DECISIÓN DE LA COMISIÓN

de 4 de mayo de 2010

relativa al plan de seguridad para el SIS II Central y la infraestructura de comunicación

(2010/261/UE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) nº 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) [1], y, en particular, su artículo 16,

Vista la 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) [2], y, en particular, su artículo 16,

Considerando lo siguiente:

(1) El artículo 16 del Reglamento (CE) nº 1987/2006 y el artículo 16 de la Decisión 2007/533/JAI establecen que la Autoridad de Gestión, en lo referente al SIS II Central, y la Comisión, en lo referente a la infraestructura de comunicación, adoptarán las medidas adecuadas, incluido un plan de seguridad.

(2) El artículo 15, apartado 4, del Reglamento (CE) nº 1987/2006 y el artículo 15, apartado 4, de la Decisión 2007/533/JAI establecen que durante un período transitorio que concluirá cuando asuma sus responsabilidades la Autoridad de Gestión, la Comisión se encargará de la gestión operativa del SIS II Central.

(3) Al no haberse establecido aún la Autoridad de Gestión, el plan de seguridad que debe adoptar la Comisión también será aplicable al SIS II Central durante un período transitorio.

(4) El Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo [3] se aplica al tratamiento de datos personales por la Comisión en el ejercicio de sus responsabilidades en cuanto a la gestión operativa del SIS II.

(5) El artículo 15, apartado 7, del Reglamento (CE) nº 1987/2006 y el artículo 15, apartado 7, de la Decisión 2007/533/JAI, establecen que, en caso de que durante el período transitorio la Comisión delegase sus responsabilidades antes de que la Autoridad de Gestión asuma las suyas, se asegurará de que dicha delegación no afecte negativamente a ningún mecanismo de control efectivo previsto en el Derecho de la Unión, corresponda este al Tribunal de Justicia, al Tribunal de Cuentas o al Supervisor Europeo de Protección de Datos.

(6) La Autoridad de Gestión debe adoptar su propio plan de seguridad en relación con SIS II Central una vez haya asumido sus responsabilidades. En consecuencia, el presente plan de seguridad expirará, en lo que respecta al SIS II Central, cuando la Autoridad de Gestión asuma sus responsabilidades.

(7) El artículo 4, apartado 3, del Reglamento (CE) nº 1987/2006 y el artículo 4, apartado 3, de la Decisión 2007/533/JAI establecen que la CS-SIS, encargada de la supervisión técnica y de la administración, estará situada en Estrasburgo (Francia), y habrá una copia de seguridad de la CS-SIS, capaz de realizar todas las funciones de la CS-SIS principal en caso de fallo del sistema, en Sankt Johann im Pongau (Austria).

(8) El plan de seguridad debe prever que un responsable de seguridad del sistema asuma las funciones de seguridad tanto con respecto al SIS II Central como a la infraestructura de comunicación, y que dos responsables locales de seguridad asuman las funciones de seguridad con respecto al SIS II Central y a la infraestructura de comunicación, respectivamente. Las tareas de los responsables de seguridad deben definirse a fin de asegurar una respuesta rápida y eficaz a los incidentes de seguridad y la presentación de informes al respecto.

(9) Debe establecerse una política de seguridad mediante la descripción de todos los detalles técnicos y organizativos, en consonancia con las disposiciones de la presente Decisión.

(10) Deben definirse las medidas que garanticen el nivel adecuado de seguridad del funcionamiento del SIS II Central y de la infraestructura de comunicación.

[1] DO L 381 de 28.12.2006, p. 4.
[2] DO L 205 de 7.8.2007, p. 63.
[3] DO L 8 de 12.1.2001, p. 1.

DECIDE:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

1. La presente Decisión establece la organización y las medidas de seguridad (plan de seguridad) para la protección del SIS II Central y de los datos tratados en él contra las amenazas que afecten a su disponibilidad, integridad y confidencialidad, con arreglo al artículo 16, apartado 1, del Reglamento (CE) nº 1987/2006 y al artículo 16, apartado 1, de la Decisión 2007/533/JAI relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) durante un período transitorio, hasta que la Autoridad de Gestión asuma sus responsabilidades.

