DECISIÓN DE LA COMISIÓN

de 4 de mayo de 2010

relativa al plan de seguridad para el funcionamiento del Sistema de Información de Visados

(2010/260/UE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) nº 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS) [1], y, en particular, su artículo 32,

Considerando lo siguiente:

(1) El artículo 32, apartado 3, del Reglamento (CE) nº 767/2008 establece que la autoridad de gestión adoptará las medidas necesarias para alcanzar los objetivos fijados en el apartado 2 del mismo artículo en relación con el funcionamiento del VIS, incluida la adopción de un plan de seguridad.

(2) El artículo 26, apartado 4, del Reglamento (CE) nº 767/2008 establece que durante un período transitorio anterior a la asunción de sus responsabilidades por parte de la autoridad de gestión, la Comisión será responsable de la gestión operativa del VIS.

(3) El Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo [2] se aplica al tratamiento de los datos personales por la Comisión en la ejecución de sus responsabilidades con respecto a la gestión operativa del VIS.

(4) El artículo 26, apartado 7, del Reglamento (CE) nº 767/2008 establece que, en caso de que, durante el período transitorio antes de que la autoridad de gestión asuma sus responsabilidades, la Comisión delegase sus responsabilidades, se asegurará de que la delegación no afecte negativamente a ningún mecanismo de control efectivo previsto en el Derecho comunitario, ya corresponda este al Tribunal de Justicia, al Tribunal de Cuentas o al Supervisor Europeo de Protección de Datos.

(5) La autoridad de gestión deberá establecer su propio plan de seguridad en relación con el VIS una vez que haya asumido sus responsabilidades.

(6) La Decisión 2008/602/CE de la Comisión, de 17 de junio de 2008, por la que se establecen la arquitectura física y las características de las interfaces nacionales y de la infraestructura de comunicación entre el Sistema central de Información de Visados y las interfaces nacionales para la fase de desarrollo [3], describe los servicios de seguridad necesarios aplicables a la red del VIS.

(7) El artículo 27 del Reglamento (CE) nº 767/2008 establece que el VIS central principal, encargado de la supervisión técnica y de la administración, estará situado en Estrasburgo (Francia), y que habrá una copia de seguridad del VIS central, capaz de realizar todas las funciones del VIS central en caso de fallo del sistema, en Sankt Johann im Pongau (Austria).

(8) Es preciso definir las funciones de los responsables de seguridad con el fin de garantizar que se responde a un incidente de seguridad y que se informa del mismo de forma rápida y eficaz.

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

(10) Es preciso definir medidas para garantizar el nivel de seguridad adecuado en la gestión del VIS.

HA ADOPTADO LA PRESENTE DECISIÓN:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

La presente Decisión establece las medidas y organización de seguridad (plan de seguridad) en el sentido del artículo 32, apartado 3, del Reglamento (CE) nº 767/2008.

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 del VIS central y de la infraestructura de comunicación a las que hace referencia la presente Decisión.

[1] DO L 218 de 13.8.2008, p. 60.
[2] DO L 8 de 12.1.2001, p. 1.
[3] DO L 194 de 23.7.2008, p. 3.

2. La Comisión deberá designar un responsable de seguridad del sistema de entre sus funcionarios. El responsable de seguridad del sistema deberá ser nombrado por el director general de la Dirección General de Justicia, Libertad y Seguridad de la Comisión. Sus cometidos incluirán, en particular:

a) la preparación, actualización y revisión de la política de seguridad descrita en el artículo 7 de la presente Decisión;

b) el control de la eficacia de la ejecución de los procedimientos de seguridad del VIS central y de la infraestructura de comunicación;

c) la contribución a la preparación de informes relacionados con la seguridad a que se hace referencia en el artículo 50, apartados 3 y 4, del Reglamento (CE) nº 767/2008;

d) la coordinación y asistencia en las tareas de control y auditoría llevadas a cabo por el Supervisor Europeo de Protección de los Datos a que se refiere el artículo 42 del Reglamento (CE) nº 767/2008;

e) 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 y el funcionamiento del VIS;

f) el mantenimiento de una lista de puntos de contacto nacionales únicos para la seguridad del VIS y su transmisión a los responsables locales de la seguridad del VIS central y de la infraestructura de comunicación.

