DECISÃO DA COMISSÃO

de 4 de Maio de 2010

relativa ao plano de segurança para o SIS II Central e a infra-estrutura de comunicação

(2010/261/UE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (CE) n.º 1987/2006 do Parlamento Europeu e do Conselho, de 20 de Dezembro de 2006, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SIS II) [1], nomeadamente o artigo 16.º,

Tendo em conta a Decisão 2007/533/JAI do Conselho, de 12 de Junho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração (SIS II) [2], nomeadamente o artigo 16.º,

Considerando o seguinte:

(1) O artigo 16.º do Regulamento (CE) n.º 1987/2006 e o artigo 16.º da Decisão 2007/533/JAI prevêem que a autoridade de gestão, relativamente ao SIS II Central, e a Comissão, relativamente à infra-estrutura de comunicação, devem adoptar as medidas necessárias, incluindo um plano de segurança.

(2) O artigo 15.º, n.º 4, do Regulamento (CE) n.º 1987/2006 e o artigo 15.º, n.º 4, da Decisão 2007/533/JAI determinam que, durante o período transitório antes de a autoridade de gestão assumir funções, a Comissão é responsável pela gestão operacional do SIS II Central.

(3) Dado que a autoridade de gestão ainda não foi estabelecida, o plano de segurança a adoptar pela Comissão deve aplicar-se igualmente ao SIS II Central durante o período transitório.

(4) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho [3] aplica-se ao tratamento dos dados pessoais a realizar pela Comissão no contexto das suas responsabilidades de gestão operacional do SIS II.

(5) O artigo 15.º, n.º 7, do Regulamento (CE) n.º 1987/2006 e o artigo 15.º, n.º 7, da Decisão 2007/533/JAI determinam que, no caso de a Comissão delegar as suas responsabilidades durante o período transitório antes de a autoridade de gestão assumir as suas funções, deve assegurar que essa delegação não tem repercussões negativas em relação a qualquer mecanismo de controlo eficaz ao abrigo do direito da União, quer por parte do Tribunal de Justiça, do Tribunal de Contas ou da Autoridade Europeia para a Protecção de Dados.

(6) A autoridade de gestão deve estabelecer o seu próprio plano de segurança relativo ao SIS II Central quando assumir funções. Por conseguinte, na medida em que se refira ao SIS II Central, o presente plano de segurança caduca quando a autoridade de gestão assumir as suas funções.

(7) Nos termos do artigo 4.º, n.º 3, do Regulamento (CE) n.º 1987/2006 e do artigo 4.º, n.º 3, da Decisão 2007/533/JAI, o CS-SIS, com funções de supervisão técnica e administração, está sedeado em Estrasburgo (França) e o CS-SIS de salvaguarda, capaz de assegurar todas as funcionalidades do CS-SIS principal em caso de falha deste último, está sedeado em Sankt Johann im Pongau (Áustria).

(8) O plano de segurança deve incluir um responsável pela segurança do sistema, que realiza tarefas relativas à segurança do SIS II Central e da infra-estrutura de comunicação e dois responsáveis locais pela segurança que realizam, respectivamente, tarefas relativas à segurança do SIS II Central e da infra-estrutura de comunicação. Devem ser definidos os papéis dos responsáveis pela segurança a fim de assegurar uma resposta rápida e eficiente a quaisquer incidentes e que estes são objecto de relatórios.

(9) Deve ser criada uma política de segurança que descreva todos os dados técnicos e organizacionais em conformidade com as disposições da presente decisão.

(10) Devem ser tomadas medidas para assegurar o nível de segurança adequado para o funcionamento do SIS II Central e da infra-estrutura de comunicação,

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

ADOPTOU A PRESENTE DECISÃO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objecto

1. A presente decisão estabelece a organização e medidas de segurança (plano de segurança) para a protecção do SIS II Central e dos dados aí tratados contra ameaças à sua disponibilidade, integridade e confidencialidade na acepção do artigo 16.º, n.º 1, do Regulamento (CE) n.º 1987/2006 e do artigo 16.º, n.º 1, da Decisão 2007/533/JAI relativa ao estabelecimento, funcionamento e utilização do Sistema de Informação de Schengen de segunda geração (SIS II) durante o período transitório até a autoridade de gestão assumir funções.

2. A presente decisão estabelece a organização e medidas de segurança (plano de segurança) para a protecção da infra-estrutura de comunicação contra ameaças à sua disponibilidade, integridade e confidencialidade na acepção do artigo 16.º do Regulamento (CE) n.º 1987/2006 e do artigo 16.º da Decisão 2007/533/JAI relativa ao estabelecimento, funcionamento e utilização do Sistema de Informação de Schengen de segunda geração (SIS II).