2. La presente Decisión establece la organización y las medidas de seguridad (plan de seguridad) para la protección de la infraestructura de comunicación contra las amenazas que afectan a su disponibilidad, integridad y confidencialidad, con arreglo al artículo 16 del Reglamento (CE) nº 1987/2006 y al artículo 16 de la Decisión 2007/533/JAI relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) .

CAPÍTULO II

ORGANIZACIÓN, RESPONSABILIDADES Y GESTIÓN DE INCIDENTES

Artículo 2

Funciones de la Comisión

1. La Comisión ejecutará y controlará la eficacia de las medidas de seguridad relativas al SIS II Central mencionadas en la presente Decisión.

2. La Comisión ejecutará y controlará la eficacia de las medidas de seguridad relativas a la infraestructura de comunicación mencionadas en la presente Decisión.

3. La Comisión designará a un responsable de seguridad del sistema entre sus funcionarios. El funcionario responsable de seguridad del sistema será designado por el Director General de la Dirección General de Justicia, Libertad y Seguridad de la Comisión. Las funciones del funcionario responsable de seguridad del sistema incluirán, en particular:

a) la elaboración de la política de seguridad tal como se describe en el artículo 7 de la presente Decisión;

b) el control de la eficacia de la aplicación de los procedimientos de seguridad del SIS II Central;

c) el control de la eficacia de la aplicación de los procedimientos de seguridad de la infraestructura de comunicación;

d) contribuir a elaborar los informes relacionados con la seguridad previstos en el artículo 50 del Reglamento (CE) nº 1987/2006 y el artículo 66 de la Decisión 2007/533/JAI;

e) funciones de coordinación y asistencia en el marco de los controles y auditorías realizados por el Supervisor Europeo de Protección de Datos previstos en el artículo 45 del Reglamento (CE) nº 1987/2006 y en el artículo 61 de la Decisión 2007/533/JAI, así como la notificación de incidentes con arreglo al artículo 5, apartado 2, al responsable de la protección de datos de la Comisión;

f) el control de la aplicación adecuada e íntegra de la presente Decisión y de la política de seguridad por todo contratista, incluidos los subcontratistas, que intervenga de alguna manera en la gestión de SIS II Central;

g) el control de la aplicación adecuada e íntegra de la presente Decisión y de la política de seguridad por todo contratista, incluidos los subcontratistas, que intervenga de alguna manera en la gestión de la infraestructura de comunicación;

h) el mantenimiento de una lista de puntos de contacto nacionales únicos para la seguridad del SIS II que se utilizará conjuntamente con el responsable local de seguridad para la infraestructura de comunicación;

i) la utilización conjunta de la lista mencionada en la letra h) con el responsable local de seguridad para el SIS II Central.

Artículo 3

Responsable local de seguridad del SIS II Central

1. Sin perjuicio de lo dispuesto en el artículo 8, la Comisión designará a un responsable local de seguridad para el SIS II Central entre sus funcionarios. Se prevendrán los conflictos de intereses entre las obligaciones del responsable local de seguridad y cualquier otra obligación oficial. El responsable local de seguridad para el SIS II Central será designado por el Director General de la Dirección General de Justicia, Libertad y Seguridad de la Comisión.

2. El responsable local de seguridad para el SIS II Central se asegurará de que se ejecuten las medidas de seguridad mencionadas en la presente Decisión y se apliquen los procedimientos de seguridad en la CS-SIS principal. En lo que respecta a la copia de seguridad de la CS-SIS, el responsable local de seguridad para el SIS II Central se asegurará también de que se ejecuten las medidas de seguridad mencionadas en la presente Decisión, a excepción de las mencionadas en el artículo 9, y de que se apliquen los procedimientos de seguridad correspondientes.

