presente Reglamento.

(85) El Supervisor Europeo de Protección de Datos fue consultado de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo[3] y emitió su dictamen el 3 de mayo de 2017.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

---

1 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).

2 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).

3 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).

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, con inclusión del mantenimiento de la seguridad y el orden públicos y la salvaguardia de la seguridad en el territorio de los Estados miembros, y garantizar la aplicación de las disposiciones de los capítulos 4 y 5 del título V de la tercera parte del TFUE relativas a la circulación de personas en sus territorios, con la ayuda de la información transmitida a través de este sistema.

Artículo 2

Objeto

1. El presente Reglamento establece las condiciones y los procedimientos para la introducción en el SIS y el tratamiento de las descripciones sobre personas y objetos, así como para el 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 de la Unión Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (eu-LISA), el tratamiento general de los datos, los derechos de los interesados y la responsabilidad.

Artículo 3

Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «descripción»: un conjunto de datos introducidos en el SIS que permiten a las autoridades competentes identificar a una persona o un objeto a fin de adoptar una medida específica;

2) «información complementaria»: información que no forma parte de los datos de una descripción almacenada en el SIS, pero que está relacionada con descripciones del SIS y se intercambiará a través de las oficinas Sirene:

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

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

   c) cuando no pueda ejecutarse la medida requerida;

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

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

   f) al tratar del ejercicio del derecho de acceso;

3) «datos adicionales»: los 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 una consulta del SIS, se localice a personas sobre las cuales se hayan introducido datos en el SIS;

4) «datos personales»: los datos personales según la definición del artículo 4, punto 1, del Reglamento (UE) 2016/679;

5) «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, inscripción, 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;

6) «coincidencia»: la realización de los siguientes pasos:

   a) un usuario final ha realizado una consulta en el SIS;

   b) la consulta ha arrojado como resultado la existencia de una descripción introducida en el SIS por otro Estado miembro;

   c) los datos relativos a la descripción en el SIS coinciden con los datos utilizados para la consulta;

7) «respuesta positiva»: toda coincidencia que cumpla los siguientes criterios:

   a) haber sido confirmada por:

      i) el usuario final, o

      ii) la autoridad competente con arreglo a los procedimientos nacionales, cuando la coincidencia en cuestión estuviese basada en la comparación de datos biométricos;

      y

   b) requerir la adopción de medidas;

8) «indicación»: la 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 vulnerables, y a las descripciones a efectos de controles discretos, de investigación y específicos;

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

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

11) «usuario final»: todo miembro del personal de una autoridad competente autorizado para consultar directamente la CS-SIS, el N.SIS o una copia técnica de estos;

12) «datos biométricos»: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características morfológicas o fisiológicas de una persona física, que permitan o confirmen la identificación única de dicha persona, a saber, fotografías, imágenes faciales, datos dactiloscópicos y perfil de ADN;

13) «datos dactiloscópicos»: los datos relativos a impresiones dactilares o 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;

14) «imagen facial»: las imágenes digitales del rostro con una resolución de imagen y calidad suficientes para ser utilizadas en el sistema de correspondencias biométricas automatizadas;

15) «perfil de ADN»: el código alfabético o numérico que representa un conjunto de características identificativas de la parte no codificante de una muestra de ADN humano analizada, es decir, la estructura molecular específica en los diversos loci (posiciones) de ADN;

16) «delitos de terrorismo»: los delitos previstos en el Derecho nacional a los que se refieren los artículos 3 a 14 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo[1] o equivalentes a alguno de tales delitos en el caso de los Estados miembros que no estén vinculados por la citada Directiva;

17) «amenaza para la salud pública»: una amenaza para la salud pública tal como se define en el artículo 2, punto 21, del Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo[2].

Artículo 4

Arquitectura técnica y funcionamiento del SIS

1. El SIS se compondrá de:

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

i) una unidad de apoyo técnico («CS-SIS»), que contendrá una base de datos (en lo sucesivo, «base de datos del SIS») y que incluirá una copia de seguridad de la CS-SIS;

ii) 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, y que incluirá al menos un N.SIS de respaldo nacional o compartido; y

---

[1] Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).

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

c) una infraestructura de comunicación entre la CS-SIS, la copia de seguridad de la CS-SIS y la NI-SIS (en lo sucesivo, «infraestructura de comunicación») que proporcione una red virtual codificada dedicada a los datos del SIS y al intercambio de datos entre las oficinas Sirene como dispone el artículo 7, apartado 2.

El N.SIS a que se refiere la letra b) podrá contener un fichero de datos («copia nacional») con una copia total o parcial de la base de datos del SIS. Dos o más Estados miembros podrán establecer en uno de sus N.SIS una copia compartida que podrá ser usada conjuntamente por esos Estados miembros. La copia compartida se considerará la copia nacional de cada uno de esos Estados miembros.

Dos o más Estados miembros podrán usar conjuntamente el N.SIS de respaldo compartido a que se refiere la letra b). En tales casos, el N.SIS de respaldo compartido se considerará el N.SIS de respaldo de cada uno de esos Estados miembros. El N.SIS y su copia de respaldo podrán utilizarse simultáneamente para garantizar una disponibilidad ininterrumpida a los usuarios finales.

Los Estados miembros que tengan previsto crear una copia compartida o un N.SIS de respaldo compartido para usarlos conjuntamente acordarán sus respectivas responsabilidades por escrito. Notificarán dicho acuerdo a la Comisión.

La infraestructura de comunicación contribuirá a garantizar la disponibilidad ininterrumpida del SIS y prestará apoyo para ello. Incluirá rutas redundantes y separadas para las conexiones entre la CS-SIS y la copia de seguridad de la CS-SIS y también incluirá rutas redundantes y separadas para las conexiones entre cada punto de acceso nacional a la red del SIS y la CS-SIS y la copia de seguridad de la CS-SIS.

2. Los Estados miembros introducirán, actualizarán, suprimirán y consultarán datos del SIS a través de sus propios N.SIS. Los Estados miembros que usen una copia nacional parcial o completa, o una copia compartida parcial o completa la hará disponible para la realización de consultas automatizadas en el territorio de cada uno de esos Estados miembros. La copia parcial nacional o compartida contendrá, como mínimo, los datos enumerados en el artículo 20, apartado 3, letras a) a v). No se permitirá la consulta de ficheros de datos del N. SIS de otros Estados miembros, excepto en el caso de las copias compartidas.

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 copia de seguridad de la CS-SIS deberán estar situadas en los dos emplazamientos técnicos de eu-LISA.

4. Eu-LISA implantará soluciones técnicas para reforzar la disponibilidad ininterrumpida del SIS, mediante el funcionamiento simultáneo de la CS-SIS y su copia de seguridad, a condición de que la copia de seguridad de la CS-SIS siga siendo capaz de garantizar el funcionamiento del SIS en caso de fallo de la CS-SIS, o mediante la duplicación del sistema o de sus componentes. Sin perjuicio de los requisitos de procedimiento establecidos en el artículo 10 del Reglamento (UE) 2018/…[+], eu-LISA preparará, a más tardar el … [un año después de la entrada en vigor del presente Reglamento], un estudio sobre las opciones en lo que respecta a las soluciones técnicas que contenga una evaluación de impacto independiente y un análisis coste-beneficio.

5. Cuando sea necesario por circunstancias excepcionales, eu-LISA podrá realizar temporalmente una copia adicional de la base de datos del SIS.

[+] DO: insértese el número de serie del Reglamento que figura en el documento PE-CONS 29/18.

6. 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. Para los Estados miembros que utilicen una copia nacional o compartida, 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; y

c) la inicialización y restauración de las copias nacionales.

7. La CS-SIS asegurará 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. Dichos costes incluirán los trabajos realizados en relación con la CS-SIS para garantizar la prestación de los servicios a que se refiere el artículo 4, apartado 6.

2. Los costes de creación, funcionamiento, mantenimiento y ulterior desarrollo de cada N.SIS correrán a cargo del Estado miembro correspondiente.

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 conectarlo a la NI-SIS.

Cada Estado miembro será responsable de garantizar la disponibilidad ininterrumpida de los datos del SIS para los usuarios finales.

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

Artículo 7

Oficina N.SIS y oficina Sirene

1. Cada Estado miembro designará una autoridad (denominada «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.

2. Cada Estado miembro designará una autoridad nacional (denominada «oficina Sirene»), operativa las veinticuatro horas del día y los siete días de la semana, que se encargará de garantizar el intercambio y la disponibilidad de toda la información complementaria, de conformidad con el Manual Sirene. Cada oficina Sirene servirá de punto de contacto único de su respectivo Estado miembro para el intercambio de información complementaria relativa a las descripciones y para facilitar la adopción de las medidas solicitadas cuando se hayan introducido en el SIS descripciones sobre personas u objetos y esas personas u objetos hayan sido localizados a raíz de una respuesta positiva.

Conforme al Derecho nacional, cada oficina Sirene podrá acceder fácilmente, de forma directa o indirecta, a toda la información nacional pertinente, incluidas las bases de datos nacionales y toda la información relativa a las descripciones de su respectivo Estado miembro, así como al asesoramiento de expertos, con el fin de poder responder a las solicitudes de información complementaria con prontitud y dentro de los plazos establecidos en el artículo 8.

Las oficinas Sirene coordinarán la verificación de la calidad de la información introducida en el SIS. Para ello, tendrán acceso a los datos tratados en el SIS.

3. Los Estados miembros comunicarán a eu-LISA los datos relativos a su oficina N.SIS y a su oficina Sirene. Eu-LISA publicará la lista de las oficinas N.SIS y de las oficinas Sirene junto con la lista a la que se refiere el artículo 56, apartado 7.

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 técnicos y humanos necesarios para garantizar la disponibilidad continua y el intercambio oportuno y eficaz de información complementaria. En caso de indisponibilidad de la infraestructura de comunicación, los Estados miembros deberán emplear otros medios técnicos dotados de características adecuadas de seguridad para intercambiar información complementaria. El Manual Sirene recogerá una lista de los medios técnicos dotados de características adecuadas de seguridad.

2. La información complementaria se utilizará únicamente para el fin para el que haya sido transmitida de conformidad con el artículo 64, a menos que se haya obtenido el consentimiento previo del Estado miembro emisor para utilizarla con otro fin.

3. Las oficinas Sirene llevarán a cabo su cometido de manera rápida y eficiente, en particular respondiendo a las solicitudes de información complementaria lo antes posible, y como máximo doce horas después de su recepción. En el caso de las descripciones relativas a delitos de terrorismo, de las descripciones sobre personas en búsqueda para su detención a efectos de entrega o extradición y de las descripciones relativas a menores a que se refiere el artículo 32, apartado 1, letra c), las oficinas Sirene actuarán inmediatamente.

   Las solicitudes de información complementaria que tengan máxima prioridad deberán marcarse con el calificativo «URGENTE» en los formularios Sirene y deberán especificarse las razones que motivan la urgencia.

4. La Comisión adoptará actos de ejecución para establecer normas detalladas sobre las funciones que competen a las oficinas Sirene en virtud del presente Reglamento y sobre el intercambio de información complementaria, que adoptarán la forma de un manual titulado «Manual Sirene». Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 9

Conformidad técnica y operativa

1. Al establecer su N.SIS, cada Estado miembro deberá ajustarse a las normas, protocolos y procedimientos técnicos comunes establecidos a fin de garantizar la compatibilidad de su N.SIS con el SIS Central para la transmisión rápida y eficaz de los datos.

2. Cuando un Estado miembro utilice una copia nacional se asegurará, mediante los servicios prestados por la CS-SIS y las actualizaciones automáticas a que se refiere el artículo 4, apartado 6, de que los datos almacenados en la copia nacional sean 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.

3. Los usuarios finales recibirán los datos necesarios para llevar a cabo sus tareas, en particular, y cuando sea necesario, todos los datos disponibles que permitan la identificación del interesado y la adopción de las medidas requeridas.

4. Los Estados miembros y eu-LISA realizarán pruebas periódicas para comprobar la conformidad técnica de las copias nacionales a que se refiere el apartado 2. Los resultados de estas pruebas se tendrán en cuenta como parte del mecanismo establecido en el Reglamento (UE) n.º 1053/2013 del Consejo[1].

5. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas, protocolos y procedimientos técnicos comunes a que se refiere el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 76, apartado 2.

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 el acceso de personas no autorizadas a las instalaciones utilizadas para el tratamiento de datos personales (control en la entrada de las instalaciones);

[1] 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).

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) impedir el tratamiento no autorizado de los datos introducidos en el SIS y toda modificación o supresión no autorizada de datos tratados en el SIS (control de la entrada de datos);

g) 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 identificadores de usuario personales e intransferibles y con modos de acceso confidenciales (control de acceso a los datos);

h) 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 que pongan dichos perfiles a disposición de las autoridades de control a que se refiere el artículo 69, apartado 1, sin dilación a petición de estas (perfiles del personal);

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

j) garantizar que pueda verificarse y determinarse a posteriori qué datos personales se han introducido en el sistema de tratamiento automatizado de datos, en qué momento, por qué persona y para qué fines (control de la introducción);

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

l) controlar la eficacia de las medidas de seguridad mencionadas en el presente apartado y adoptar las medidas necesarias de organización relativas al control interno, a fin de garantizar el cumplimiento del presente Reglamento (auditoría interna);

m) asegurar que los sistemas instalados puedan ser restaurados a un funcionamiento normal (recuperación) en caso de interrupción; y

n) asegurar que las funciones del SIS se realicen satisfactoriamente, que se notifiquen los defectos de funcionamiento (fiabilidad) y que los datos personales conservados en el SIS no puedan ser corrompidos por el mal funcionamiento del sistema (integridad).

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 garantizando la seguridad de las instalaciones de las oficinas Sirene.

3. Los Estados miembros tomarán medidas equivalentes a las mencionadas en el apartado 1 del presente artículo en materia de seguridad en relación con el tratamiento de los datos del SIS por las autoridades mencionadas en el artículo 44.

4. Las medidas descritas en los apartados 1, 2 y 3 podrán formar parte de un planteamiento y un plan de seguridad generales de ámbito nacional aplicables a múltiples sistemas informáticos. En tales casos, los requisitos previstos en el presente artículo y su aplicabilidad al SIS deberán figurar de forma claramente identificable en ese plan y quedar garantizados por él.

Artículo 11

Confidencialidad – Estados miembros

1. 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 Derecho nacional. Dicha obligación seguirá siendo aplicable después del cese en el cargo o el empleo de dichas personas o tras la terminación de las actividades de dichos organismos.

2. Cuando un Estado miembro coopere con contratistas externos en cometidos relacionados con el SIS, deberá supervisar atentamente las actividades del contratista para garantizar el cumplimiento de todas las disposiciones del presente Reglamento, en particular en materia de seguridad, confidencialidad y protección de datos.

3. No se encomendará a empresas u organizaciones privadas la gestión operativa del N.SIS o de cualesquiera copias técnicas.

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, se proceda a un control interno y se garantice el correcto funcionamiento del N.SIS, así como para la integridad y seguridad de los datos. Este requisito no se aplicará a los tratamientos automáticos a que se refiere el artículo 4, apartado 6, letras a), b) y c).

2. Los registros contendrán, en particular, el historial de la descripción, la fecha y hora de la actividad de tratamiento de los datos, los datos utilizados para realizar una consulta, una referencia a los datos tratados y los identificadores de usuario personales e intransferibles de la autoridad competente y de la persona que efectúa el tratamiento de los datos.

3. Como excepción a lo dispuesto en el apartado 2 del presente artículo, si la consulta se realiza con datos dactiloscópicos o imágenes faciales de conformidad con el artículo 43, los registros mostrarán el tipo de datos utilizados para efectuar la consulta en lugar de los datos reales.

4. Los registros solo se utilizarán para los fines mencionados en el apartado 1 y se suprimirán en un plazo de tres años a partir de su creación. Los registros que incluyan el historial de las descripciones serán suprimidos transcurrido un plazo de tres años a partir de la supresión de las descripciones.