CAPÍTULO II

ORGANIZAÇÃO, RESPONSABILIDADES E GESTÃO DE INCIDENTES

Artigo 2.º

Tarefas da Comissão

1. A Comissão aplica e controla a eficácia das medidas de segurança para o SIS II Central referido na presente decisão.

2. A Comissão aplica e controla a eficácia das medidas de segurança para a infra-estrutura de comunicação referida na presente decisão.

3. A Comissão designa, de entre os seus funcionários, um responsável pela segurança do sistema. O responsável pela segurança do sistema é nomeado pelo director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança da Comissão. As tarefas do responsável pela segurança do sistema incluem, em especial:

a) Preparar a política de segurança, conforme descrita no artigo 7.º da presente decisão;

b) Controlar a eficácia da aplicação dos procedimentos de segurança do SIS II Central;

c) Controlar a eficácia da aplicação dos procedimentos de segurança da infra-estrutura de comunicação;

d) Contribuir para a elaboração do relatório de segurança referido no artigo 50.º do Regulamento (CE) n.º 1987/2006 e no artigo 66.º da Decisão 2007/533/JAI;

e) Executar tarefas de coordenação e assistência nas verificações e auditorias realizadas pela Autoridade Europeia para a Protecção de Dados referidas no artigo 45.º do Regulamento (CE) n.º 1987/2006 e no artigo 61.º da Decisão 2007/533/JAI, bem como comunicar os incidentes na acepção do artigo 5.º, n.º 2, ao responsável pela protecção dos dados da Comissão;

f) Verificar se a presente decisão e a política de segurança são correcta e integralmente aplicadas pelos contratantes, incluindo subcontratantes, que estejam por qualquer forma implicados na gestão do SIS II Central;

g) Verificar se a presente decisão e a política de segurança são correcta e integralmente aplicadas pelos contratantes, incluindo subcontratantes, que estejam por qualquer forma implicados na gestão da infra-estrutura de comunicação;

h) Manter uma lista dos pontos de contacto nacionais únicos para segurança do SIS II e partilhá-la com o responsável local pela segurança da infra-estrutura de comunicação;

i) Partilhar a lista referida na alínea h) com o responsável local pela segurança do SIS II Central.

Artigo 3.º

Responsável local pela segurança do SIS II Central

1. Sem prejuízo do disposto no artigo 8.º, a Comissão designa, de entre os seus funcionários, um responsável local pela segurança do SIS II Central. Devem ser evitados quaisquer conflitos de interesses entre as funções de responsável local pela segurança e quaisquer outras funções oficiais. O responsável local pela segurança do SIS II Central é nomeado pelo director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança da Comissão.

2. O responsável local pela segurança do SIS II Central assegura que as medidas de segurança referidas na presente decisão são aplicadas e que os procedimentos de segurança são respeitados no CS-SIS principal. No que diz respeito ao CS-SIS de salvaguarda, o responsável local pela segurança do SIS II Central assegura que as medidas de segurança referidas na presente decisão são aplicadas, com excepção das referidas no artigo 9.º, e que os respectivos procedimentos de segurança são respeitados.

3. O responsável local pela segurança do SIS II Central pode delegar algumas das suas tarefas no pessoal subordinado. Devem ser evitados quaisquer conflitos de interesses entre as funções inerentes à execução destas tarefas e quaisquer outras funções oficiais. Através de um número de telefone e endereço de contacto único, será possível contactar a qualquer momento o responsável local pela segurança ou o seu subordinado de serviço.

4. O responsável local pela segurança do SIS II Central executa as tarefas inerentes às medidas de segurança a adoptar nos locais onde o CS-SIS principal e o CS-SIS de salvaguarda estão localizados nos termos do n.º 1, incluindo, em especial:

a) Realizar as tarefas operacionais de segurança local, incluindo auditorias à barreira de segurança (*firewall*), testes regulares de segurança, auditorias e relatórios;

b) Verificar a eficácia do plano de continuidade das actividades e assegurar a realização de exercícios regulares;

c) Recolher elementos de prova e comunicar ao responsável pela segurança do sistema qualquer incidente que possa ter impacto na segurança do SIS II Central ou da infra-estrutura de comunicação;

d) Informar o responsável pela segurança do sistema no caso de a política de segurança dever ser alterada;

e) Verificar se a presente decisão e a política de segurança são aplicadas pelos contratantes, incluindo subcontratantes, que estejam por qualquer forma implicados na gestão operacional do SIS II Central;

f) Assegurar que o pessoal está consciente das suas obrigações e verificar a aplicação da política de segurança;

g) Acompanhar os desenvolvimentos em matéria de segurança das TI e assegurar que o pessoal dispõe da formação adequada;

h) Preparar a informação e opções subjacentes à definição, actualização e revisão da política de segurança nos termos do artigo 7.º.