3. El responsable local de seguridad para el SIS II Central podrá confiar cualquiera de sus funciones al personal subordinado. Se prevendrán los conflictos de intereses entre la obligación de ejercer estas funciones y cualquier otra obligación oficial. Un número de teléfono único y una dirección única permitirán ponerse en contacto en todo momento con el responsable local de seguridad o con su subordinado que esté de servicio.

4. El responsable local de seguridad para el SIS II Central ejercerá las funciones derivadas de las medidas de seguridad que se adopten en los locales en que se encuentren la CS-SIS principal y la copia de seguridad de la CS-SIS, dentro de los límites del apartado 1, funciones entre las que se incluyen, en particular:

a) las funciones de seguridad operativa local, incluida la auditoría de cortafuegos (*firewall*), los controles regulares de seguridad y la elaboración de auditorías e informes;

b) controlar la eficacia del plan de continuidad de la actividad y asegurarse de que se realicen ejercicios regulares;

c) asegurarse de los indicios en relación con cualquier incidente que se produzca en el SIS II Central que pueda repercutir en la seguridad del SIS II Central o la infraestructura de comunicación, y presentar informes al respecto al responsable de seguridad del sistema;

d) informar al responsable de seguridad del sistema sobre la necesidad de modificar la política de seguridad;

e) controlar la aplicación de la presente Decisión y de la política de seguridad por todo contratista, incluidos los subcontratistas, que intervenga de alguna manera en la gestión operativa del SIS II Central;

f) garantizar que el personal conozca sus obligaciones y controlar la aplicación de la política de seguridad;

g) seguir los avances en materia de seguridad informática y garantizar la formación adecuada del personal;

h) preparar la información necesaria y las opciones para el establecimiento, la actualización y la revisión de la política de seguridad de conformidad con el artículo 7.

Artículo 4

Responsable local de seguridad de la infraestructura de comunicación

1. Sin perjuicio de lo dispuesto en el artículo 8, la Comisión designará a un responsable local de seguridad para la infraestructura de comunicación entre sus funcionarios. Se evitarán los conflictos de intereses entre las funciones del responsable local de seguridad y cualquier otra función oficial. El responsable local de seguridad para la infraestructura de comunicación será designado por el Director General de la Dirección General de Justicia, Libertad y Seguridad de la Comisión.

2. El responsable local de seguridad para la infraestructura de comunicación supervisará el funcionamiento de la infraestructura de comunicación y se asegurará de que se ejecuten las medidas de seguridad y se apliquen los procedimientos de seguridad.

3. El responsable local de seguridad para la infraestructura de comunicación podrá confiar cualquiera de sus funciones al personal subordinado. Se prevendrán los conflictos de intereses entre la obligación de ejercer estas funciones y cualquier otra obligación oficial. Un número de teléfono único y una dirección única permitirán ponerse en contacto en todo momento con el responsable local de seguridad o con su subordinado que esté de servicio.

4. El funcionario local de seguridad para la infraestructura de comunicación ejercerá las funciones derivadas de las medidas de seguridad que deban adoptarse en la infraestructura de la comunicación, funciones entre las que se incluyen, en particular:

a) las funciones de seguridad operativa relacionadas con la infraestructura de comunicación, incluida la auditoría de sistemas *firewall*, los controles regulares de seguridad y la elaboración de auditorías e informes;

b) controlar la eficacia del plan de continuidad de la actividad y asegurarse de que se realicen ejercicios regulares;

c) asegurarse de los indicios en relación con cualquier incidente que se produzca en la infraestructura de comunicación que pueda repercutir en la seguridad del SIS II Central o en la estructura de comunicación, y presentar informes al respecto al responsable de seguridad del sistema;

d) informar al responsable de seguridad del sistema de la necesidad de modificar la política de seguridad;

e) controlar la aplicación de la presente Decisión y de la política de seguridad por todo contratista, incluidos los subcontratistas, que intervenga de alguna manera en la gestión de la infraestructura de comunicación;

f) garantizar que el personal conozca sus obligaciones y controlar la aplicación de la política de seguridad;

g) seguir los avances en materia de seguridad informática y garantizar la formación adecuada del personal;

h) preparar la información necesaria y las opciones para el establecimiento, la actualización y la revisión de la política de seguridad de conformidad con el artículo 7.