Artículo 3

Responsable local de la seguridad para el VIS central

1. Sin perjuicio de lo dispuesto en el artículo 8, la Comisión nombrará un responsable local de la seguridad para el VIS central de entre sus funcionarios. Se deberán evitar los conflictos de intereses entre las obligaciones como responsable local de la seguridad y cualquier otra obligación oficial. El responsable local de la seguridad para el VIS central será nombrado por el director general de la Dirección General de Justicia, Libertad y Seguridad de la Comisión.

2. El responsable local de la seguridad del VIS central velará por la aplicación de las medidas de seguridad contempladas en la presente Decisión y por el respeto de los procedimientos de seguridad en el VIS central principal. Por lo que se refiere a la copia de seguridad del VIS central principal, el responsable local de la seguridad para el VIS central garantizará la aplicación de las medidas de seguridad a las que se refiere la presente Decisión, excepto las recogidas en el artículo 10, y el respeto de los procedimientos de seguridad correspondientes.

3. El responsable local de seguridad para el VIS central podrá asignar algunas de sus funciones al personal subordinado. Se deberán evitar los conflictos de intereses entre la obligación de ejecutar dichas funciones y cualquier otra obligación oficial. El responsable local de la seguridad o su subordinado en servicio deberán estar disponibles a cualquier hora a través de un número de contacto único y una dirección única.

4. El responsable local de la seguridad para el VIS central ejercerá las funciones derivadas de las medidas de seguridad a adoptar en la sede del VIS central principal y en la sede de la copia de seguridad del VIS central, dentro de los límites del apartado 1, y 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 pueda repercutir en la seguridad del VIS 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 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 y en la operación del VIS 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 evitarán 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 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 pueda repercutir en la seguridad del VIS 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 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 VIS y pueda causar un daño o una pérdida al VIS 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. La política de seguridad deberá establecer los procedimientos para subsanar los incidentes. Los incidentes de seguridad se gestionarán para garantizar una respuesta rápida, efectiva y adecuada de conformidad con la política de seguridad.

3. La información relativa a un incidente de seguridad que repercuta o pueda repercutir en el funcionamiento del VIS en un Estado miembro o en la disponibilidad, integridad y confidencialidad de los datos del VIS introducidos 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 VIS deberán señalar y comunicar cualquier deficiencia de seguridad que observen o sospechen en el funcionamiento del VIS al responsable de seguridad del sistema o al responsable local de seguridad para la infraestructura de comunicación, según proceda.

2. En caso de que se detecte un incidente que afecte o pueda afectar a la seguridad del funcionamiento del VIS, el responsable local de seguridad para el VIS central o 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 VIS, cuando dicho punto de contacto exista en el Estado miembro de que se trate, por escrito o, en caso de extrema urgencia, por otros canales 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 el VIS central o el responsable local de la seguridad para la infraestructura de comunicación, según proceda, 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. Se definirán mecanismos de respuesta para garantizar que la información sobre los resultados se comunique, una vez que el incidente haya sido resuelto y cerrado.

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 del VIS, 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 responsable local de seguridad para el VIS central y el responsable local de seguridad para la infraestructura de comunicación.

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 del 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 el VIS, así como las oficinas y demás lugares de trabajo del personal encargado del funcionamiento del VIS. 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 2, letra f), 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 del VIS.

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 el VIS y sobre la infraestructura de comunicación deberá estar disponible. Esta documentación deberá protegerse contra el acceso no autorizado.

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 VIS en el VIS central, 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 VIS:

i) se limitará a las personas autorizadas,

ii) se limitará a los casos en los que pueda observarse un objetivo legítimo con arreglo a los artículos 42 y 50, apartado 2, del Reglamento (CE) nº 767/2008,

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 el VIS solo se utilizarán las consolas y los programas informáticos autorizados por el responsable local de seguridad para el VIS 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 VIS a partir del VIS central serán controladas por el responsable local de seguridad para el VIS 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 VIS 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 VIS 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 VIS, 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 34, apartado 1, del Reglamento (CE) nº 767/2008 en relación con cada acceso a los datos y con todas las operaciones de tratamiento de datos en el VIS central, se conservarán de forma segura y serán accesibles desde los locales donde se encuentren el VIS principal y la copia de seguridad del VIS central durante el período mencionado en el artículo 34, apartado 2, del Reglamento (CE) nº 767/2008.

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 VIS, incluida la infraestructura de comunicación.

2. 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.

3. 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 VIS 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 la Comisión de conformidad con el artículo 48, apartado 1, del Reglamento (CE) nº 767/2008.

2. La presente Decisión expirará 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