5. Los registros podrán conservarse durante plazos mayores que los indicados en el apartado 4 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 los registros, dentro de los límites de sus competencias y previa petición, a fin de poder desempeñar sus funciones.

7. Cuando los Estados miembros, de conformidad con la legislación nacional, lleven a cabo consultas automatizadas mediante escaneo de las matrículas de vehículos de motor utilizando sistemas de reconocimiento automático de matrículas, deberán mantener un registro de la consulta de conformidad con la legislación nacional. En caso necesario, podrá llevarse a cabo una consulta completa en el SIS para verificar si se ha obtenido una respuesta positiva. Los apartados 1 a 6 se aplicarán a toda consulta completa.

8. La Comisión adoptará actos de ejecución para determinar el contenido del registro a que se refiere el apartado 7 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

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 de control.

Artículo 14

Formación del personal

1. Antes de ser autorizado a tratar 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, derechos fundamentales, incluida la protección de datos, y sobre las normas y procedimientos del Manual Sirene en lo que respecta al tratamiento de datos. El personal será informado acerca de las disposiciones aplicables en materia de delitos y sanciones penales, incluidas las establecidas de conformidad con el artículo 73.

2. Los Estados miembros deberán disponer de un programa nacional de formación sobre el SIS, que incluirá la formación destinada a los usuarios finales y al personal de las oficinas Sirene.

   Dicho programa de formación podrá formar parte de un programa de formación general de ámbito nacional aplicable a la formación en otros ámbitos pertinentes.

3. Se organizarán cursos de formación comunes a nivel de la Unión al menos una vez al año para reforzar la cooperación entre las oficinas Sirene.

CAPÍTULO III
RESPONSABILIDADES DE Eu-LISA

Artículo 15

Gestión operativa

1. Eu-LISA será responsable de la gestión operativa del SIS Central. Eu-LISA se asegurará, en cooperación con los Estados miembros, de que en el SIS Central se utilice en todo momento la mejor tecnología disponible, con sujeción a un análisis de costes y beneficios.

2. Eu-LISA 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;

   d) ejecución del presupuesto;

   e) adquisición y renovación; y

   f) cuestiones contractuales.

3. Eu-LISA será responsable asimismo de las siguientes funciones relacionadas con las oficinas Sirene y la comunicación entre ellas:

a) coordinación, gestión y apoyo de las actividades de prueba;

b) mantenimiento y actualización de las especificaciones técnicas relativas al intercambio de información complementaria entre las oficinas Sirene y la infraestructura de comunicación, y

c) gestión del impacto de los cambios técnicos cuando afecten al SIS y al intercambio de información complementaria entre las oficinas Sirene.

4. Eu-LISA desarrollará y mantendrá un mecanismo y procedimientos para realizar controles de calidad de los datos de la CS-SIS. A este respecto, presentará informes regulares a los Estados miembros.

Eu-LISA presentará a la Comisión un informe periódico sobre los problemas detectados y los Estados miembros afectados.

La Comisión transmitirá al Parlamento Europeo y al Consejo un informe periódico sobre los problemas detectados en relación con la calidad de los datos.

5. Eu-LISA también desempeñará funciones relacionadas con la oferta de formación sobre la utilización técnica del SIS y sobre medidas encaminadas a mejorar la calidad de los datos del SIS.

6. La gestión operativa del SIS Central consistirá en todas las funciones necesarias para mantenerlo en funcionamiento ininterrumpido (las 24 horas del día, los 7 días de la semana), de conformidad con el presente Reglamento y, en particular, en el trabajo de mantenimiento y de adaptación técnica necesario para el buen funcionamiento del sistema. Estas tareas incluirán asimismo la coordinación, gestión y apoyo de las actividades de prueba para el SIS Central y los N.SIS, cuyo fin es garantizar que el SIS Central y los N.SIS funcionen con arreglo a los requisitos de conformidad técnica y operativa establecidos en el artículo 9.

7. La Comisión adoptará actos de ejecución para determinar los requisitos técnicos de la infraestructura de comunicación. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 16

Seguridad – eu-LISA

1. Eu-LISA 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 el acceso de personas no autorizadas a las instalaciones utilizadas para el tratamiento de datos personales (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) impedir el tratamiento no autorizado de los datos introducidos en el SIS y toda modificación o supresión no autorizada de datos tratados en el SIS (control de la entrada de datos);

g) 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 identificadores de usuario personales e intransferibles y con modos de acceso confidenciales (control de acceso a los datos);

h) 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 poner dichos perfiles a disposición del Supervisor Europeo de Protección de Datos, sin dilación a petición de este (perfiles del personal);

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

j) garantizar que pueda verificarse y determinarse a posteriori qué datos personales se han introducido en el sistema de tratamiento automatizado de datos, en qué momento y por qué persona (control de la introducción);

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

l) 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 el control interno, a fin de garantizar el cumplimiento del presente Reglamento (auditoría interna);

m) asegurar que los sistemas instalados puedan ser restaurados a su funcionamiento normal (recuperación) en caso de interrupción;

n) asegurar que las funciones del SIS se realicen satisfactoriamente, que se notifiquen los defectos de funcionamiento (fiabilidad) y que los datos personales conservados en el SIS no puedan ser corrompidos por el mal funcionamiento del sistema (integridad); y

o) garantizar la seguridad de sus emplazamientos técnicos.

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

Artículo 17

Confidencialidad – eu-LISA

1. Sin perjuicio del artículo 17 del Estatuto de los funcionarios, eu-LISA aplicará a todo miembro de su personal que trabaje con datos del SIS normas adecuadas sobre secreto profesional u otras obligaciones equivalentes de confidencialidad, de nivel comparable al de las normas previstas en el artículo 11 del presente Reglamento. Dicha obligación seguirá siendo aplicable después del cese en el cargo o el empleo de dichas personas o tras la terminación de sus actividades.

2. Eu-LISA 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.

3. Cuando eu-LISA coopere con contratistas externos en cometidos relacionados con el SIS, supervisará atentamente las actividades del contratista para garantizar el cumplimiento de todas las disposiciones del presente Reglamento, en particular en materia de seguridad, confidencialidad y protección de datos.

4. No se encomendará a empresas u organizaciones privadas la gestión operativa de la CS-SIS.

Artículo 18

Registros centrales

1. Eu-LISA garantizará que todo acceso a datos personales y todo intercambio de datos personales en la CS-SIS queden registrados para los fines expresados en el artículo 12, apartado 1.

2. Los registros contendrán, en particular, el historial de la descripción, la fecha y hora de la actividad de tratamiento de los datos, los datos utilizados para realizar una consulta, una referencia a los datos tratados y los identificadores de usuario personales e intransferibles de la autoridad competente que efectúa el tratamiento de los datos.

3. Como excepción a lo dispuesto en el apartado 2 del presente artículo, si la consulta se realiza con datos dactiloscópicos o imágenes faciales de conformidad con el artículo 43, los registros mostrarán el tipo de datos utilizados para efectuar la consulta en lugar de los datos reales.

4. Los registros solo se utilizarán para los fines mencionados en el apartado 1 y se suprimirán en un plazo de tres años a partir de su creación. Los registros que incluyan el historial de las descripciones serán suprimidos transcurrido un plazo de tres años a partir de la supresión de las descripciones.

5. Los registros podrán conservarse durante plazos mayores que los indicados en el apartado 4, si son necesarios para procedimientos de control ya en curso.

6. A efectos de control interno y para garantizar el funcionamiento adecuado de la CS-SIS y la integridad y seguridad de los datos, eu-LISA tendrá acceso a los registros, dentro de los límites de sus competencias.

   El Supervisor Europeo de Protección de Datos tendrá acceso a dichos registros previa solicitud, dentro de los límites de sus competencias y a fin de poder desempeñar sus funciones.

CAPÍTULO IV
INFORMACIÓN AL PÚBLICO

Artículo 19

Campañas de información del SIS

Al iniciarse la aplicación del presente Reglamento, la Comisión, en cooperación con las autoridades de control y el Supervisor Europeo de Protección de Datos, realizará una campaña para informar al público sobre los objetivos del SIS, los datos almacenados en el SIS, las autoridades con acceso al SIS y los derechos de los interesados. La Comisión repetirá estas campañas periódicamente, en cooperación con las autoridades de control y el Supervisor Europeo de Protección de Datos. La Comisión mantendrá un sitio web abierto al público en el que se facilite toda la información pertinente sobre el SIS. Los Estados miembros, en cooperación con sus autoridades de control, definirán y aplicarán las medidas necesarias para informar al conjunto de sus ciudadanos y residentes 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, 38 y 40.

2. Las categorías de datos serán las siguientes:

   a) información sobre las personas respecto de las cuales se haya introducido una descripción;

   b) información sobre los objetos mencionados en los artículos 26, 32, 34, 36 y 38.

3. Las descripciones del SIS que incluyan información sobre personas contendrán solo los datos siguientes:

   a) apellidos;

   b) nombres;

   c) nombres y apellidos de nacimiento;

d) nombres y apellidos usados con anterioridad y alias;

e) rasgos físicos particulares, objetivos e inalterables;

f) lugar de nacimiento;

g) fecha de nacimiento;

h) sexo;

i) nacionalidad o nacionalidades;

j) indicación de si la persona afectada:

   i) va armada;

   ii) es violenta;

   iii) está fugada o se ha evadido;

   iv) presenta un riesgo de suicidio;

   v) es una amenaza para la salud pública; o

   vi) está implicada en alguna actividad de las recogidas en los artículos 3 a 14 de la Directiva (UE) 2017/541;

k) motivo de la descripción;

l) autoridad que creó la descripción;

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

n) medidas que deben tomarse en caso de respuesta positiva;

o) conexión con otras descripciones de conformidad con el artículo 63;

p) tipo de delito;

q) número de registro de la persona en un registro nacional;

r) para las descripciones a que se refiere el artículo 32, apartado 1, categorización del tipo de caso;

s) categoría de los documentos de identificación de la persona;

t) país de expedición de los documentos de identificación de la persona;

u) número o números de los documentos de identificación de la persona;

v) fecha de expedición de los documentos de identificación de la persona;

w) fotografías e imágenes faciales;

x) con arreglo al artículo 42, apartado 3, perfiles de ADN pertinentes;

y) datos dactiloscópicos;

z) fotocopia, a ser posible en color, de los documentos de identificación.

4. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en los apartados 2 y 3 del presente artículo y las normas comunes a que se refiere el apartado 5 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

5. Las normas técnicas serán similares para las consultas en la CS-SIS, en las copias nacionales o compartidas y en las copias técnicas efectuadas con arreglo al artículo 56, apartado 2. Se basarán en normas comunes.

Artículo 21

Proporcionalidad

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

2. Cuando se busque a una persona o un objeto en virtud de una descripción relacionada con un delito de terrorismo, el caso se considerará adecuado, pertinente y suficientemente importante como para justificar una descripción en el SIS. Los Estados miembros podrán abstenerse excepcionalmente, por motivos de seguridad pública o nacional, de introducir una descripción, si ello pudiera obstaculizar indagaciones, investigaciones o procedimientos administrativos o judiciales.

Artículo 22

Requisitos para la introducción de una descripción

1. Los datos mínimos necesarios para introducir una descripción en el SIS serán los previstos en el artículo 20, apartado 3, letras a), g), k) y n), excepto en las situaciones contempladas en el artículo 40. Los demás datos enumerados en dicho apartado se introducirán en el SIS si se dispone de ellos.

2. Los datos a que se refiere el artículo 20, apartado 3, letra e), del presente Reglamento solo se introducirán cuando sea estrictamente necesario para la identificación de la persona de que se trate. Cuando se introduzcan dichos datos, los Estados miembros garantizarán que se cumpla el artículo 10 de la Directiva (UE) 2016/680.

Artículo 23

Compatibilidad de las descripciones

1. Antes de introducir una descripción, el Estado miembro verificará si la persona o el objeto afectados ya son objeto de una descripción en el SIS. A fin de comprobar si la persona ya ha sido objeto de una descripción, también se efectuará una comprobación con los datos dactiloscópicos, si estos están disponibles.

2. Cada Estado miembro podrá introducir en el SIS una única descripción por persona u objeto. En caso necesario, otros Estados miembros podrán introducir nuevas descripciones sobre la misma persona u objeto, de conformidad con el apartado 3.

3. En caso de que una persona u objeto ya haya sido objeto de una descripción en el SIS, el Estado miembro que desee introducir una nueva descripción verificará que no existe incompatibilidad entre las descripciones. En caso de no existir incompatibilidad, el Estado miembro podrá introducir la nueva descripción. Si las descripciones son incompatibles, las correspondientes oficinas Sirene de los Estados miembros se consultarán mediante el intercambio de información complementaria para alcanzar un acuerdo. Las normas sobre compatibilidad de las descripciones se establecerán en el Manual Sirene. Se podrán establecer excepciones a esas normas de compatibilidad, previa consulta entre los Estados miembros, cuando así lo requieran intereses nacionales esenciales.

4. En caso de que se produzcan respuestas positivas sobre descripciones múltiples relativas a la misma persona u objeto, el Estado miembro de ejecución cumplirá las normas sobre prioridad de las descripciones establecidas en el Manual Sirene.

En caso de que una persona sea objeto de descripciones múltiples introducidas por distintos Estados miembros, se dará prioridad a las descripciones para la detención introducidas de conformidad con el artículo 26, a reserva de lo dispuesto en el artículo 25.

Artículo 24

Disposiciones generales sobre la introducción de indicaciones

1. Si un Estado miembro considera que la ejecución de la medida solicitada en una descripción introducida de conformidad con los artículos 26, 32 o 36 es incompatible con su legislación nacional, sus obligaciones internacionales o sus intereses nacionales esenciales, podrá exigir que se añada una indicación a la 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 de ejecución examinará si puede o no permitir que la indicación añadida a instancia suya sea 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 detención a efectos de entrega

1. Cuando la Decisión Marco 2002/584/JAI sea aplicable, un Estado miembro pedirá al Estado miembro emisor que añada a la descripción para detención a efectos de entrega una indicación destinada a impedir la detención, si la autoridad judicial competente para la ejecución de una orden de detención europea con arreglo al Derecho nacional hubiese denegado la ejecución acogiéndose a uno de los motivos de no ejecución previstos y se hubiese pedido añadir la correspondiente indicación.

   Un Estado miembro podrá pedir asimismo que se añada una indicación a la descripción si, durante el proceso de entrega, su autoridad judicial competente pone en libertad a la persona objeto de la descripción.

2. No obstante, a instancia de una autoridad judicial competente con arreglo al Derecho nacional que haya dado una instrucción general o para un caso concreto, un Estado miembro también podrá pedir al Estado miembro emisor que añada una indicación a una descripción para detención a efectos de entrega cuando sea obvio que tendrá que denegarse la ejecución de la orden de detención europea.

CAPÍTULO VI
DESCRIPCIONES SOBRE PERSONAS EN BÚSQUEDA PARA SU DETENCIÓN A EFECTOS DE ENTREGA O EXTRADICIÓN

Artículo 26

Objetivos y condiciones para introducir descripciones

1. Las descripciones sobre personas en búsqueda para su detención a efectos de entrega sobre la base 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 descripciones para detención a efectos de entrega sobre la base de órdenes de detención dictadas con arreglo a los acuerdos celebrados entre la Unión y terceros países en virtud de los Tratados, 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.

3. Cualquier referencia del presente Reglamento a las disposiciones de la Decisión Marco 2002/584/JAI se entenderá en el sentido de que se incluyen las disposiciones correspondientes de los acuerdos celebrados entre la Unión y terceros países en virtud de los Tratados, 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. Cuando haya una operación en curso, el Estado miembro emisor podrá desactivar temporalmente la posibilidad de que los usuarios finales en los Estados miembros que participan en la operación consulten una descripción a efectos de detención introducida con arreglo al presente artículo. En tales casos, únicamente tendrán acceso a la descripción las oficinas Sirene. Los Estados miembros solo impedirán el acceso a una descripción si:

a) el objetivo de la operación no puede lograrse con otras medidas;

b) la autoridad judicial competente del Estado miembro de emisión ha dado su autorización previa; y

c) todos los Estados miembros que participan en la operación han sido informados mediante el intercambio de información complementaria.