Artículo 5

Incidentes de seguridad

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

2. Los incidentes de seguridad se gestionarán para garantizar una respuesta rápida, efectiva y adecuada de conformidad con la política de seguridad. Se adoptarán procedimientos para subsanar incidentes.

3. La información relativa a un incidente de seguridad que repercuta o pueda repercutir en el funcionamiento del SIS II en un Estado miembro o en la disponibilidad, integridad y confidencialidad de los datos introducidos o enviados por un Estado miembro, se facilitará al Estado miembro afectado. Los incidentes de la seguridad se notificarán al responsable de la protección de datos de la Comisión.

Artículo 6

Gestión de incidentes

1. El personal y los contratistas que se ocupen del desarrollo, la gestión o el funcionamiento del SIS II deberán señalar y comunicar cualquier deficiencia de seguridad que observen o sospechen en la infraestructura de comunicación al responsable de seguridad del sistema o al responsable local de seguridad para la infraestructura de comunicación.

2. En caso de que se detecte un incidente que afecte o pueda afectar a la seguridad del SIS II, el responsable local de seguridad para la infraestructura de comunicación informará lo antes posible al responsable de seguridad del sistema y, en su caso, al punto de contacto nacional único para la seguridad del SIS II, cuando dicho punto de contacto exista en el Estado miembro de que se trate, por escrito o, en caso de extrema urgencia, por otros medios de comunicación. El informe contendrá la descripción del incidente de seguridad, el nivel de riesgo, las posibles consecuencias y las medidas adoptadas o que deberán adoptarse para mitigar el riesgo.

3. El responsable local de seguridad para la infraestructura de comunicación recopilará inmediatamente cualquier indicio relacionado con el incidente de seguridad. En la medida que lo permitan las disposiciones aplicables en materia de protección de datos, dichos indicios se pondrán a disposición del responsable de seguridad del sistema a petición de este último.

4. En el marco de la política de seguridad, se definirán mecanismos de respuesta para garantizar que la información sobre la naturaleza, la gestión y el resultado del incidente de seguridad se comunique al responsable de seguridad del sistema y al responsable local de la seguridad para la infraestructura de la comunicación, una vez que el incidente haya sido resuelto y cerrado.

5. Los apartados 1 a 4 se aplicarán, *mutatis mutandis*, a los incidentes en el SIS II Central. A este respecto, las referencias al responsable local de la seguridad para la infraestructura de comunicación en los apartados 1 a 4 deberán entenderse como referencias al responsable local de seguridad para el SIS II Central.

CAPÍTULO III

MEDIDAS DE SEGURIDAD

Artículo 7

Política de seguridad

1. El Director General de la Dirección General de Justicia, Libertad y Seguridad establecerá, actualizará y revisará regularmente la política de seguridad obligatoria de conformidad con la presente Decisión. La política de seguridad preverá medidas y procedimientos detallados de protección contra las amenazas que afectan a la disponibilidad, integridad y confidencialidad de la infraestructura de comunicación, incluida la planificación de emergencia, a fin de garantizar un nivel de seguridad adecuado con arreglo a lo prescrito en la presente Decisión. La política de seguridad cumplirá lo dispuesto en la presente Decisión.

2. La política de seguridad se basará en una evaluación de riesgos. Las medidas descritas en la política de seguridad serán proporcionadas a los riesgos señalados.

3. La evaluación de riesgos y la política de seguridad se actualizarán cuando los cambios tecnológicos, la identificación de nuevas amenazas u otras circunstancias lo exijan. La política de seguridad se revisará en todo caso anualmente para garantizar que siga siendo una respuesta adecuada y conforme a la última evaluación de riesgos o a cualquier otro cambio tecnológico, amenaza o circunstancia pertinente recientemente señalados.

4. La política de seguridad será elaborada por el responsable de seguridad del sistema, en coordinación con el funcionario local de seguridad para el SIS II Central y el responsable local de seguridad para la infraestructura de comunicación.