Artigo 4.º

Responsável local pela segurança da infra-estrutura de comunicação

1. Sem prejuízo do disposto no artigo 8.º, a Comissão designa, de entre os seus funcionários, um responsável local pela segurança da infra-estrutura de comunicação. Devem ser evitados quaisquer conflitos de interesses entre as funções de responsável local pela segurança e quaisquer outras funções oficiais. O responsável local pela segurança da infra-estrutura de comunicação é nomeado pelo director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança da Comissão.

2. O responsável local pela segurança da infra-estrutura de comunicação verifica o funcionamento da infra-estrutura de comunicação e assegura que as medidas de segurança são aplicadas e que os procedimentos de segurança são respeitados.

3. O responsável local pela segurança da infra-estrutura de comunicação pode delegar algumas das suas tarefas no pessoal subordinado. Devem ser evitados quaisquer conflitos de interesses entre as funções inerentes à execução destas tarefas e quaisquer outras funções oficiais. Através de um número de telefone e endereço de contacto único, será possível contactar a qualquer momento o responsável local pela segurança ou o seu subordinado de serviço.

4. O responsável local pela segurança da infra-estrutura de comunicação executa as tarefas inerentes às medidas de segurança relativas à infra-estrutura de comunicação, incluindo, em especial:

a) Realizar todas as tarefas operacionais de segurança relativas à infra-estrutura de comunicação, incluindo auditorias à barreira de segurança (*firewall*), testes regulares de segurança, auditorias e relatórios;

b) Verificar a eficácia do plano de continuidade das actividades e assegurar a realização de exercícios regulares;

c) Recolher elementos de prova e comunicar ao responsável pela segurança do sistema qualquer incidente ocorrido na infra-estrutura de comunicação que possa ter impacto na segurança do SIS II Central ou da infra-estrutura de comunicação;

d) Informar o responsável pela segurança do sistema no caso de a política de segurança dever ser alterada;

e) Verificar se a presente decisão e a política de segurança são aplicadas pelos contratantes, incluindo subcontratantes, que estejam por qualquer forma implicados na gestão da infra-estrutura de comunicação;

f) Assegurar que o pessoal está consciente das suas obrigações e acompanhar a aplicação da política de segurança;

g) Acompanhar os desenvolvimentos em matéria de segurança das TI e assegurar que o pessoal dispõe da formação adequada;

h) Preparar a informação e opções subjacentes à definição, actualização e revisão da política de segurança nos termos do artigo 7.º.

Artigo 5.º

Incidentes de segurança

1. Qualquer acontecimento que tenha ou possa ter impacto na segurança do SIS II e que possa causar-lhe danos é considerado um incidente de segurança, nomeadamente quando possa ter havido acesso aos dados ou quando a disponibilidade, integridade e confidencialidade dos dados tenha ou possa ter sido posta em causa.

2. Os incidentes de segurança são geridos por forma a assegurar uma resposta rápida, eficaz e adequada, em conformidade com a política de segurança. Devem ser definidos procedimentos de recuperação em caso de incidente.

3. As informações relativas a um incidente de segurança que tenha ou possa ter impacto no funcionamento do SIS II num Estado-Membro ou na disponibilidade, integridade e confidencialidade dos dados registados ou enviados por um Estado-Membro são facultadas ao Estado-Membro em causa. Os incidentes de segurança são comunicados ao responsável pela protecção de dados da Comissão.

Artigo 6.º

Gestão de incidentes

1. Todos os membros do pessoal e contratantes envolvidos no desenvolvimento, gestão ou funcionamento do SIS II devem registar e comunicar ao responsável pela segurança do sistema ou ao responsável local pela segurança da infra-estrutura de comunicação quaisquer constatações ou suspeitas de problemas de segurança na infra-estrutura de comunicação.

2. Caso detecte qualquer incidente que tenha ou possa ter impacto na segurança do SIS II, o responsável local pela segurança da infra-estrutura de comunicação deve informar o mais rapidamente possível o responsável pela segurança do sistema e, se necessário, o ponto de contacto nacional único para segurança do SIS II, quando este existir no Estado-Membro em questão, devendo fazê-lo por escrito ou, em caso de extrema urgência, através de outros canais de comunicação. O relatório deve conter a descrição do incidente de segurança, o nível de risco, as eventuais consequências e as medidas que foram ou devem ser adoptadas para atenuar o risco.

3. Quaisquer elementos relativos ao incidente de segurança são imediatamente salvaguardados pelo responsável local pela segurança da infra-estrutura de comunicação. Na medida do possível, nos termos das disposições aplicáveis à protecção dos dados, esses elementos são disponibilizados ao responsável pela segurança do sistema, a seu pedido.