La funcionalidad prevista en el párrafo primero solo podrá utilizarse durante un período que no exceda de 48 horas. Sin embargo, en caso de que sea necesario por razones operativas, podrá prorrogarse por períodos sucesivos de 48 horas. Los Estados miembros llevarán estadísticas del número de descripciones con respecto a las cuales se haya utilizado esta funcionalidad.

5. Cuando haya indicios claros de que los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h), j) y k), están relacionados con una persona que es objeto de una descripción con arreglo a los apartados 1 y 2 del presente artículo, podrán introducirse descripciones relativas a dichos objetos para localizar a la persona. En tales casos, se establecerá una conexión entre las descripciones relativas a la persona y al objeto con arreglo a lo dispuesto en el artículo 63.

6. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en el apartado 5 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 27

Datos adicionales sobre personas en búsqueda para su detención a efectos de entrega

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

   Los Estados miembros podrán introducir la copia de varias órdenes de detención europeas en una descripción para la detención a efectos de entrega.

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

Artículo 28

Información complementaria sobre personas en búsqueda para su detención a efectos de entrega

El Estado miembro emisor de una descripción 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
en búsqueda para su detención a efectos de extradición

1. El Estado miembro emisor de una descripción a efectos de extradición comunicará los siguientes datos a todos los Estados miembros mediante el intercambio de información complementaria:

   a) la autoridad que emitió la orden de detención;

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

   c) la naturaleza y la tipificación jurídica del delito;

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

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

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

2. Los datos mencionados en el apartado 1 del presente artículo 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 ejecución ejecute la medida.

Artículo 30

Conversión de medidas que se deban tomar en relación con descripciones para la detención a efectos de entrega o extradición

Cuando no sea posible proceder a la detención, bien porque el Estado miembro requerido para realizarla se niegue, 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 haya concluido, el Estado miembro al que se pida realizar la detención actuará en relación con la descripción mediante la comunicación del paradero de la persona de que se trate.

Artículo 31

Ejecución de medidas basadas en una descripción para la detención a efectos de entrega o extradición

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

2. En los casos en que no sea aplicable la Decisión Marco 2002/584/JAI, las descripciones introducidas en el SIS de conformidad con los artículos 26 y 29 tendrán la misma fuerza jurídica que una solicitud de detención preventiva 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 SOBRE PERSONAS DESAPARECIDAS O PERSONAS VULNERABLES A QUIENES SE DEBE IMPEDIR VIAJAR

Artículo 32

Objetivos y condiciones para introducir descripciones

1. A petición de la autoridad competente del Estado miembro emisor se introducirán en el SIS descripciones sobre las siguientes categorías de personas:

   a) personas desaparecidas que requieran medidas de protección

      i) para su propia protección;

      ii) para prevenir una amenaza para el orden público o la seguridad pública;

   b) personas desaparecidas que no requieran medidas de protección;

   c) menores en riesgo de sustracción por parte de uno de los padres, un miembro de la familia o un tutor, a quienes se deba impedir viajar;

d) menores a quienes se deba impedir viajar por existir un riesgo concreto y evidente de que abandonen el territorio de un Estado miembro o sean trasladados fuera de él y de que:

i) sean víctimas de trata de personas, o de matrimonios forzados, mutilación genital femenina u otras formas de violencia de género,

ii) sean víctimas de delitos de terrorismo o se vean involucrados en ellos, o

iii) sean reclutados o alistados en grupos armados u obligados a participar activamente en hostilidades;

e) personas vulnerables mayores de edad a quienes se deba impedir viajar por su propia protección, debido a un riesgo concreto y evidente de que abandonen el territorio de un Estado miembro o sean trasladadas fuera de él y sean víctimas de trata de personas o violencia de género.

2. El apartado 1, letra a), se aplicará en particular a los menores y a las personas que deban ser internadas por resolución de una autoridad competente.

3. Las descripciones relativas a menores a que se hace referencia en el apartado 1, letra c), se introducirán previa decisión de las autoridades competentes, incluidas las autoridades judiciales de los Estados miembros que tengan jurisdicción en materia de responsabilidad parental, cuando exista un riesgo concreto y evidente de que el menor sea trasladado de manera inminente e ilegal fuera del Estado miembro en el que estén situadas las autoridades competentes.

4. Las descripciones relativas a las personas a que se hace referencia en el apartado 1, letras d) y e), se introducirán previa decisión de las autoridades competentes, incluidas las autoridades judiciales.

5. El Estado miembro emisor revisará periódicamente la necesidad de mantener las descripciones a que hace referencia el apartado 1, letras c), d) y e), del presente artículo, con arreglo al artículo 53, apartado 4.

6. El Estado miembro emisor garantizará que:

   a) los datos que introduzca en el SIS indiquen a cuál de las categorías previstas en el apartado 1 pertenece la persona objeto de la descripción;

   b) los datos que introduzca en el SIS indiquen de qué tipo de caso se trata, siempre que este se conozca; y

   c) en relación con las descripciones introducidas con arreglo al apartado 1, letras c), d) y e), su oficina Sirene ponga a su disposición toda la información pertinente, en el momento de la creación de la descripción.

7. Cuatro meses antes de que un menor que sea objeto de una descripción prevista en el presente artículo alcance la mayoría de edad con arreglo a la legislación nacional del Estado miembro emisor, la CS-SIS notificará automáticamente al Estado miembro emisor que el motivo de la descripción y la medida requerida han de actualizarse o que la descripción debe suprimirse.

8. Cuando haya indicios claros de que los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h) y k), están relacionados con una persona que sea objeto de una descripción con arreglo al apartado 1 del presente artículo, podrán introducirse descripciones relativas a dichos objetos para localizar a la persona. En tales casos, se establecerá una conexión entre las descripciones relativas a la persona y al objeto con arreglo a lo dispuesto en el artículo 63.

9. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas sobre la categorización de los tipos de casos y la introducción de los datos a los que se hace referencia en el apartado 6. Los tipos de casos de personas desaparecidas que sean menores incluirán, sin carácter exhaustivo, las fugas, los menores no acompañados en el contexto de la migración y los menores en riesgo de sustracción parental.

La Comisión adoptará también actos de ejecución a fin de establecer y desarrollar las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en el apartado 8.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 33

Ejecución de medidas basada en una descripción

1. Cuando se localice a una persona de las mencionadas en el artículo 32, las autoridades competentes del Estado miembro de ejecución comunicarán, con sujeción a los requisitos establecidos en el apartado 4, su paradero al Estado miembro emisor.

2. Cuando se trate de personas que requieran medidas de protección según se indica en el artículo 32, apartado 1, letras a), c), d) y e), el Estado miembro de ejecución consultará inmediatamente a sus autoridades competentes y a las del Estado miembro emisor mediante el intercambio de información complementaria con el fin de acordar sin demora las medidas que deben adoptarse. Las autoridades competentes del Estado miembro de ejecución podrán, con arreglo al Derecho nacional, trasladar a dichas personas a un lugar seguro con el fin de impedirles que continúen su viaje.

3. En el caso de los menores, toda decisión sobre las medidas que deban adoptarse o toda decisión de trasladar al menor a un lugar seguro con arreglo al apartado 2 se adoptará atendiendo al interés superior del menor. Tales decisiones se adoptarán de inmediato y como máximo doce horas después del momento en el que se localice al menor, en consulta con las autoridades correspondientes de protección de menores, según proceda.

4. 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 autoridades competentes podrán comunicar a la persona que informó de la desaparición el hecho de que se ha suprimido la descripción ya que se ha localizado a la persona desaparecida.

CAPÍTULO VIII
DESCRIPCIONES SOBRE PERSONAS EN BÚSQUEDA A EFECTOS DE UN PROCEDIMIENTO JUDICIAL

Artículo 34

Objetivos y condiciones para introducir descripciones

1. A efectos de la comunicación del lugar de residencia o del domicilio de una persona, los Estados miembros, previa solicitud de la autoridad competente, introducirán en el SIS descripciones sobre:

   a) testigos;

b) personas citadas o en búsqueda 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 que respondan 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 los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h) y k), están relacionados con una persona objeto de una descripción con arreglo al apartado 1 del presente artículo, podrán introducirse descripciones relativas a dichos objetos para localizar a la persona. En tales casos, se establecerá una conexión entre las descripciones relativas a la persona y al objeto con arreglo a lo dispuesto en el artículo 63.

3. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 35

Ejecución de medidas basada en una descripción

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

CAPÍTULO IX
DESCRIPCIONES SOBRE PERSONAS Y OBJETOS A EFECTOS DE CONTROLES DISCRETOS, DE INVESTIGACIÓN O ESPECÍFICOS

Artículo 36

Objetivos y condiciones para introducir descripciones

1. Las descripciones sobre personas, sobre los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h), i), j), k) y l), y sobre medios de pago distintos del efectivo serán introducidas de conformidad con el Derecho nacional del Estado miembro emisor, a efectos de controles discretos, de investigación o específicos de conformidad con el artículo 37, apartados 3, 4 y 5.

2. Cuando introduzca descripciones a efectos de controles discretos, de investigación o específicos y la información que solicite el Estado miembro emisor complemente la prevista en el artículo 37, apartado 1, letras a) a h), el Estado miembro emisor añadirá a la descripción toda la información que solicite. Si dicha información se refiere a las categorías especiales de datos personales mencionadas en el artículo 10 de la Directiva (UE) 2016/680, únicamente podrá solicitarse si resulta estrictamente necesaria para el fin concreto de la descripción y en lo que respecta al delito para el que se haya introducido la descripción.

3. Las descripciones sobre personas a efectos de controles discretos, de investigación o específicos podrán introducirse a efectos de la prevención, la detección, la investigación o el enjuiciamiento de delitos, la ejecución de una condena penal y la prevención de amenazas para la seguridad pública en una o varias de las circunstancias siguientes:

   a) cuando haya indicios claros de que una persona pretende cometer o está cometiendo cualquiera de los delitos mencionados en el artículo 2, apartados 1 y 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 pena de privación de libertad o una orden de detención en relación con una persona condenada por cualquiera de los delitos mencionados en el artículo 2, apartados 1 y 2, de la Decisión Marco 2002/584/JAI;

   c) cuando la evaluación global de una persona, en particular sobre la base de hechos delictivos anteriores, permita suponer que también podría cometer en el futuro los delitos mencionados en el artículo 2, apartados 1 y 2, de la Decisión Marco 2002/584/JAI.

4. Además, podrá introducirse una descripción sobre personas a efectos de controles discretos, de investigación o específicos de conformidad con el Derecho nacional a instancia de las autoridades competentes en materia de seguridad nacional, cuando haya indicios concretos de que la información mencionada en el artículo 37, apartado 1, es necesaria con objeto de evitar la amenaza grave que entrañe la persona de que se trate u otras amenazas graves para la seguridad nacional interior o exterior. El Estado miembro que haya introducido una descripción con arreglo al presente apartado informará de dicha descripción a los demás Estados miembros. Cada Estado miembro determinará a qué autoridades se transmitirá esta información. La información se transmitirá a través de las oficinas Sirene.

5. Cuando existan indicios claros de que los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h), j), k) o l), o medios de pago distintos del efectivo están relacionados con los delitos graves a que se refiere el apartado 3 del presente artículo o con las amenazas graves a que se refiere el apartado 4 del presente artículo, se podrá introducir una descripción sobre dichos objetos y vincularla a las descripciones introducidas con arreglo a los apartados 3 y 4 del presente artículo.

6. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en el apartado 5 del presente artículo y la información adicional mencionada en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 37

Ejecución de las medidas basada en una descripción

1. A efectos de controles discretos, de investigación o específicos, el Estado miembro de ejecución recogerá y comunicará al Estado miembro emisor la totalidad o parte de la información siguiente:

   a) el hecho de que se ha localizado a la persona objeto de una descripción o de que se han localizado los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h), j), k) o l), o los medios de pago distintos del efectivo objeto de una descripción;

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

   c) el itinerario y el destino del viaje;

   d) los acompañantes de la persona objeto de la descripción o los ocupantes del vehículo, embarcación o aeronave, o los acompañantes del titular del documento oficial en blanco o del documento de identidad expedido, de quienes pueda suponerse razonablemente que tienen relación con la persona objeto de la descripción;

   e) cualquier identidad revelada y descripción personal de la persona que utilizaba el documento oficial en blanco o el documento de identidad expedido objeto de la descripción;

   f) los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h), j), k) o l), o los medios de pago distintos del efectivo utilizados;

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

h) las circunstancias en las que se ha localizado a la persona o los objetos mencionados en el artículo 38, apartado 2, letras a), b), c), e), g), h), j), k) o l), o los medios de pago distintos del efectivo;

i) cualquier otra información solicitada por el Estado miembro emisor con arreglo a lo dispuesto en el artículo 36, apartado 2.

Si la información mencionada en la letra i) del párrafo primero del presente apartado tiene que ver con las categorías especiales de datos personales a que se refiere el artículo 10 de la Directiva (UE) 2016/680, se tratará de conformidad con las condiciones establecidas en dicho artículo y solo si complementa otros datos personales tratados para el mismo fin.

2. El Estado miembro de ejecución comunicará la información a que se refiere el apartado 1 mediante el intercambio de información complementaria.

3. Un control discreto comprenderá la recopilación discreta de tanta información de la descrita en el apartado 1 como sea posible durante las actividades habituales de las autoridades nacionales competentes del Estado miembro de ejecución. La recopilación de dicha información no deberá comprometer el carácter discreto de los controles, y la persona objeto de la descripción no será informada en modo alguno de la existencia de la descripción.

4. Un control de investigación comprenderá una entrevista a la persona, en particular sobre la base de información o cuestiones específicas añadidas a la descripción por el Estado miembro emisor de conformidad con el artículo 36, apartado 2. La entrevista se realizará de acuerdo con la legislación nacional del Estado miembro de ejecución.

5. Durante los controles específicos, las personas, vehículos, embarcaciones, aeronaves, contenedores y objetos transportados podrán ser registrados a los fines recogidos en el artículo 36. Los registros se llevarán a cabo de acuerdo con el Derecho nacional del Estado miembro de ejecución.

6. Los controles específicos se sustituirán por controles de investigación en los Estados miembros de ejecución cuyo Derecho nacional no autorice los controles específicos. Los controles de investigación se sustituirán por controles discretos en los Estados miembros de ejecución cuyo Derecho nacional no autorice los controles de investigación. Cuando sea de aplicación la Directiva 2013/48/UE, los Estados miembros garantizarán que se respete el derecho de los sospechosos y acusados a tener acceso a un abogado con arreglo a las condiciones establecidas en dicha Directiva.

7. El apartado 6 se entiende sin perjuicio de la obligación de los Estados miembros de facilitar a los usuarios finales la información solicitada en virtud del artículo 36, apartado 2.

CAPÍTULO X
DESCRIPCIONES SOBRE OBJETOS A EFECTOS DE INCAUTACIÓN O UTILIZACIÓN COMO PRUEBA EN UN PROCESO PENAL

Artículo 38

Objetivos y condiciones para introducir descripciones

1. Los Estados miembros introducirán en el SIS descripciones sobre objetos en búsqueda a efectos de su incautación o de su utilización como pruebas en un proceso penal.

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

a) vehículos de motor independientemente del sistema de propulsión;

b) remolques cuyo peso en vacío sea superior a 750 kg;

c) caravanas;

d) equipos industriales;

e) embarcaciones;

f) motores de embarcaciones;

g) contenedores;

h) aeronaves;

i) motores de aeronaves;

j) armas de fuego;

k) documentos oficiales en blanco que hayan sido robados, sustraídos o extraviados, o que se presenten como uno de estos documentos pero que sean falsos;

l) documentos de identidad expedidos, tales como pasaportes, tarjetas de identidad, permisos de residencia, documentos de viaje y permisos de conducción, que hayan sido robados, sustraídos, extraviados o anulados, o que se presenten como uno de estos documentos pero que sean falsos;

m) certificados de matriculación de vehículos y placas de matrícula de vehículos que hayan sido robados, sustraídos, extraviados o anulados, o que se presenten como uno de estos documentos o placas pero que sean falsos;

n) billetes de banco (billetes registrados) y billetes falsos;

o) artículos de tecnología de la información;

p) componentes identificables de vehículos de motor;

q) componentes identificables de equipos industriales;

r) otros objetos identificables de alto valor, tal como se definan con arreglo al apartado 3.