5. Los apartados 1 a 4 se aplicarán, *mutatis mutandis*, a la política de seguridad para el SIS II Central. A este respecto, las referencias al responsable local de seguridad para la infraestructura de comunicación en los apartados 1 a 4 deberán entenderse como referencias al responsable local de seguridad para el SIS II Central.

Artículo 8

Ejecución de las medidas de seguridad

1. La ejecución de las funciones y los requisitos establecidos en la presente Decisión y en la política de seguridad, incluida la función de designación del responsable local de seguridad, podrá subcontratarse o confiarse a organismos públicos o privados.

2. En tal caso, la Comisión, mediante un acuerdo jurídicamente vinculante, se asegurará de que se cumplan plenamente los requisitos establecidos en la presente Decisión y en la política de seguridad. En caso de delegación o subcontratación de la función de designación del responsable local de seguridad, la Comisión, mediante un acuerdo jurídicamente vinculante, se asegurará de que se le consulte sobre la persona que deba designarse como responsable local de seguridad.

Artículo 9

Control de acceso a las instalaciones

1. Se utilizarán perímetros de seguridad con barreras y controles de entrada adecuados para proteger las zonas en las que se encuentren las instalaciones de tratamiento de datos.

2. Dentro de los perímetros de seguridad, se definirán zonas seguras para proteger los elementos físicos (activos), incluidos los equipos informáticos, los soportes de datos y las consolas, los planes y otros documentos sobre SIS II, así como las oficinas y demás lugares de trabajo del personal encargado del funcionamiento del SIS II. Estas zonas seguras se protegerán mediante controles de entrada adecuados que garantizarán el acceso únicamente al personal autorizado. El trabajo en las zonas seguras estará sujeto a las normas de seguridad detalladas establecidas en la política de seguridad.

3. Se preverán e instalarán dispositivos de seguridad física de las oficinas, salas e instalaciones. Se controlarán los puntos de acceso como las zonas de entrega y de carga y otros puntos por los que personas no autorizadas puedan entrar en los locales y, cuando sea posible, dichos puntos se aislarán de las instalaciones de tratamiento de datos para evitar el acceso no autorizado.

4. La protección física de los perímetros de seguridad contra daños causados por catástrofes naturales o de origen humano se concebirá y aplicará de forma proporcional al riesgo.

5. Los equipos se protegerán contra las amenazas físicas y medioambientales, así como contra cualquier posibilidad de acceso no autorizado.

6. Cuando la Comisión disponga de la información pertinente, añadirá a la lista mencionada en el artículo 2, apartado 3, letra h), un punto de contacto único para supervisar la aplicación de lo dispuesto en el presente artículo en los locales en los que se encuentre la copia de seguridad de la CS-SIS.

Artículo 10

Soportes de datos y control de activos

1. Los soportes extraíbles que contengan datos se protegerán contra el acceso no autorizado, el uso indebido y los daños, y se garantizará su legibilidad durante el tiempo de vida completo de los datos.

2. Cuando ya no se necesiten, los soportes se eliminarán por medios seguros y protegidos, de conformidad con los procedimientos detallados que se establezcan en la política de seguridad

3. Los inventarios garantizarán la disponibilidad de información sobre el lugar de almacenamiento, el período de retención aplicable y las autorizaciones de acceso.

4. Se identificarán todos los activos importantes de la infraestructura de comunicación, a fin de protegerlos según su importancia. Se mantendrá un registro actualizado de los equipos informáticos pertinentes.

5. La documentación actualizada sobre la infraestructura de comunicación deberá estar disponible. Esta documentación deberá protegerse contra el acceso no autorizado.

6. Los apartados 1 a 5 se aplicarán, *mutatis mutandis*, al SIS II Central. A este respecto, las referencias a la infraestructura de comunicación se entenderán como referencias al SIS II Central.

Artículo 11

Control de almacenamiento

1. Se adoptarán las medidas necesarias para garantizar el almacenamiento adecuado de los datos y evitar el acceso no autorizado a estos.