Con respecto a los documentos a los que se hace referencia en las letras k), l) y m), el Estado miembro emisor podrá especificar si dichos documentos han sido robados, sustraídos, extraviados, anulados o si son falsos.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 75 para modificar el presente Reglamento definiendo nuevas subcategorías de los objetos enumerados en el apartado 2, letras o), p), q) y r), del presente artículo.

4. La Comisión adoptará actos de ejecución para establecer y desarrollar las normas técnicas necesarias para la introducción, actualización, supresión y consulta de los datos mencionados en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 39

Ejecución de medidas basada en una descripción

1. Cuando como resultado de una consulta se compruebe la existencia de una descripción sobre un objeto que haya sido localizado, la autoridad competente se incautará del objeto de conformidad con el Derecho nacional y se pondrá en contacto con la autoridad del Estado miembro emisor para acordar las medidas que deban tomarse. 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 mediante el intercambio de información complementaria.

3. El Estado miembro de ejecución adoptará las medidas solicitadas de conformidad con su Derecho nacional.

CAPÍTULO XI
DESCRIPCIONES SOBRE PERSONAS DESCONOCIDAS EN BÚSQUEDA PARA SU IDENTIFICACIÓN CON ARREGLO AL DERECHO NACIONAL

Artículo 40

Descripciones sobre personas desconocidas en búsqueda para su identificación con arreglo al Derecho nacional

Los Estados miembros podrán introducir en el SIS descripciones sobre personas desconocidas en búsqueda que contengan solo datos dactiloscópicos. Esos datos dactiloscópicos serán conjuntos completos o incompletos de impresiones dactilares o palmares descubiertas en los lugares de comisión de delitos de terrorismo u otros delitos graves que estén siendo investigados. Solo se introducirán en el SIS cuando pueda acreditarse con un grado muy alto de probabilidad que pertenecen a uno de los autores del delito.

Si la autoridad competente del Estado miembro emisor no pudiera determinar la identidad del sospechoso a partir de los datos de ninguna otra base de datos nacional, de la Unión o internacional pertinente, los datos dactiloscópicos a que se hace referencia en el párrafo primero solo podrán introducirse en esta categoría de descripciones con la mención «persona desconocida en búsqueda» para su identificación.

Artículo 41

Ejecución de medidas basada en una descripción

En caso de se obtenga una respuesta positiva a partir de los datos introducidos con arreglo al artículo 40, la identidad de la persona se establecerá de conformidad con el Derecho nacional, debiendo verificar un perito que los datos dactiloscópicos en el SIS pertenecen a dicha persona. Los Estados miembros de ejecución comunicarán información sobre la identidad y paradero de la persona al Estado miembro emisor mediante el intercambio de información complementaria con el fin de facilitar una investigación oportuna del caso.

CAPÍTULO XII
NORMAS ESPECÍFICAS PARA DATOS BIOMÉTRICOS

Artículo 42

Normas específicas aplicables a la introducción de fotografías imágenes faciales, datos dactiloscópicos y perfiles de ADN

1. Solo se introducirán en el SIS las fotografías, las imágenes faciales y los datos dactiloscópicos mencionados en el artículo 20, apartado 3, letras w) e y), que cumplan las normas mínimas de calidad de los datos y las especificaciones técnicas. Antes de introducir ese tipo de datos, se comprobará su calidad, para determinar si se han cumplido las normas mínimas de calidad de los datos y las especificaciones técnicas.

2. Los datos dactiloscópicos introducidos en el SIS podrán consistir en una a diez impresiones dactilares planas y en una a diez impresiones dactilares rodadas. También podrán consistir en hasta dos impresiones palmares.

3. Solo se podrá añadir a las descripciones un perfil de ADN en las situaciones previstas en el artículo 32, apartado 1, letra a), únicamente tras un control de calidad que determine si se cumplen las normas mínimas de calidad de los datos y las especificaciones técnicas y solo cuando no se disponga de fotografías, imágenes faciales o datos dactiloscópicos o estos no sean adecuados para la identificación. Los perfiles de ADN de personas que sean ascendientes o descendientes directos o hermanos de la persona objeto de la descripción podrán añadirse a la descripción siempre que dichas personas den su consentimiento expreso. Cuando se añada un perfil de ADN a una descripción, dicho perfil deberá contener la mínima información estrictamente necesaria para la identificación de la persona desaparecida.

4. De conformidad con el apartado 5 del presente artículo, se establecerán normas mínimas de calidad de los datos y especificaciones técnicas para el almacenamiento de los datos biométricos a que se refieren los apartados 1 y 3 del presente artículo. Dichas normas mínimas de calidad de los datos y especificaciones técnicas determinarán el nivel de calidad necesario para utilizar los datos a efectos de comprobar la identidad de una persona de conformidad con el artículo 43, apartado 1, y de identificar a una persona de conformidad con el artículo 43, apartados 2 a 4.

5. La Comisión adoptará actos de ejecución a fin de establecer las normas mínimas de calidad de los datos y las especificaciones técnicas a que se refieren los apartados 1 y 3 y 4 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 43

Normas específicas aplicables a la comprobación o consulta mediante fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN

1. Cuando una descripción del SIS disponga de fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN, esas fotografías, imágenes faciales, datos dactiloscópicos y perfiles de ADN se utilizarán para confirmar la identidad de una persona que haya sido localizada como consecuencia de una consulta alfanumérica realizada en el SIS.

2. Los datos dactiloscópicos podrán consultarse en todos los casos para identificar a una persona. Ahora bien, los datos dactiloscópicos se consultarán para identificar a una persona cuando su identidad no pueda determinarse por otros medios. A tal fin, el SIS Central incluirá un sistema automático de identificación dactilar (SAID).

3. Los datos dactiloscópicos del SIS en relación con descripciones introducidas con arreglo a los artículos 26, 32, 36 y 40 también podrán cotejarse utilizando conjuntos completos o incompletos de impresiones dactilares o palmares descubiertas en los lugares de comisión de delitos graves o delitos de terrorismo que estén siendo investigados, cuando pueda acreditarse con un alto grado de probabilidad que los conjuntos de impresiones pertenecen a un autor del delito y siempre que la consulta se realice de forma simultánea en las pertinentes bases de datos nacionales de los Estados miembros de impresiones dactilares.

4. Tan pronto como sea técnicamente posible, y siempre que se garantice un alto nivel de fiabilidad de la identificación, podrán utilizarse fotografías e imágenes faciales para identificar a una persona en el contexto de los pasos fronterizos oficiales.

Antes de que se incorpore esta función en el SIS, la Comisión presentará un informe en el que examine si la tecnología necesaria está disponible, es fiable y está lista para su uso. Se consultará al Parlamento Europeo sobre este informe.

Una vez que se haya empezado a utilizar esta función en los pasos fronterizos oficiales, la Comisión estará facultada para adoptar actos delegados con arreglo al artículo 75 a fin de completar el presente Reglamento en lo que se refiere a la determinación de otras circunstancias en las que se puedan utilizar fotografías e imágenes faciales para la identificación de personas.

CAPÍTULO XIII
DERECHO DE ACCESO A LAS DESCRIPCIONES Y REVISIÓN DE DESCRIPCIONES

Artículo 44

Autoridades nacionales competentes con derecho de acceso a los datos del SIS

1. Las autoridades nacionales competentes tendrán acceso a los datos introducidos en el SIS y tendrán derecho a consultarlos directamente o en una copia de la base de datos del SIS, con los siguientes fines:

   a) los controles fronterizos, de conformidad con el Reglamento (UE) 2016/399;

   b) los controles policiales y aduaneros realizados en el Estado miembro de que se trate y la coordinación de dichos controles por las autoridades designadas;

   c) la prevención, la detección, la investigación o el enjuiciamiento de delitos de terrorismo u otros delitos graves o la ejecución de sanciones penales, dentro del Estado miembro de que se trate, siempre que se aplique la Directiva (UE) 2016/680;

d) el examen de las condiciones de entrada y estancia de nacionales de terceros países en el territorio de los Estados miembros, y la toma de decisiones sobre dicha entrada y estancia, en particular en lo que respecta a los permisos de residencia y los visados para estancia de larga duración, y de decisiones sobre el retorno de nacionales de terceros países, así como efectuar inspecciones de nacionales de terceros países que estén entrando o residiendo irregularmente en el territorio de los Estados miembros;

e) la realización de inspecciones de seguridad a nacionales de terceros países que soliciten protección internacional, en la medida en que las autoridades que las realicen no sean «autoridades decisorias» tal como se definen en el artículo 2, letra f), de la Directiva 2013/32/UE del Parlamento Europeo y del Consejo[1], y, en su caso, la prestación de asesoramiento de conformidad con el Reglamento (CE) n.º 377/2004 del Consejo[2].

2. El derecho de acceso a los datos del SIS y el derecho a consultarlos directamente podrán ser ejercidos por las autoridades nacionales competentes responsables de las naturalizaciones, según disponga el Derecho nacional, a los efectos de examinar las solicitudes de naturalización.

3. El derecho de acceso a los datos del SIS y el derecho a consultarlos directamente podrán ser ejercidos asimismo por las autoridades judiciales nacionales, incluidas las competentes para incoar el proceso penal y la instrucción judicial previa a la acusación de una persona, en el ejercicio de sus funciones, con arreglo a lo dispuesto en el Derecho nacional, así como por sus autoridades de coordinación.

---

[1] Directiva 2013/32/UE del Parlamento Europeo y del Consejo, 26 de junio de 2013, sobre procedimientos comunes para la concesión o la retirada de la protección internacional (DO L 180 de 29.6.2013, p. 60).

[2] Reglamento (CE) n.º 377/2004 del Consejo, de 19 de febrero de 2004, sobre la creación de una red de funcionarios de enlace de inmigración (DO L 64 de 2.3.2004, p. 1).

4. Las autoridades competentes a que se refiere el presente artículo se incluirán en la lista mencionada en el artículo 56, apartado 7.

Artículo 45

Servicios de matriculación de vehículos

1. Los servicios de los Estados miembros competentes para la expedición de los certificados de matriculación de vehículos, a que se refiere la Directiva 1999/37/CE del Consejo[1], tendrán acceso a los datos introducidos en el SIS de conformidad con el artículo 38, apartado 2, letras a), b), c), m) y p), del presente Reglamento con el único fin de comprobar si los vehículos y sus certificados de matriculación de vehículos y placas de matrícula presentados para su matriculación han sido robados, sustraídos, extraviados, se presentan como uno de estos documentos pero son falsos, o son requeridos como pruebas en un proceso penal.

   El acceso a los datos por parte de los servicios a los que se refiere el párrafo primero estará regulado por el Derecho nacional y se limitará al ámbito de competencias específico 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 del SIS.

[1] Directiva 1999/37/CE del Consejo, de 29 de abril de 1999, relativa a los documentos de matriculación de los vehículos (DO L 138 de 1.6.1999, p. 57).

3. Los servicios a los que se refiere el apartado 1 del presente artículo que no sean servicios públicos tendrán acceso a los datos del SIS solo a través de una de las autoridades a que se refiere el artículo 44. Dicha 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 estén obligados a respetar todas las limitaciones de utilización de los datos que la autoridad les comunique.

4. El artículo 39 no se aplicará al acceso al SIS 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 del presente artículo, de información obtenida mediante el acceso al SIS se regirá por el Derecho nacional.

Artículo 46

Servicios de registro de embarcaciones y aeronaves

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

a) datos sobre embarcaciones;

b) datos sobre motores de embarcaciones;

c) datos sobre aeronaves;

d) datos sobre motores de aeronaves.

El acceso a los datos por parte de los servicios a los que se refiere el párrafo primero estará regulado por el Derecho nacional y se limitará al ámbito de competencias específico 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 del SIS.

3. Los servicios a los que se refiere el apartado 1 del presente artículo que no sean servicios públicos tendrán acceso a los datos del SIS solo a través de una de las autoridades a que se refiere el artículo 44. 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 estén obligados a respetar todas las limitaciones de utilización de los datos que la autoridad les comunique.

4. El artículo 39 no se aplicará al acceso al SIS 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 del presente artículo, de información obtenida mediante el acceso al SIS se regirá por el Derecho nacional.

Artículo 47

Autoridades de registro de armas de fuego

1. Los servicios de los Estados miembros competentes para la expedición de certificados de registro de armas de fuego tendrán acceso a los datos sobre personas introducidas en el SIS de conformidad con los artículos 26 y 36 y a los datos sobre armas de fuego introducidas en el SIS de conformidad con el artículo 38, apartado 2. Este acceso se ejercerá con el fin de comprobar si la persona que solicita el registro está en búsqueda para su detención a efectos de entrega o extradición o a efectos de controles discretos, de investigación o específicos, o si las armas de fuego presentadas para su registro son buscadas con vistas a su incautación o requeridas como pruebas en un proceso penal.

2. El acceso a los datos por parte de los servicios a los que se refiere el apartado 1 estará regulado por el Derecho nacional y se limitará al ámbito de competencias específico de los servicios de que se trate.

3. Los servicios a los que se refiere el apartado 1 que sean servicios públicos tendrán derecho a acceder directamente a los datos del SIS.

4. Los servicios a los que se refiere el apartado 1 que sean servicios no gubernamentales tendrán acceso a los datos del SIS solo a través de una de las autoridades a que se refiere el artículo 44. Dicha autoridad tendrá derecho a acceder a los datos directamente y comunicará al servicio de que se trate si el arma de fuego puede ser registrada. El Estado miembro correspondiente velará por que el servicio en cuestión y sus empleados estén obligados a respetar todas las limitaciones de utilización de los datos que les comunique la autoridad que actúe como intermediaria.

5. El artículo 39 no se aplicará al acceso al SIS 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 del presente artículo, de información obtenida mediante el acceso al SIS se regirá por el Derecho nacional.

Artículo 48

Acceso de Europol a los datos del SIS

1. La Agencia de la Unión Europea para la Cooperación Policial (Europol), establecida por el Reglamento (UE) 2016/794, tendrá derecho, cuando sea necesario para cumplir su mandato, a acceder a los datos del SIS y a consultarlos. Europol también podrá intercambiar y solicitar información complementaria de conformidad con lo dispuesto en el Manual Sirene.

2. En caso de que una consulta efectuada por Europol revele la existencia de una descripción en el SIS, Europol informará al Estado miembro emisor mediante el intercambio de información complementaria a través de la infraestructura de comunicación y de conformidad con lo dispuesto en el Manual Sirene. Hasta que Europol esté en condiciones de utilizar las funciones previstas para el intercambio de información complementaria, Europol informará al Estado miembro emisor a través de los canales establecidos por el Reglamento (UE) 2016/794.

3. Europol podrá tratar la información complementaria que le proporcionen los Estados miembros para cotejarla con sus bases de datos y proyectos de análisis operativos, con el fin de detectar conexiones u otros vínculos pertinentes, y para llevar a cabo los análisis estratégicos, temáticos u operativos a los que se refiere el artículo 18, apartado 2, letras a), b) y c), del Reglamento (UE) 2016/794. Todo tratamiento de la información complementaria llevado a cabo por Europol a efectos del presente artículo se realizará de conformidad con lo dispuesto en dicho Reglamento.

4. El uso por parte de Europol de la información obtenida como consecuencia de una consulta del SIS o del tratamiento de información complementaria estará sujeto al consentimiento del Estado miembro emisor. 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 comunicar esa información a terceros países u organismos con el consentimiento del Estado miembro emisor y con pleno cumplimiento del Derecho de la Unión en materia de protección de datos.

5. Europol deberá:

a) sin perjuicio de lo dispuesto en los apartados 4 y 6, no conectar las partes del SIS a las que acceda ni transferir los datos contenidos en él a ningún sistema de recopilación y tratamiento de datos gestionado o alojado por Europol, ni descargar ni copiar de otra manera parte alguna del SIS;

b) no obstante lo dispuesto en el artículo 31, apartado 1, del Reglamento (UE) 2016/794, suprimir la información complementaria que contenga datos personales a más tardar un año después de que la descripción correspondiente haya sido suprimida. Como excepción, cuando Europol disponga de información en sus bases de datos o en proyectos de análisis operativos sobre un caso relacionado con la información complementaria, Europol, a título excepcional y a fin de desempeñar sus funciones, podrá seguir conservando la información complementaria cuando sea necesario. Europol informará al Estado miembro emisor y al Estado miembro de ejecución de la prolongación de la conservación de dicha información complementaria y la justificará;

c) limitar el acceso a los datos del SIS, incluida la información complementaria, al personal de Europol expresamente autorizado para ello que necesite acceso a esos datos para desempeñar sus funciones;

d) adoptar y aplicar medidas para garantizar la seguridad, la confidencialidad y el control interno, de conformidad con los artículos 10, 11 y 13;

e) garantizar que su personal autorizado para tratar los datos del SIS reciba la formación y la información adecuadas, de conformidad con el artículo 14, apartado 1; y

f) sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/794, permitir que el Supervisor Europeo de Protección de Datos supervise y examine las actividades que Europol realiza tanto en el ejercicio de su derecho a acceder a los datos del SIS y a consultarlos, como en el marco del intercambio y tratamiento de información complementaria.

6. Europol solo podrá copiar datos del SIS con fines técnicos cuando la copia sea necesaria para la consulta directa por el personal autorizado de Europol. El presente Reglamento será aplicable a esas copias. La copia técnica solo se utilizará para almacenar datos del SIS mientras se consultan dichos datos. Una vez que los datos hayan sido consultados, se suprimirán. Estos usos no se considerarán descargas o copias ilegales de datos del SIS. Europol no podrá copiar datos de las descripciones ni datos adicionales emitidos por Estados miembros o procedentes de la CS-SIS en otros sistemas de Europol.

7. A fin de verificar la legalidad del tratamiento de datos, de llevar a cabo un control interno y de garantizar la adecuada seguridad e integridad de los datos, Europol conservará un registro de cada acceso al SIS y de cada consulta en este, de conformidad con lo dispuesto en el artículo 12. Ese tipo de registros y de documentación no se considerarán copias o descargas ilegales de partes del SIS.

8. Los Estados miembros informarán a Europol mediante el intercambio de información complementaria de cualquier respuesta positiva para descripciones relacionadas con delitos de terrorismo. Con carácter excepcional, los Estados miembros podrán no informar a Europol si ello perjudicase investigaciones en curso o la seguridad de una persona o fuera contrario a los intereses esenciales de seguridad del Estado miembro emisor.

9. El apartado 8 será de aplicación a partir de la fecha en que Europol pueda recibir información complementaria de conformidad con el apartado 1.

Artículo 49

Acceso de Eurojust a los datos del SIS

1. Solo los miembros nacionales de Eurojust y sus asistentes tendrán derecho, cuando sea necesario para cumplir su mandato, a acceder a los datos del SIS y a consultarlos en el marco de su mandato, de conformidad con los artículos 26, 32, 34, 38 y 40.

2. En caso de que una consulta efectuada por un miembro nacional de Eurojust revele la existencia de una descripción en el SIS, dicho miembro nacional informará al Estado miembro emisor. Eurojust solo comunicará la información obtenida mediante dicha consulta a terceros países u organismos con el consentimiento del Estado miembro emisor y con pleno cumplimiento de lo dispuesto en el Derecho de la Unión en materia de protección de datos.

3. El presente artículo se entenderá sin perjuicio de las disposiciones del Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo[1+] y del Reglamento (UE) 2018/…[++] 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 los miembros nacionales de Eurojust o de sus asistentes, y de las potestades del Supervisor Europeo de Protección de Datos de conformidad con dichos Reglamentos.

4. A fin de verificar la legalidad del tratamiento de datos, de llevar a cabo un control interno y de garantizar la adecuada seguridad e integridad de los datos, Eurojust conservará un registro de cada acceso al SIS y de cada consulta en este que efectúe un miembro nacional de Eurojust o un asistente, de conformidad con lo dispuesto en el artículo 12.

5. Ninguna parte del SIS se conectará a ningún sistema de recopilación y tratamiento de datos gestionado o alojado por Eurojust, y los datos del SIS a los que los miembros nacionales o sus asistentes tengan acceso no se transferirán a dicho sistema. No se descargará ni copiará ninguna parte del SIS. El registro de los accesos y consultas no se considerará descarga o copia ilegal de datos del SIS.

6. Eurojust adoptará y aplicará medidas para garantizar la seguridad, la confidencialidad y el control interno de conformidad con los artículos 10, 11 y 13.

---

1 Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo, de …, sobre la Agencia Europea de Cooperación en materia de Justicia Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (DO L …).

\+ DO: insértese en el texto el número de serie del Reglamento que figura en el documento PE-CONS 37/18 y complétese en la nota a pie de página la referencia de publicación.

++ DO: insértese el número de serie del Reglamento que figura en el documento PE-CONS 31/18.

Artículo 50

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

1. De conformidad con el artículo 40, apartado 8, del Reglamento (UE) 2016/1624, los miembros de los equipos mencionados en el artículo 2, puntos 8 y 9, de dicho Reglamento, en el marco de su mandato y siempre que estén autorizados a llevar a cabo inspecciones de conformidad con lo dispuesto en el artículo 44, apartado 1, del presente Reglamento y hayan recibido la formación necesaria de conformidad con el artículo 14, apartado 1, del presente Reglamento, tendrán derecho a acceder a los datos del SIS y a consultarlos en la medida de lo necesario para el cumplimiento de sus funciones y siempre que lo exija el plan operativo de una operación específica. El acceso a los datos del SIS no se hará extensivo a ningún otro miembro del equipo.

2. Los miembros de los equipos mencionados en el apartado 1 ejercerán el derecho a acceder a los datos del SIS y a consultarlos de conformidad con el apartado 1 a través de una interfaz técnica. La Agencia Europea de la Guardia de Fronteras y Costas establecerá y mantendrá la interfaz técnica, la cual permitirá la conexión directa con el SIS Central.

3. En caso de que una consulta efectuada por un miembro de los equipos mencionados en el apartado 1 del presente artículo revele la existencia de una descripción en el SIS, se informará de ello al Estado miembro emisor. De conformidad con el artículo 40 del Reglamento (UE) 2016/1624, los miembros de los equipos solo actuarán en respuesta a una descripción del SIS siguiendo las instrucciones de los guardias de fronteras del Estado miembro de acogida en el que estén trabajando o del personal de este que participe en tareas relacionadas con el retorno y, como norma general, en su presencia. El Estado miembro de acogida podrá autorizar a los miembros de los equipos para que actúen en su nombre.

4. A fin de verificar la legalidad del tratamiento de datos, de llevar a cabo un control interno y de garantizar la adecuada seguridad e integridad de los datos, la Agencia Europea de la Guardia de Fronteras y Costas conservará un registro de cada acceso al SIS y de cada consulta en este, de conformidad con lo dispuesto en el artículo 12.

5. La Agencia Europea de la Guardia de Fronteras y Costas adoptará y aplicará medidas para garantizar la seguridad, la confidencialidad y el control interno, de conformidad con los artículos 10, 11 y 13, y se asegurará de que los equipos mencionados en el apartado 1 del presente artículo aplican dichas medidas.

6. Ninguna disposición del presente artículo podrá interpretarse en el sentido de que afecta a lo dispuesto en el Reglamento (UE) 2016/1624 por lo que respecta a la protección de datos o a la responsabilidad de la Agencia Europea de la Guardia de Fronteras y Costas por el tratamiento no autorizado o incorrecto de datos por su parte.

7. Sin perjuicio del apartado 2, ninguna parte del SIS se conectará a ningún sistema de recopilación y tratamiento de datos gestionado por los equipos mencionados en el apartado 1 o por la Agencia Europea de la Guardia de Fronteras y Costas, y los datos del SIS a los que dichos equipos tengan acceso no se transferirán a dicho sistema. No se descargará ni copiará ninguna parte del SIS. El registro de los accesos y consultas no se considerará descarga o copia ilegal de datos del SIS.

8. La Agencia Europea de la Guardia de Fronteras y Costas permitirá al Supervisor Europeo de Protección de Datos supervisar y examinar las actividades que realicen los equipos mencionados en el presente artículo en el ejercicio de su derecho a acceder a los datos del SIS y a consultarlos. La presente disposición se entenderá sin perjuicio de las demás disposiciones del Reglamento (UE) 2018/…[+].

[+] DO: insértese el número de serie del Reglamento que figura en el documento PE-CONS 31/18.

Artículo 51

Evaluación de la utilización del SIS por parte de Europol, de Eurojust y de la Agencia Europea de la Guardia de Fronteras y Costas*

1. La Comisión llevará a cabo al menos cada cinco años una evaluación del funcionamiento y la utilización del SIS por parte de Europol, de los miembros nacionales de Eurojust y sus asistentes, y de los equipos mencionados en el artículo 50, apartado 1.

2. Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas garantizarán un seguimiento adecuado de las conclusiones y recomendaciones derivadas de la evaluación.

3. Se enviará al Parlamento Europeo y al Consejo un informe sobre los resultados de la evaluación y las consiguientes medidas.

Artículo 52

Alcance del acceso

Los usuarios finales, incluidos Europol, los miembros nacionales de Eurojust y sus asistentes y los miembros de los equipos mencionados en el artículo 2, puntos 8 y 9, del Reglamento (UE) 2016/1624, solo podrán acceder a los datos que requieran para el desempeño de sus funciones.

Artículo 53

Plazo de revisión de las descripciones sobre personas

1. Las descripciones sobre personas se conservarán solo durante el tiempo necesario para alcanzar los fines para los que hayan sido introducidas.

2. Todo Estado miembro podrá introducir una descripción sobre una persona a efectos del artículo 26 y del artículo 32, apartado 1, letras a) y b), por un período de cinco años. El Estado miembro emisor revisará, en ese plazo de cinco años, la necesidad de conservar la descripción.

3. Todo Estado miembro podrá introducir una descripción sobre una persona a efectos de los artículos 34 y 40 por un período de tres años. El Estado miembro emisor revisará, en ese plazo de tres años, la necesidad de conservar la descripción.

4. Todo Estado miembro podrá introducir una descripción sobre una persona a efectos del artículo 32, apartado 1, letras c), d) y e), y del artículo 36 por un período de un año. El Estado miembro emisor revisará, en ese plazo de un año, la necesidad de conservar la descripción.

5. Cada Estado miembro fijará, cuando corresponda, plazos de revisión más cortos con arreglo al Derecho nacional.

6. Durante el plazo de revisión a que se hace referencia en los apartados 2, 3 y 4, el Estado miembro emisor podrá decidir, tras una evaluación completa del caso concreto, de la que deberá quedar constancia, que se conserve la descripción sobre una persona durante un período de tiempo más largo que el de revisión, cuando ello sea necesario y proporcionado para los fines que motivaron la introducción de la descripción. En estos casos, el apartado 2, 3 o 4 también se aplicará a la prórroga. Toda prórroga será comunicada a la CS-SIS.

7. Las descripciones sobre personas se suprimirán automáticamente una vez que expire el plazo de revisión a que se refieren los apartados 2, 3 y 4, excepto cuando el Estado miembro emisor haya comunicado la prórroga a la CS-SIS con arreglo al apartado 6. La CS-SIS informará automáticamente al Estado miembro emisor acerca de la supresión programada de los datos, con una antelación de cuatro meses.

8. Los Estados miembros llevarán estadísticas del número de descripciones sobre personas cuyos plazos de conservación hayan sido prorrogados con arreglo al apartado 6 del presente artículo y las transmitirán, previa solicitud, a las autoridades de control mencionadas en el artículo 69.

9. Desde el momento en que una oficina Sirene tenga constancia de que una descripción sobre una persona ha cumplido su objetivo y, por consiguiente, debe suprimirse, lo notificará inmediatamente a la autoridad que haya creado la descripción. La autoridad dispondrá de quince días naturales desde la recepción de esa notificación para indicar que la descripción se ha suprimido o se suprimirá, o para justificar su conservación. Si no se recibiese ninguna respuesta antes de expirar el plazo de quince días, la oficina Sirene se asegurará de que se suprima la descripción. Siempre que el Derecho nacional lo permita, la oficina Sirene suprimirá la descripción. Las oficinas Sirene comunicarán a sus respectivas autoridades de control todo problema recurrente que detecten cuando actúen con arreglo al presente apartado.

Artículo 54

Plazo de revisión de las descripciones sobre objetos

1. Las descripciones sobre objetos se conservarán solo durante el tiempo necesario para alcanzar los fines para los que hayan sido introducidas.

2. Todo Estado miembro podrá introducir una descripción sobre objetos a efectos de los artículos 36 y 38 por un período de diez años. El Estado miembro emisor revisará, en ese plazo de diez años, la necesidad de conservar la descripción.

3. Las descripciones sobre objetos introducidas con arreglo a los artículos 26, 32, 34 y 36 se revisarán con arreglo al artículo 53 cuando estén relacionadas con una descripción sobre una persona. Dichas descripciones se conservarán únicamente mientras se conserve la descripción sobre la persona.

4. Durante el plazo de revisión a que se hace referencia en los apartados 2 y 3, el Estado miembro emisor podrá decidir que se conserve una descripción sobre un objeto durante un período de tiempo más largo que el de revisión, cuando ello sea necesario para los fines que motivaron la introducción de la descripción. En estos casos, se aplicarán los apartados 2 o 3, según el caso.

5. La Comisión podrá adoptar actos de ejecución para fijar plazos de revisión más cortos para determinadas categorías de descripciones sobre objetos. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

6. Los Estados miembros llevarán estadísticas del número de descripciones sobre objetos cuyos plazos de conservación hayan sido prorrogados con arreglo al apartado 4.

CAPÍTULO XIV
SUPRESIÓN DE LAS DESCRIPCIONES

Artículo 55

Supresión de descripciones

1. Las descripciones para la detención a efectos de entrega o extradición con arreglo al artículo 26 se suprimirán cuando la persona haya sido entregada o extraditada a las autoridades competentes del Estado miembro emisor. También se suprimirán cuando la resolución judicial en la que se basó la descripción haya sido revocada por la autoridad judicial competente con arreglo al Derecho nacional. También se suprimirán una vez que alcancen la fecha de expiración de la descripción de acuerdo con el artículo 53.

2. Las descripciones sobre personas desaparecidas o personas vulnerables a quienes se debe impedir viajar con arreglo al artículo 32 se suprimirán de conformidad con las siguientes normas:

   a) en lo relativo a los menores desaparecidos y a los menores en riesgo de sustracción, la descripción se suprimirá:

      i) en cuanto se resuelva el asunto, por ejemplo, cuando el menor haya sido localizado o repatriado o las autoridades competentes del Estado miembro de ejecución adopten una resolución sobre su custodia;

      ii) en cuanto expire la descripción de conformidad con el artículo 53; o

      iii) en cuanto la autoridad competente del Estado miembro emisor adopte una decisión;

b) en lo relativo a los adultos desaparecidos respecto de los cuales no se pidan medidas de protección, la descripción se suprimirá:

i) en cuanto se haya ejecutado la medida que deba adoptarse, cuando el Estado miembro de ejecución determine su paradero;

ii) en cuanto expire la descripción de conformidad con el artículo 53; o

iii) en cuanto la autoridad competente del Estado miembro emisor adopte una decisión;

c) en lo relativo a adultos desaparecidos respecto de los cuales se pidan medidas de protección, la descripción se suprimirá:

i) en cuanto se haya ejecutado la medida que deba adoptarse, cuando se preste protección a la persona;

ii) en cuanto expire la descripción de conformidad con el artículo 53; o

iii) en cuanto la autoridad competente del Estado miembro emisor adopte una decisión;

d) en lo relativo a personas vulnerables mayores de edad a quienes se deba impedir viajar por su propia seguridad, y a los menores a los que se deba impedir viajar, la descripción se suprimirá:

i) en cuanto se haya ejecutado la medida que deba adoptarse, por ejemplo, prestar protección a la persona;

ii) en cuanto expire la descripción de conformidad con el artículo 53; o

iii) en cuanto la autoridad competente del Estado miembro emisor adopte una decisión.