2. Los elementos de los equipos que contengan soportes de almacenamiento serán sometidos a una verificación que garantice la retirada o sobreescritura completa de los datos sensibles antes de su eliminación, o serán destruidos por medios seguros.

Artículo 12

Control de contraseña

1. Las contraseñas se conservarán con seguridad y se tratarán de forma confidencial. Cuando se sospeche que ha sido revelada, la contraseña deberá cambiarse inmediatamente o bien se desactivará la cuenta de que se trate. Se utilizarán identidades de usuario individuales y únicas.

2. En el marco de la política de seguridad se definirán los procedimientos para iniciar y cerrar la sesión, así como para prevenir el acceso no autorizado.

Artículo 13

Control de acceso

1. La política de seguridad establecerá un procedimiento formal de registro y de anulación del registro del personal por el que se concederá y retirará el acceso a los equipos físicos y los programas informáticos del SIS II, a efectos de la gestión operativa. La atribución y la utilización de credenciales de acceso adecuadas (contraseñas u otros medios adecuados) se controlarán mediante un proceso de gestión formal establecido en el marco de la política de seguridad.

2. El acceso a los equipos físicos y a los programas informáticos del SIS II en la CS-SIS:

i) se limitará a las personas autorizadas,

ii) se limitará a los casos en los que pueda observarse un objetivo legítimo con arreglo al artículo 45 del Reglamento (CE) nº 1987/2006 y el artículo 61 de la Decisión 2007/533/JAI, o al artículo 50, apartado 2, del Reglamento (CE) nº 1987/2006 y el artículo 66, apartado 2, de la Decisión 2007/533/JAI,

iii) no superará la duración ni el alcance necesarios para los fines de acceso, y

iv) únicamente tendrá lugar con arreglo a la política de control de acceso que deberá definirse en el marco de la política de seguridad.

3. En la CS-SIS solo se utilizarán las consolas y los programas informáticos autorizados por el responsable local de seguridad para el SIS II Central. Se limitará y controlará el uso de utilidades del sistema que puedan reemplazar a los controles de aplicación y del sistema. Se aplicarán procedimientos para controlar la instalación de programas informáticos.

Artículo 14

Control de comunicación

La infraestructura de comunicación se controlará para facilitar la disponibilidad, integridad y confidencialidad necesarias para los intercambios de información. Se utilizarán medios criptográficos para proteger los datos transmitidos en la infraestructura de comunicación.

Artículo 15

Control de entrada

Las cuentas de las personas autorizadas para acceder a los programas informáticos del SIS II a partir de la CS-SIS serán controladas por el responsable local de seguridad para el SIS II Central. Se registrará la utilización de dichas cuentas, incluidas la fecha, la hora y la identidad del usuario.

Artículo 16

Control de transporte

1. En el marco de la política de seguridad, se definirán las medidas adecuadas para evitar la lectura, copia, modificación o supresión no autorizadas de datos personales en la transmisión al o desde SIS II o durante el transporte de soportes de datos. Se adoptarán disposiciones, en el marco de la política de seguridad, con respecto a los tipos de envío o transporte admisibles, así como respecto de los procedimientos de responsabilidad aplicables al transporte de elementos y su llegada al lugar de destino. El soporte de datos no contendrá ningún dato distinto de los datos que deban enviarse.

2. Los servicios prestados por terceros que impliquen el acceso, el tratamiento, la comunicación o la gestión de instalaciones de tratamiento de datos o la adición de productos o servicios a las instalaciones de tratamiento de datos, serán objeto de controles de seguridad integrados y adecuados.

Artículo 17

Seguridad de la infraestructura de comunicación

1. La infraestructura de comunicación será gestionada y controlada convenientemente a fin de protegerla contra las amenazas y garantizar su propia seguridad y la del SIS II Central, incluidos los datos intercambiados a través de ella.

2. Las especificaciones de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red se definirán en el acuerdo de servicio de red con el proveedor del servicio.

3. Además de proteger los puntos de acceso del SIS II, se protegerá también cualquier otro servicio adicional utilizado por la infraestructura de comunicación. Las medidas adecuadas se definirán en el marco de la política de seguridad.