Sin perjuicio del Derecho nacional, cuando una persona haya sido internada por resolución de una autoridad competente, la descripción podrá conservarse hasta que la persona haya sido repatriada.

3. Las descripciones sobre personas en búsqueda a efectos de un procedimiento judicial con arreglo al artículo 34 se suprimirán:

a) en cuanto se haya comunicado el paradero de la persona a la autoridad competente del Estado miembro emisor;

b) en cuanto expire la descripción de conformidad con el artículo 53; o

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

Si la información contenida en la comunicación a que se refiere la letra a) no permitiera la adopción de medidas, la oficina Sirene del Estado miembro emisor informará a la oficina Sirene del Estado miembro de ejecución con el fin de resolver el problema.

En el supuesto de obtenerse una respuesta positiva en la que los datos del domicilio se hayan enviado al Estado miembro emisor y que en el mismo Estado miembro de ejecución se obtenga con posterioridad una respuesta positiva con los mismos datos del domicilio, el Estado miembro de ejecución conservará un registro de la respuesta positiva pero no volverá a enviar al Estado miembro emisor ni los datos del domicilio ni la información complementaria. En estos casos, el Estado miembro de ejecución informará al Estado miembro emisor acerca de la repetición de la respuesta positiva, y el Estado miembro emisor llevará a cabo una evaluación completa del caso concreto a fin de determinar la necesidad de conservar la descripción.

4. Las descripciones sobre controles discretos, de investigación y específicos con arreglo al artículo 36, se suprimirán:

a) en cuanto expire la descripción de conformidad con el artículo 53; o

b) en cuanto la autoridad competente del Estado miembro emisor así lo decida.

5. Las descripciones sobre objetos para su incautación o utilización como pruebas en un proceso penal con arreglo al artículo 38, se suprimirán:

a) en cuanto se produzca la incautación del objeto o se ejecute una medida equivalente, una vez que se haya producido el necesario intercambio de información complementaria de seguimiento entre las oficinas Sirene correspondientes o que el objeto haya quedado sujeto a otro procedimiento administrativo o judicial;

b) en cuanto expire la descripción de conformidad con el artículo 53; o

c) en cuanto la autoridad competente del Estado miembro emisor así lo decida.

6. Las descripciones sobre personas desconocidas en búsqueda con arreglo al artículo 40 se suprimirán:

a) en cuanto se haya identificado a la persona;

b) en cuanto expire la descripción de conformidad con el artículo 53; o

c) en cuanto la autoridad competente del Estado miembro emisor así lo decida.

7. Las descripciones sobre objetos introducidas con arreglo a los artículos 26, 32, 34 y 36 que estén relacionadas con una descripción sobre una persona se suprimirán cuando se suprima la descripción sobre la persona con arreglo al presente artículo.

CAPÍTULO XV
NORMAS GENERALES DE TRATAMIENTO DE DATOS

Artículo 56

Tratamiento de los datos del SIS

1. Los Estados miembros solo podrán tratar los datos enumerados en el artículo 20 a los efectos 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 copiarse con fines técnicos, cuando sea necesario para la consulta directa por las autoridades competentes mencionadas en el artículo 44. El presente Reglamento se aplicará a esas copias. Los Estados miembros no podrán copiar los datos de una descripción o datos adicionales introducidos por otro Estado miembro desde su N.SIS o la CS-SIS en 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 durante 48 horas como máximo.

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

4. El acceso a los datos del SIS por las autoridades nacionales competentes mencionadas en el artículo 44 solo se autorizará dentro de los límites de sus competencias y únicamente al personal debidamente autorizado.

5. Por lo que respecta a las descripciones previstas en los artículos 26, 32, 34, 36, 38 y 40 del presente Reglamento, todo tratamiento de información del SIS con fines distintos de aquellos para los que la descripción se introdujo en el SIS deberá guardar relación con algún caso concreto y estar justificado por la necesidad de prevenir una amenaza grave e inminente para el orden y la seguridad públicos, por razones graves de seguridad nacional o por la necesidad de prevenir un delito grave. A tal fin, deberá obtenerse autorización previa del Estado miembro emisor.

6. Toda utilización de datos del SIS que no cumpla lo dispuesto en los apartados 1 a 5 del presente artículo se considerará una desviación de la finalidad con arreglo al Derecho nacional de cada Estado miembro y estará sujeta a sanciones de conformidad con el artículo 73.

7. Cada Estado miembro remitirá a eu-LISA la lista de las autoridades competentes que estén autorizadas a consultar directamente los datos del SIS con arreglo al presente Reglamento, así como cualquier modificación introducida en ella. La lista indicará, para cada autoridad, los datos que puede consultar y para qué fines. Eu-LISA garantizará la publicación anual de la lista en el *Diario Oficial de la Unión Europea*. Eu-LISA mantendrá una lista constantemente actualizada en su página web, con los cambios enviados por los Estados miembros entre las publicaciones anuales.

8. En la medida en que el Derecho de la Unión no establezca disposiciones especiales, la normativa de cada Estado miembro se aplicará a los datos de sus N.SIS.

Artículo 57

Datos del SIS y ficheros nacionales

1. El artículo 56, apartado 2, se entenderá sin perjuicio del derecho de cada Estado miembro a conservar en sus ficheros nacionales datos del SIS en relación con los cuales se hayan tomado medidas en su territorio. Dichos datos se conservarán en los ficheros nacionales durante un período máximo de tres años, salvo si la normativa nacional contiene disposiciones específicas que prevean un plazo de conservación más largo.

2. El artículo 56, apartado 2, se entenderá sin perjuicio del derecho de cada Estado miembro a conservar en sus ficheros nacionales los datos contenidos en una descripción concreta que dicho Estado miembro haya introducido en el SIS.

Artículo 58

Información en caso de no ejecución de una descripción

Si no fuera posible ejecutar una medida requerida, el Estado miembro al que se pide actuar informará de ello inmediatamente al Estado miembro emisor mediante el intercambio de información complementaria.

Artículo 59

Calidad de los datos del SIS

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

2. Cuando un Estado miembro emisor reciba datos adicionales o modificados pertinentes de los enumerados en el artículo 20, apartado 3, completará o modificará sin demora la descripción de que se trate.

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

4. Si un Estado miembro distinto del Estado miembro emisor dispone de datos adicionales o modificados pertinentes de los enumerados en el artículo 20, apartado 3, los transmitirá sin demora, mediante el intercambio de información complementaria, al Estado miembro emisor para que este último pueda completar o modificar la descripción. Si los datos adicionales o modificados se refieren a personas solo se transmitirán si se ha determinado la identidad de la persona.

5. Si un Estado miembro distinto del Estado miembro emisor dispone de indicios que permitan presumir que un dato contiene errores de hecho o que ha sido almacenado ilegalmente, informará, mediante el intercambio de información complementaria, al Estado miembro emisor en cuanto sea posible y, a más tardar, dos días laborables después de haber tenido conocimiento de dichos indicios. El Estado miembro emisor comprobará la información y, en caso necesario, corregirá o suprimirá ese dato sin demora.

6. Si los Estados miembros no pudieran llegar a un acuerdo en el plazo de dos meses a partir del momento en que se tuvo conocimiento de los indicios a que se refiere el apartado 5 del presente artículo, el Estado miembro que no ha introducido la descripción someterá el asunto a las autoridades de control competentes y al Supervisor Europeo de Protección de Datos para que adopten una decisión, recurriendo a la cooperación con arreglo al artículo 71.

7. Los Estados miembros intercambiarán información complementaria cuando una persona alegue que no es la persona objeto de la descripción. Si de la comprobación se desprende que la persona objeto de la descripción no es la persona que hace la alegación, se informará a quien la hace de las medidas establecidas en el artículo 62 y del derecho de recurso con arreglo al artículo 68, apartado 1.

Artículo 60

Incidentes de seguridad

1. Cualquier acontecimiento que repercuta o pueda repercutir en la seguridad del SIS o pueda causar daños o pérdidas de datos del SIS o de información complementaria será considerado un incidente de seguridad, especialmente cuando se haya podido producir un acceso ilegal a los datos o cuando se haya puesto o se haya podido poner en peligro la disponibilidad, integridad y confidencialidad de estos.

2. Los incidentes de seguridad se gestionarán de tal modo que se garantice una respuesta rápida, efectiva y adecuada.

3. Sin perjuicio de la notificación y comunicación de cualquier violación de la seguridad de los datos personales de conformidad con el artículo 33 del Reglamento (UE) 2016/679 o con el artículo 30 de la Directiva (UE) 2016/680, los Estados miembros, Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas notificarán sin demora a la Comisión, a eu-LISA, a la autoridad de control competente y al Supervisor Europeo de Protección de Datos los incidentes de seguridad que se produzcan. Eu-LISA comunicará sin demora a la Comisión y al Supervisor Europeo de Protección de Datos cualquier incidente de seguridad relativo al SIS Central.

4. La información sobre un incidente de seguridad que repercuta o pueda repercutir en el funcionamiento del SIS en un Estado miembro o en eu-LISA, en la disponibilidad, integridad y confidencialidad de los datos introducidos o enviados por otros Estados miembros o en la información complementaria intercambiada se transmitirá sin demora a todos los Estados miembros y se comunicará de conformidad con el plan de gestión de incidentes establecido por eu-LISA.

5. Los Estados miembros y eu-LISA colaborarán cuando se produzca un incidente de seguridad.

6. La Comisión informará de inmediato al Parlamento Europeo y al Consejo sobre los incidentes graves. Se asignará a esos informes la clasificación EU RESTRICTED/RESTREINT UE de conformidad con las normas de seguridad aplicables.

7. Cuando un incidente de seguridad se deba a la utilización indebida de datos, los Estados miembros, Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas velarán por que se impongan sanciones de conformidad con el artículo 73.

Artículo 61

Distinción entre personas con características similares

1. Cuando, al introducirse una nueva descripción, se ponga de manifiesto que ya existe una descripción en el SIS sobre una persona con las mismas características identificativas, la oficina Sirene se pondrá en contacto, en un plazo de doce horas, con el Estado miembro emisor mediante el intercambio de información complementaria para comprobar si los sujetos de las dos descripciones son la misma persona.

2. Si al cotejar las descripciones resulta que la persona objeto de la nueva descripción y la persona objeto de la descripción ya introducida en el SIS son efectivamente la misma persona, la oficina Sirene aplicará el procedimiento de introducción de descripciones múltiples previsto en el artículo 23.

3. Si el resultado del cotejo indicase que las descripciones se refieren de hecho a dos personas diferentes, la oficina Sirene aprobará la solicitud de introducción de la segunda descripción añadiendo los datos necesarios para evitar cualquier error de identificación.

Artículo 62

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 añadir, con el consentimiento expreso de esta última, datos sobre ella a la descripción, a fin de evitar las consecuencias negativas de los errores de identificación. Cualquier persona cuya identidad haya sido usurpada tendrá derecho a revocar su consentimiento en relación con el tratamiento de los datos personales añadidos.

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

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

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

3. A efectos del presente artículo y a reserva del consentimiento expreso de la persona cuya identidad haya sido usurpada para cada categoría de datos, solo podrán introducirse y tratarse en el SIS los siguientes datos personales de la persona cuya identidad haya sido usurpada:

   a) apellidos;

   b) nombres;

c) nombres y apellidos de nacimiento;

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

e) rasgos físicos particulares, objetivos e inalterables;

f) lugar de nacimiento;

g) fecha de nacimiento;

h) sexo;

i) fotografías e imágenes faciales;

j) impresiones dactilares, palmares o ambas;

k) nacionalidad o nacionalidades;

l) categoría de los documentos de identificación de la persona;

m) país de expedición de los documentos de identificación de la persona;

n) número o números de los documentos de identificación de la persona;

o) fecha de expedición de los documentos de identificación de la persona;

p) dirección de la persona;

q) nombre del padre de la persona;

r) nombre de la madre de la persona.

4. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas técnicas necesarias para la introducción y el ulterior tratamiento de los datos a los que se hace referencia en el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, 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 63

Conexiones entre descripciones

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

2. La creación de una conexión no afectará a la medida específica que deba tomarse en virtud de cada una de las descripciones conectadas, ni al período de revisión de cada una de las descripciones conectadas.

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

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

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

6. La Comisión adoptará actos de ejecución a fin de establecer y desarrollar las normas técnicas necesarias para la conexión entre descripciones. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 64

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, a fin de apoyar el intercambio de información complementaria.

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

3. El apartado 2 se entenderá sin perjuicio del derecho de cada Estado miembro a conservar en sus ficheros nacionales datos relativos a una descripción concreta que haya introducido o a una descripción en relación con la cual se hayan tomado medidas en su territorio. El período durante el que podrán conservarse dichos datos en esos ficheros se regirá por el Derecho nacional.

Artículo 65

Transferencia de datos personales a terceros

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

CAPÍTULO XVI
PROTECCIÓN DE DATOS

Artículo 66

Legislación aplicable

1. El Reglamento (UE) 2018/…[+] será aplicable al tratamiento de datos personales por eu-LISA, por la Agencia Europea de la Guardia de Fronteras y Costas, y por Eurojust realizado en el marco del presente Reglamento. El Reglamento (UE) 2016/794 será aplicable al tratamiento de datos personales realizado por Europol en el marco del presente Reglamento.

2. La Directiva (UE) 2016/680 será aplicable al tratamiento de datos personales con arreglo al presente Reglamento por las autoridades y servicios nacionales competentes para fines de prevención, detección, investigación o enjuiciamiento de delitos, o de ejecución de sanciones penales, incluida la protección frente a amenazas para la seguridad pública y la prevención de estas.

[+] DO: insértese el número de serie del Reglamento que figura en el documento PE-CONS 31/18.

3. El Reglamento (UE) 2016/679 será aplicable al tratamiento de datos personales realizado en el marco del presente Reglamento por las autoridades y servicios nacionales competentes, excepto el tratamiento para fines de prevención, detección, investigación o enjuiciamiento de delitos, o de ejecución de sanciones penales, incluida la protección frente a amenazas para la seguridad pública y la prevención de estas.

Artículo 67

Derecho de acceso, rectificación de datos que contengan errores y supresión de datos almacenados ilegalmente

1. Los interesados podrán ejercer los derechos que les asisten en virtud de los artículos 15, 16 y 17 del Reglamento (UE) 2016/679 y del artículo 14 y artículo 16, apartados 1 y 2, de la Directiva (UE) 2016/680.

2. Un Estado miembro que no sea el Estado miembro emisor podrá facilitar al interesado información relativa a cualquiera de los datos personales del interesado que estén siendo tratados, únicamente si ha dado antes al Estado miembro emisor ocasión de pronunciarse al respecto. La comunicación entre esos Estados miembros tendrá lugar mediante el intercambio de información complementaria.

3. Los Estados miembros tomarán, de conformidad con el Derecho nacional, la decisión de no facilitar la información al interesado, en su totalidad o en parte, en la medida en que dicha limitación total o parcial sea una medida necesaria y proporcionada en una sociedad democrática, y la mantendrán mientras siga siéndolo, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos del interesado, con el fin de:

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

b) no comprometer la prevención, detección, investigación o enjuiciamiento de delitos o la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional; o

e) proteger los derechos y libertades de otras personas.

En los casos enumerados en el párrafo primero, el Estado miembro informará al interesado por escrito, sin dilaciones indebidas, de cualquier denegación o restricción del acceso y de los motivos de la denegación o restricción. Esta información podrá omitirse si su comunicación puede comprometer alguno de los motivos enumerados en las letras a) a e) del párrafo primero. El Estado miembro informará al interesado de las posibilidades de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.

El Estado miembro documentará los fundamentos de hecho o de Derecho en los que se base la decisión de no facilitar la información al interesado. Dicha información se pondrá a la disposición de las autoridades de control.

En estos casos, el interesado también podrá ejercer sus derechos a través de las autoridades de control competentes.

4. Tras ser presentada una solicitud de acceso, rectificación o supresión, el Estado miembro informará al interesado lo antes posible y, en todo caso, dentro de los plazos a que se refiere el artículo 12, apartado 3, del Reglamento (UE) 2016/679, del curso dado al ejercicio de los derechos que le confiere el presente artículo.

Artículo 68

Vías de recurso

1. Sin perjuicio de las disposiciones sobre vías de recurso del Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680, toda persona podrá emprender acciones ante cualquier autoridad competente, incluidos los órganos jurisdiccionales, en virtud de la normativa de cualquier Estado miembro, para acceder a información o para 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 del artículo 72.

3. Los Estados miembros presentarán al Comité Europeo de Protección de Datos 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 de control y el número de casos en que se haya concedido el acceso a los datos;

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

   d) el número de solicitudes de rectificación de datos inexactos y de supresión de datos almacenados ilegalmente presentadas a la autoridad de control;

e) el número de procedimientos judiciales iniciados;

f) el número de casos en los que el órgano jurisdiccional haya fallado a favor del demandante;

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

La Comisión elaborará una plantilla para presentar los informes mencionados en el presente apartado.

4. Los informes de los Estados miembros se incluirán en el informe conjunto al que se refiere el artículo 71, apartado 4.

Artículo 69

Supervisión de los N.SIS

1. Los Estados miembros velarán por que las autoridades de control independientes designadas en cada Estado miembro y dotadas de las potestades mencionadas en el capítulo VI del Reglamento (UE) 2016/679 o en el capítulo VI de la Directiva (UE) 2016/680 supervisen la legalidad del tratamiento de datos personales del SIS en su territorio, su transmisión a partir de él y el intercambio y posterior tratamiento de información complementaria en su territorio.

2. Las autoridades de control velarán por que se lleve a cabo una auditoría de las operaciones de tratamiento de datos en los N.SIS de acuerdo con las normas internacionales de auditoría, al menos cada cuatro años. La auditoría será realizada por las autoridades de control o bien encargada directamente por estas a un auditor independiente especializado en protección de datos. Las autoridades de control se encargarán en todo momento de la supervisión del auditor independiente y serán responsables de su labor.

3. Los Estados miembros velarán por que sus autoridades de control dispongan de medios suficientes para desempeñar las funciones que les encomienda el presente Reglamento y tengan acceso al asesoramiento de personas con conocimientos suficientes sobre datos biométricos.

Artículo 70

Supervisión de eu-LISA

1. El Supervisor Europeo de Protección de Datos será responsable de supervisar el tratamiento de datos personales por parte de eu-LISA y de asegurarse de que se lleve a cabo conforme al presente Reglamento. En consecuencia, serán de aplicación las disposiciones sobre funciones y competencias previstas en los artículos 57 y 58 del Reglamento (UE) 2018/…[+].

2. Al menos cada cuatro años, el Supervisor Europeo de Protección de Datos llevará a cabo una auditoría del tratamiento de datos personales por parte de eu-LISA siguiendo normas de auditoría internacionales. Se enviará un informe sobre esta auditoría al Parlamento Europeo, al Consejo, a eu-LISA, a la Comisión y a las autoridades de control. Deberá darse a eu-LISA la ocasión de formular observaciones antes de que se adopte el informe.

[+] DO: insértese el número de serie del Reglamento que figura en el documento PE-CONS 31/18.

Artículo 71

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

1. Las autoridades de control y el Supervisor Europeo de Protección de Datos, dentro de sus respectivos ámbitos de competencia, cooperarán activamente en el ejercicio de sus responsabilidades y garantizarán una supervisión coordinada del SIS.

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

3. A efectos de lo dispuesto en el apartado 2, las autoridades de control y el Supervisor Europeo de Protección de Datos se reunirán al menos dos veces al año en el marco del Comité Europeo de Protección de Datos. Los gastos y la organización de las reuniones correrán a cargo del Comité Europeo de Protección de Datos. El reglamento interno se adoptará en la primera reunión. Los métodos de trabajo se irán precisando conjuntamente en función de las necesidades.

4. El Comité Europeo de Protección de Datos enviará anualmente al Parlamento Europeo, al Consejo y a la Comisión un informe conjunto de actividades en lo que respecta a la supervisión coordinada.

CAPÍTULO XVII
RESPONSABILIDAD Y SANCIONES

Artículo 72

Responsabilidad

1. Sin perjuicio del derecho a indemnización y de la exigencia de responsabilidad con arreglo al Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/…[+]:

   a) cualquier persona o Estado miembro que haya sufrido daños o perjuicios materiales o inmateriales, como resultado de una operación ilegal de tratamiento de datos personales mediante la utilización del N.SIS o de cualquier otro acto incompatible con el presente Reglamento por parte de un Estado miembro, tendrá derecho a recibir una indemnización de dicho Estado miembro; y

   b) cualquier persona o Estado miembro que haya sufrido daños o perjuicios materiales o inmateriales como resultado de cualquier acto de eu-LISA incompatible con el presente Reglamento tendrá derecho a recibir una indemnización de eu-LISA;

   El Estado miembro o eu-LISA quedarán exentos, total o parcialmente, de responsabilidad de acuerdo con el párrafo primero, si demuestran que no son responsables del hecho que causó los daños y perjuicios.

[+] DO: insértese el número de serie del Reglamento que figura en el documento PE-CONS 31/18.

2. Si el incumplimiento por un Estado miembro de las obligaciones que le impone el presente Reglamento causa daños y perjuicios al SIS, dicho Estado miembro será considerado responsable de ellos, salvo y en la medida en que eu-LISA u otro Estado miembro participante en el SIS no haya adoptado medidas razonables para impedir que se produjeran dichos daños y perjuicios o para minimizar sus efectos.

3. Las reclamaciones de indemnización contra un Estado miembro por los daños y perjuicios a que se refieren los apartados 1 y 2 se regirán por el Derecho nacional de dicho Estado miembro. Las reclamaciones de indemnización contra eu-LISA por los daños y perjuicios a que se refieren los apartados 1 y 2 estarán sujetas a las condiciones previstas en los Tratados.

Artículo 73

Sanciones

Los Estados miembros garantizarán que toda utilización indebida de los datos del SIS y todo tratamiento de estos o intercambio de información complementaria que sean contrarios a lo dispuesto en el presente Reglamento se sancionen con arreglo al Derecho nacional.

Las sanciones así establecidas serán efectivas, proporcionadas y disuasorias.

CAPÍTULO XVIII
DISPOSICIONES FINALES

Artículo 74

Seguimiento y estadísticas

1. Eu-LISA garantizará que se establezcan procedimientos para el seguimiento del funcionamiento del SIS en relación con los objetivos, los resultados, la relación coste-eficacia, la seguridad y la calidad del servicio.

2. A efectos de mantenimiento técnico, elaboración de informes, elaboración de informes sobre calidad de los datos y estadísticas, eu-LISA tendrá acceso a la información necesaria relacionada con las operaciones de tratamiento que se realizan en el SIS Central.

3. Eu-LISA elaborará estadísticas diarias, mensuales y anuales que muestren el número de inscripciones por categoría de descripción, tanto para cada Estado miembro como agregadas. Eu-LISA también elaborará informes anuales que muestren el número de respuestas positivas anuales por categoría de descripción, el número de ocasiones en que se ha consultado el SIS y el número de ocasiones en que se ha accedido al SIS para introducir, actualizar o suprimir una descripción, tanto para cada Estado miembro como en número agregado. Las estadísticas no contendrán datos personales. El informe estadístico anual se publicará.

4. Los Estados miembros, Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas, facilitarán a eu-LISA y a la Comisión la información necesaria para elaborar los informes a que se refieren los apartados 3, 6, 8 y 9.

5. Esta información incluirá estadísticas separadas sobre el número de consultas realizadas por (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 (incluidos los motores de aeronaves) y armas de fuego. Las estadísticas también indicarán el número de respuestas positivas por categoría de descripción.

6. Eu-LISA facilitará al Parlamento Europeo, el Consejo, los Estados miembros, la Comisión, Europol, Eurojust, la Agencia Europea de la Guardia de Fronteras y Costas y el Supervisor Europeo de Protección de Datos los informes estadísticos que elabore.

Con el fin de controlar la aplicación de los actos jurídicos de la Unión, también a los efectos del Reglamento (UE) n.º 1053/2013, la Comisión podrá solicitar que eu-LISA elabore informes estadísticos específicos adicionales, ya sea de forma periódica o ad hoc, sobre el funcionamiento del SIS, la utilización del SIS y el intercambio de información complementaria.

La Agencia Europea de la Guardia de Fronteras y Costas podrá solicitar que eu-LISA elabore informes estadísticos específicos adicionales para realizar los análisis de riesgos y las evaluaciones de la vulnerabilidad a que se refieren los artículos 11 y 13 del Reglamento (UE) 2016/1624, ya sea de forma periódica o ad hoc.

7. A efectos del artículo 15, apartado 4, y de los apartados 3, 4 y 6 del presente artículo, eu-LISA establecerá, pondrá en funcionamiento y alojará en sus centros técnicos un repositorio central que contenga los datos a que se refieren el artículo 15, apartado 4, y el apartado 3 del presente artículo, el cual no permitirá la identificación de las personas pero sí permitirá a la Comisión y a las agencias a que se refiere el apartado 6 del presente artículo obtener los mencionados informes y estadísticas. Previa solicitud, eu-LISA dará acceso al repositorio central a los Estados miembros y la Comisión, así como a Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas, en la medida en que sea necesario para el desempeño de sus funciones, por medio de un acceso seguro a través de la infraestructura de comunicación. Eu-LISA realizará controles de acceso y perfiles de usuario específicos con el fin de garantizar que únicamente se acceda al repositorio central a efectos de la presentación de informes y estadísticas.

8. Transcurridos dos años desde la fecha de aplicación del presente Reglamento de conformidad con el artículo 79, apartado 5, párrafo primero, y a continuación cada dos años, eu-LISA presentará al Parlamento Europeo y al Consejo un informe sobre el funcionamiento técnico del SIS Central y de la infraestructura de comunicación, incluida la seguridad de ambos, sobre el SAID y sobre el intercambio bilateral y multilateral de información complementaria entre los Estados miembros. Dicho informe también incluirá, una vez que la tecnología esté en uso, una evaluación de la utilización de imágenes faciales para identificar a personas.

9. Transcurridos tres años desde la fecha de aplicación del presente Reglamento de conformidad con el artículo 79, apartado 5, párrafo primero, y a continuación cada cuatro años, la Comisión efectuará una evaluación global del SIS Central y del intercambio bilateral y multilateral de información complementaria entre los Estados miembros. Esta evaluación global incluirá un examen de los resultados obtenidos en relación con los objetivos y una valoración de los principios básicos, para determinar si siguen siendo válidos, de la aplicación del presente Reglamento con respecto al SIS Central y de la seguridad del SIS Central, con un análisis de sus consecuencias para futuras operaciones. El informe de evaluación incluirá también una valoración del SAID y las campañas de información sobre el SIS efectuadas por la Comisión de conformidad con el artículo 19.

La Comisión transmitirá el informe de evaluación al Parlamento Europeo y al Consejo.

10. La Comisión adoptará actos de ejecución para desarrollar en detalle las normas sobre el funcionamiento del repositorio central a que se refiere el apartado 7 del presente artículo y las normas de protección de datos y seguridad aplicables al repositorio. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 76, apartado 2.

Artículo 75

Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar actos delegados mencionados en el artículo 38, apartado 3, y en el artículo 43, apartado 4, se otorgan a la Comisión por un período de tiempo indefinido a partir del … [fecha de entrada en vigor del presente Reglamento].

3. La delegación de poderes mencionada en el artículo 38, apartado 3, y en el artículo 43, apartado 4, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 38, apartado 3, o del artículo 43, apartado 4, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 76

Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 77

Modificaciones de la Decisión 2007/533/JAI

La Decisión 2007/533/JAI se modifica como sigue:

1) El artículo 6 se sustituye por el texto siguiente:

«Artículo 6

Sistemas nacionales

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

2. Cada Estado miembro será responsable de garantizar la disponibilidad ininterrumpida de los datos del SIS II para los usuarios finales.».

2) El artículo 11 se sustituye por el texto siguiente:

«Artículo 11
Confidencialidad – Estados miembros

1. 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 II y con información complementaria, de conformidad con su legislación nacional. Esta obligación seguirá siendo aplicable después del cese en el cargo o el empleo de dichas personas o tras la terminación de las actividades de dichos organismos.

2. Cuando un Estado miembro coopere con contratistas externos en cometidos relacionados con el SIS II, deberá supervisar atentamente las actividades del contratista para garantizar el cumplimiento de todas las disposiciones de la presente Decisión, en particular en materia de seguridad, confidencialidad y protección de datos.

3. No se encomendará a empresas u organizaciones privadas la gestión operativa del N.SIS II o de cualesquiera copias técnicas.».

3) El artículo 15 se modifica como sigue:

a) se inserta el apartado siguiente:

«3 *bis*. La Autoridad de Gestión desarrollará y mantendrá un mecanismo y procedimientos para realizar controles de calidad de los datos de la CS-SIS. Presentará informes periódicos a los Estados miembros a este respecto.

La Autoridad de Gestión presentará a la Comisión un informe periódico sobre los problemas detectados y los Estados miembros afectados.

La Comisión transmitirá al Parlamento Europeo y al Consejo un informe periódico sobre los problemas que se detecten en relación con la calidad de los datos.»;

b) el apartado 8 se sustituye por el texto siguiente:

«8. La gestión operativa del SIS II Central consistirá en todas las actuaciones necesarias para mantenerlo en funcionamiento ininterrumpido, de conformidad con la presente Decisión y, en particular, en el trabajo de mantenimiento y de adaptación técnica necesario para el buen funcionamiento del sistema. Estas actuaciones incluirán asimismo la coordinación, gestión y apoyo a las actividades de ensayo para el SIS II Central y los N.SIS II, que garantizan que el SIS II Central y los N.SIS II funcionen con arreglo a los requisitos de conformidad técnica establecidos en el artículo 9.».

4) En el artículo 17, se añaden los apartados siguientes:

«3. Cuando la Autoridad de Gestión coopere con contratistas externos en cometidos relacionados con el SIS II, deberá supervisar atentamente las actividades del contratista para garantizar el cumplimiento de todas las disposiciones de la presente Decisión, en particular en materia de seguridad, confidencialidad y protección de datos.

4. No se encomendará a empresas u organizaciones privadas la gestión operativa de la CS-SIS.».

5) En el artículo 21 se añade el párrafo siguiente:

«Cuando se busque a una persona o un objeto en virtud de una descripción relacionada con un delito de terrorismo, el caso se considerará adecuado, pertinente y suficientemente importante como para justificar una descripción en el SIS II. Con carácter excepcional, los Estados miembros podrán abstenerse, por motivos de seguridad pública o nacional, de introducir una descripción, cuando sea probable que obstaculice indagaciones, investigaciones o procedimientos administrativos o judiciales.».

6) El artículo 22 se sustituye por el texto siguiente:

«Artículo 22
Normas específicas aplicables a la introducción de fotografías e impresiones dactilares, su comprobación o consulta

1. Las fotografías e impresiones dactilares solo se introducirán tras ser sometidas a un control de calidad especial para determinar si satisfacen unas normas mínimas de calidad de los datos. Las especificaciones relativas al control de calidad especial se establecerán de conformidad con el procedimiento contemplado en el artículo 67.