Artículo 18

Supervisión

1. Los registros que contengan la información a que se refiere el artículo 18, apartado 1, del Reglamento (CE) nº 1987/2006 y el artículo 18, apartado 1, de la Decisión 2007/533/JAI, en relación con cada acceso a datos personales y cualquier intercambio de datos personales en la CS-SIS, se conservarán de forma segura y serán accesibles desde los locales donde se encuentren la CS-SIS principal y la copia de seguridad de la CS-SIS durante el período máximo mencionado en el artículo 18, apartado 3, del Reglamento (CE) nº 1987/2006 y el artículo 18, apartado 3, de la Decisión 2007/533/JAI.

2. En el marco de la política de seguridad, se establecerán los procedimientos de seguimiento de la utilización o de los fallos de las instalaciones de tratamiento de datos, y los resultados de las actividades de seguimiento se revisarán regularmente. En caso necesario, se adoptarán las medidas oportunas.

3. Los dispositivos de registro y los registros se protegerán contra las alteraciones y el acceso no autorizado a fin de cumplir los requisitos de recogida y retención de indicios para el período de retención de los datos.

Artículo 19

Métodos criptográficos

Se aplicarán, en su caso, métodos criptográficos para proteger la información. Su utilización, así como sus finalidades y condiciones, deberán ser aprobadas previamente por el responsable de seguridad del sistema.

CAPÍTULO IV

SEGURIDAD DE LOS RECURSOS HUMANOS

Artículo 20

Perfiles de los miembros del personal

1. La política de seguridad definirá las funciones y responsabilidades de las personas autorizadas para acceder al SIS II Central.

2. La política de seguridad definirá las funciones y responsabilidades de las personas autorizadas para acceder a la infraestructura de comunicación.

3. Las funciones y responsabilidades de seguridad del personal de la Comisión, los contratistas y el personal que interviene en la gestión operativa se definirán, documentarán y comunicarán a las personas interesadas. En la descripción del puesto de trabajo y los objetivos se definirán las funciones y responsabilidades del personal de la Comisión; en los contratos o los acuerdos de nivel de servicios se definirán las de los contratistas.

4. Se celebrarán acuerdos de confidencialidad y secreto profesional con las personas que no estén sujetas a las normas de la función pública de la Unión Europea o de un Estado miembro. El personal que deba trabajar con datos del SIS II dispondrá de la autorización o certificación necesaria, de conformidad con los procedimientos detallados que se adoptarán en el marco de la política de seguridad.

Artículo 21

Información del personal

1. El personal y los contratistas recibirán una formación adecuada en el ámbito de la sensibilización respecto de la seguridad, los requisitos jurídicos, las políticas y los procedimientos, en la medida necesaria para el ejercicio de sus funciones.

2. Al término de la actividad o del contrato, la política de seguridad definirá las responsabilidades relacionadas con el cambio de empleo o la terminación de la actividad que incumban al personal o los contratistas; la política de seguridad también establecerá los procedimientos de devolución de activos y retirada de derechos de acceso.

CAPÍTULO V

DISPOSICIÓN FINAL

Artículo 22

Aplicabilidad

1. La presente Decisión será aplicable en la fecha fijada por el Consejo de conformidad con el artículo 55, apartado 2, del Reglamento (CE) nº 1987/2006, y el artículo 71, apartado 2, de la Decisión 2007/533/JAI.

2. El artículo 1, apartado 1, el artículo 2, apartado 1, el artículo 2, apartado 3, letras b), d), f) e i), el artículo 3, el artículo 6, apartado 5, el artículo 7, apartado 5, el artículo 9, apartado 6, el artículo 10, apartado 6, el artículo 13, apartados 2 y 3, el artículo 15, el artículo 18 y el artículo 20, apartado 1, expirarán en el momento en que la Autoridad de Gestión asuma sus responsabilidades.

Hecho en Bruselas, el 4 de mayo de 2010.

Por la Comisión

El Presidente

José Manuel BARROSO