2. Cuando una descripción del SIS II disponga de fotografías e impresiones dactilares, esas fotografías e impresiones dactilares se utilizarán para confirmar la identidad de una persona que haya sido localizada como consecuencia de una consulta alfanumérica realizada en el SIS II.

3. Las impresiones dactilares podrán consultarse en todos los casos para identificar a una persona. Ahora bien, las impresiones dactilares se consultarán para identificar a una persona cuando su identidad no pueda determinarse por otros medios. A tal fin, el SIS II Central incluirá un sistema automático de identificación dactilar (SAID).

4. Los datos del SIS II relativos a impresiones dactilares por lo que respecta a descripciones introducidas conforme a los artículos 26, 32 y 36 también podrán cotejarse utilizando conjuntos completos o incompletos de impresiones dactilares descubiertas en los lugares de comisión de delitos graves o delitos de terrorismo que estén siendo investigados, cuando pueda acreditarse con un alto grado de probabilidad que esos conjuntos de impresiones pertenecen a un autor del delito y siempre que la consulta también se realice de forma simultánea en las bases de datos nacionales pertinentes de impresiones dactilares de los Estados miembros.».

7) El artículo 41 se sustituye por el texto siguiente:

«Artículo 41
Acceso de Europol a los datos del SIS II

1. La Agencia de la Unión Europea para la Cooperación Policial (Europol), establecida por el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo*, tendrá derecho, cuando sea necesario para cumplir su mandato, a acceder a los datos del SIS II y a consultarlos. Europol también podrá intercambiar y solicitar información complementaria de conformidad con lo dispuesto en el Manual Sirene.

2. En caso de que una consulta efectuada por Europol revele la existencia de una descripción en el SIS II, Europol informará al Estado miembro emisor mediante el intercambio de información complementaria a través de la infraestructura de comunicación y de conformidad con lo dispuesto en el Manual Sirene. Hasta que Europol esté en condiciones de utilizar las funciones previstas para el intercambio de información complementaria, Europol informará al Estado miembro emisor a través de los canales establecidos por el Reglamento (UE) 2016/794.

3. Europol podrá tratar la información complementaria que le proporcionen los Estados miembros para cotejarla con sus bases de datos y proyectos de análisis operativos, con el fin de detectar conexiones u otros vínculos pertinentes, y para llevar a cabo los análisis estratégicos, temáticos u operativos a los que se refiere el artículo 18, apartado 2, letras a), b) y c), del Reglamento (UE) 2016/794. Todo tratamiento de la información complementaria llevado a cabo por Europol a efectos del presente artículo se realizará de conformidad con lo dispuesto en dicho Reglamento.

4. El uso por parte de Europol de la información obtenida como consecuencia de una consulta del SIS II o del tratamiento de información complementaria estará sujeto al consentimiento del Estado miembro emisor. 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 comunicar esa información a terceros países u organismos con el consentimiento del Estado miembro emisor y con pleno cumplimiento del Derecho de la Unión en materia de protección de datos.

5. Europol deberá:

a) sin perjuicio de lo dispuesto en los apartados 4 y 6, no conectar las partes del SIS II a las que acceda ni transferir los datos contenidos en él a ningún sistema de recopilación y tratamiento de datos gestionado o alojado por Europol, ni descargar ni copiar de otra manera parte alguna del SIS II;

b) no obstante lo dispuesto en el artículo 31, apartado 1, del Reglamento (UE) 2016/794, suprimir la información complementaria que contenga datos personales a más tardar un año después de que la descripción correspondiente haya sido suprimida. Como excepción, cuando Europol disponga de información en sus bases de datos o en proyectos de análisis operativos sobre un caso relacionado con la información complementaria, Europol, a título excepcional y a fin de desempeñar sus funciones, podrá seguir conservando la información complementaria cuando sea necesario. Europol informará al Estado miembro emisor y al Estado miembro de ejecución de la prolongación de la conservación de dicha información complementaria y la justificará;

c) limitar el acceso a los datos del SIS II, incluida la información complementaria, al personal de Europol expresamente autorizado para ello que necesite acceso a esos datos para desempeñar sus funciones;

d) adoptar y aplicar medidas para garantizar la seguridad, la confidencialidad y el control interno, de conformidad con los artículos 10, 11 y 13;

e) garantizar que su personal autorizado para tratar los datos del SIS II reciba la formación y la información adecuadas, de conformidad con el artículo 14; y

f) sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/794, permitir que el Supervisor Europeo de Protección de Datos supervise y examine las actividades que Europol realiza tanto en el ejercicio de su derecho a acceder a los datos del SIS II y a consultarlos, como en el marco del intercambio y tratamiento de información complementaria.

6. Europol solo podrá copiar datos del SIS II con fines técnicos, cuando la copia sea necesaria para la consulta directa por el personal autorizado de Europol. La presente Decisión será aplicable a esas copias. La copia técnica solo se utilizará para almacenar datos del SIS II mientras se consultan dichos datos. Una vez que los datos hayan sido consultados, se suprimirán. Estos usos no se considerarán descargas o copias ilegales de datos del SIS II. Europol no podrá copiar datos de las descripciones ni datos adicionales emitidos por Estados miembros o procedentes de la CS-SIS II en otros sistemas de Europol.

7. A fin de verificar la legalidad del tratamiento de datos, de llevar a cabo un control interno y de garantizar la adecuada seguridad e integridad de los datos, Europol conservará un registro de cada acceso al SIS II y de cada consulta en este, de conformidad con lo dispuesto en el artículo 12. Ese tipo de registros y de documentación no se considerarán copias o descargas ilegales de partes del SIS II.

8. Los Estados miembros informarán a Europol mediante el intercambio de información complementaria de cualquier respuesta positiva para descripciones relacionadas con delitos de terrorismo. Con carácter excepcional, los Estados miembros podrán no informar a Europol si ello perjudicase investigaciones en curso o la seguridad de una persona o fuera contrario a los intereses esenciales de seguridad del Estado miembro emisor.

9. El apartado 8 será de aplicación a partir de la fecha en que Europol pueda recibir información complementaria de conformidad con el apartado 1.

---

* Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).».

8) Se inserta el artículo siguiente:

«Artículo 42

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

1. De conformidad con el artículo 40, apartado 8, del Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo*, los miembros de los equipos mencionados en el artículo 2, puntos 8 y 9, de dicho Reglamento, en el marco de su mandato y siempre que estén autorizados a llevar a cabo inspecciones de conformidad con lo dispuesto en el artículo 40, apartado 1, de la presente Decisión, y hayan recibido la formación necesaria de conformidad con el artículo 14 de la presente Decisión, tendrán derecho a acceder a los datos del SIS II y a consultarlos en la medida de lo necesario para el cumplimiento de sus funciones y siempre que lo exija el plan operativo de una operación específica. El acceso a los datos del SIS II no se hará extensivo a ningún otro miembro del equipo.

2. Los miembros de los equipos mencionados en el apartado 1 ejercerán el derecho a acceder a los datos del SIS II y a consultarlos de conformidad con el apartado 1 a través de una interfaz técnica. La Agencia Europea de la Guardia de Fronteras y Costas creará y mantendrá la interfaz técnica, la cual permitirá la conexión directa con el SIS II Central.

3. En caso de que una consulta efectuada por un miembro de los equipos mencionados en el apartado 1 del presente artículo revele la existencia de una descripción en el SIS II, se informará de ello al Estado miembro emisor. De conformidad con el artículo 40 del Reglamento (UE) 2016/1624, los miembros de los equipos solo actuarán en respuesta a una descripción en el SIS II siguiendo las instrucciones de los guardias de fronteras del Estado miembro de acogida en el que estén trabajando o del personal de este que participe en tareas relacionadas con el retorno y, como norma general, en su presencia. El Estado miembro de acogida podrá autorizar a los miembros de los equipos para que actúen en su nombre.

4. A fin de verificar la legalidad del tratamiento de datos, de llevar a cabo un control interno y de garantizar la adecuada seguridad e integridad de los datos, la Agencia Europea de la Guardia de Fronteras y Costas conservará un registro de cada acceso al SIS II y de cada consulta en este, de conformidad con lo dispuesto en el artículo 12.

5. La Agencia Europea de la Guardia de Fronteras y Costas adoptará y aplicará medidas para garantizar la seguridad, la confidencialidad y el control interno, de conformidad con los artículos 10, 11 y 13, y se asegurará de que los equipos mencionados en el apartado 1 del presente artículo aplican dichas medidas.

6. Ninguna disposición del presente artículo podrá interpretarse en el sentido de que afecta a lo dispuesto en el Reglamento (UE) 2016/1624 por lo que respecta a la protección de datos o a la responsabilidad de la Agencia Europea de la Guardia de Fronteras y Costas por el tratamiento no autorizado o incorrecto de datos por su parte.

7. Sin perjuicio del apartado 2, ninguna parte del SIS II se conectará a ningún sistema de recopilación y tratamiento de datos gestionado por los equipos mencionados en el apartado 1 o por la Agencia Europea de la Guardia de Fronteras y Costas, y los datos del SIS II a los que dichos equipos tengan acceso no se transferirán a dicho sistema. No se descargará ni copiará ninguna parte del SIS II. El registro de los accesos y consultas no se considerará descarga o copia ilegal de datos del SIS II.

8. La Agencia Europea de la Guardia de Fronteras y Costas permitirá al Supervisor Europeo de Protección de Datos supervisar y examinar las actividades que realicen los equipos mencionados en el presente artículo en el ejercicio de su derecho a acceder a los datos del SIS II y a consultarlos. La presente disposición se entenderá sin perjuicio de las demás disposiciones del Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo**+.

---

* 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).

** Reglamento (UE) 2018/… del Parlamento Europeo y del Consejo, de …, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO …).».

+ DO: insértese en el texto el número de serie del Reglamento que figura en el documento PE-CONS 31/18 y complétese en la nota correspondiente la referencia de publicación.

Artículo 78

Derogación

Quedan derogados el Reglamento (CE) n.º 1986/2006 y las Decisiones 2007/533/JAI y 2010/261/UE a partir de la fecha de aplicación del presente Reglamento, establecida en el artículo 79, apartado 5, párrafo primero.

Las referencias al Reglamento (CE) n.º 1986/2006 derogado y a la Decisión 2007/533/JAI derogada se entenderán hechas al presente Reglamento con arreglo a la tabla de correspondencias que figura en el anexo.

Artículo 79

Entrada en vigor, entrada en funcionamiento y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. A más tardar el … [tres años después de la entrada en vigor del presente Reglamento], la Comisión adoptará una decisión por la que establezca la fecha en la que el SIS entrará en funcionamiento de conformidad con el presente Reglamento, una vez que se verifique que se cumplen las condiciones siguientes:

   a) se han adoptado los actos de ejecución necesarios para la aplicación del presente Reglamento;

   b) los Estados miembros han 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; y

c) eu-LISA ha informado a la Comisión de la conclusión satisfactoria de todas las actividades de ensayo por lo que respecta a la CS-SIS y a la interacción entre la CS-SIS y los N.SIS.

3. La Comisión hará un atento seguimiento del proceso de cumplimiento gradual de las condiciones establecidas en el apartado 2 e informará al Parlamento Europeo y al Consejo del resultado de la verificación a la que se refiere dicho apartado.

4. A más tardar el … [un año después de la entrada en vigor del presente Reglamento] y, a continuación, todos los años hasta que se haya adoptado la decisión de la Comisión a que se refiere el apartado 2, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la situación de los preparativos para la plena aplicación del presente Reglamento. Dicho informe contendrá también información pormenorizada sobre los costes soportados y sobre los riesgos que puedan afectar a los costes globales.

5. El presente Reglamento será aplicable a partir de la fecha determinada de conformidad con el apartado 2.

Como excepción a lo dispuesto en el párrafo primero:

a) el artículo 4, apartado 4, el artículo 5, el artículo 8, apartado 4, el artículo 9, apartados 1 y 5, el artículo 12, apartado 8, el artículo 15, apartado 7, el artículo 19, el artículo 20, apartados 4 y 5, el artículo 26, apartado 6, el artículo 32, apartado 9, el artículo 34, apartado 3, el artículo 36, apartado 6, el artículo 38, apartados 3 y 4, el artículo 42, apartado 5, el artículo 43, apartado 4, el artículo 54, apartado 5, el artículo 62, apartado 4, el artículo 63, apartado 6, el artículo 74, apartados 7 y 10, los artículos 75 y 76, el artículo 77, puntos 1 a 5, y los apartados 3 y 4 del presente artículo serán aplicables a partir de la fecha de entrada en vigor del presente Reglamento;

b) el artículo 77, puntos 7 y 8, será aplicable a partir del … [un año después de la entrada en vigor del presente Reglamento];

c) el artículo 77, punto 6, será aplicable a partir del … [dos años después de la entrada en vigor del presente Reglamento].

6. La decisión de la Comisión a que se refiere el apartado 2 se publicará en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en los Estados miembros de conformidad con los Tratados.

Hecho en …, el

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

ANEXO

Tabla de correspondencias

Decisión 2007/533/JAI	El presente Reglamento
Artículo 1	Artículo 1
Artículo 2	Artículo 2
Artículo 3	Artículo 3
Artículo 4	Artículo 4
Artículo 5	Artículo 5
Artículo 6	Artículo 6
Artículo 7	Artículo 7
Artículo 8	Artículo 8
Artículo 9	Artículo 9
Artículo 10	Artículo 10
Artículo 11	Artículo 11
Artículo 12	Artículo 12
Artículo 13	Artículo 13
Artículo 14	Artículo 14
Artículo 15	Artículo 15
Artículo 16	Artículo 16
Artículo 17	Artículo 17
Artículo 18	Artículo 18
Artículo 19	Artículo 19
Artículo 20	Artículo 20
Artículo 21	Artículo 21
Artículo 22	Artículos 42 y 43

Decisión 2007/533/JAI	El presente Reglamento
Artículo 23	Artículo 22
–	Artículo 23
Artículo 24	Artículo 24
Artículo 25	Artículo 25
Artículo 26	Artículo 26
Artículo 27	Artículo 27
Artículo 28	Artículo 28
Artículo 29	Artículo 29
Artículo 30	Artículo 30
Artículo 31	Artículo 31
Artículo 32	Artículo 32
Artículo 33	Artículo 33
Artículo 34	Artículo 34
Artículo 35	Artículo 35
Artículo 36	Artículo 36
Artículo 37	Artículo 37
Artículo 38	Artículo 38
Artículo 39	Artículo 39
–	Artículo 40
–	Artículo 41
Artículo 40	Artículo 44
–	Artículo 45
–	Artículo 46
–	Artículo 47

Decisión 2007/533/JAI	El presente Reglamento
Artículo 41	Artículo 48
Artículo 42	Artículo 49
–	Artículo 51
Artículo 42 bis	Artículo 50
Artículo 43	Artículo 52
Artículo 44	Artículo 53
Artículo 45	Artículo 54
–	Artículo 55
Artículo 46	Artículo 56
Artículo 47	Artículo 57
Artículo 48	Artículo 58
Artículo 49	Artículo 59
–	Artículo 60
Artículo 50	Artículo 61
Artículo 51	Artículo 62
Artículo 52	Artículo 63
Artículo 53	Artículo 64
Artículo 54	Artículo 65
Artículo 55	–
Artículo 56	–
Artículo 57	Artículo 66
Artículo 58	Artículo 67
Artículo 59	Artículo 68
Artículo 60	Artículo 69

Decisión 2007/533/JAI	El presente Reglamento
Artículo 61	Artículo 70
Artículo 62	Artículo 71
Artículo 63	–
Artículo 64	Artículo 72
Artículo 65	Artículo 73
Artículo 66	Artículo 74
–	Artículo 75
Artículo 67	Artículo 76
Artículo 68	–
–	Artículo 77
Artículo 69	–
–	Artículo 78
Artículo 70	–
Artículo 71	Artículo 79

Reglamento (CE) n.º 1986/2006	El presente Reglamento
Artículos 1, 2 y 3	Artículo 45