4. Os procedimentos de comunicação são definidos na política de segurança para assegurar que a informação sobre o tipo, solução e resultado de um incidente de segurança é comunicada ao responsável pela segurança do sistema e ao responsável local pela segurança da infra-estrutura de comunicação, quando o incidente tiver sido tratado e terminado.

5. Os n.os 1 a 4 aplicam-se *mutatis mutandis* aos incidentes do SIS II Central. Nesse caso, as referências ao responsável local pela segurança da infra-estrutura de comunicação nos n.os 1 a 4 devem ser entendidas como referências ao responsável pela segurança do SIS II Central.

CAPÍTULO III

MEDIDAS DE SEGURANÇA

Artigo 7.º

Política de segurança

1. O director-geral da Direcção-Geral da Justiça, da Liberdade e da Segurança estabelece, actualiza e revê regularmente uma política de segurança vinculativa, em conformidade com a presente decisão. A política de segurança prevê, de forma pormenorizada, os procedimentos e medidas de protecção contra ameaças à disponibilidade, integridade e confidencialidade da infra-estrutura de comunicação, incluindo um plano de emergência, a fim de assegurar o nível adequado de segurança, conforme previsto na presente decisão. A política de segurança deve respeitar a presente decisão.

2. A política de segurança é baseada numa avaliação dos riscos. As medidas descritas na política de segurança devem ser proporcionais aos riscos identificados.

3. A avaliação dos riscos e da política de segurança serão actualizadas sempre que a evolução tecnológica, a identificação de novas ameaças ou quaisquer outras circunstâncias o tornem necessário. Em todo o caso, a política de segurança é revista numa base anual, para assegurar que continua a responder adequadamente à última avaliação dos riscos, a quaisquer outras evoluções tecnológicas ou ameaças recentemente identificadas ou a outras circunstâncias relevantes.

4. A política de segurança é elaborada pelo responsável pela segurança do sistema, em coordenação com o responsável local pela segurança do SIS II Central e o responsável local pela infra-estrutura de comunicação.

5. Os n.os 1 a 4 aplicam-se *mutatis mutandis* à política de segurança do SIS II Central. Nesse caso, qualquer referência ao responsável local pela segurança da infra-estrutura de comunicação nos n.os 1 a 4 deve ser entendida como referência ao responsável pela segurança do SIS II Central.

Artigo 8.º

Aplicação das medidas de segurança

1. A realização das tarefas e a aplicação dos requisitos estabelecidos na presente decisão e na política de segurança, incluindo a tarefa de designar um responsável local pela segurança, pode ser objecto de subcontratação ou confiada a organismos privados ou públicos.

2. Neste caso, a Comissão deve assegurar, através de acordos juridicamente vinculativos, que os requisitos estabelecidos na presente decisão e na política de segurança são integralmente respeitados. Em caso de delegação ou subcontratação da tarefa de designar um responsável local pela segurança, a Comissão deve assegurar, através de acordos juridicamente vinculativos, que será consultada relativamente à pessoa a designar para esta função.

Artigo 9.º

Controlo de acesso às instalações

1. Devem ser utilizados perímetros de segurança com barreiras e controlos de entrada adequados para proteger as instalações onde se realiza o tratamento de dados.

2. Dentro dos perímetros de segurança devem ser definidas áreas seguras para proteger os componentes físicos (bens), incluindo o equipamento informático, os suportes de dados e consolas, os planos e outros documentos sobre o SIS II, bem como os gabinetes e outros locais de trabalho do pessoal envolvido no funcionamento do SIS II. Estas áreas seguras devem ser protegidas por controlos de entrada adequados, para assegurar que só o pessoal autorizado pode ter acesso. O trabalho nas áreas seguras deve estar sujeito a regras de segurança pormenorizadas estabelecidas na política de segurança.

3. Deve ser prevista e instalada a segurança física dos gabinetes, salas e instalações. Os pontos de acesso, como as áreas de cargas e descargas e outros pontos onde possam entrar nas instalações pessoas não autorizadas, devem ser controlados e, se possível, isolados das instalações de tratamento dos dados, para evitar o acesso não autorizado.

4. Deve ser concebida uma protecção física dos perímetros de segurança contra danos resultantes de catástrofes naturais ou de origem humana e aplicada proporcionalmente ao respectivo risco.

5. O equipamento deve ser protegido contra as ameaças físicas e ambientais, bem como contra a possibilidade de acesso não autorizado.

6. Se a Comissão dispuser de tal informação, deve acrescentar à lista referida no artigo 2.º, n.º 3, alínea h), um ponto de contacto único para acompanhar a aplicação do disposto no presente artigo nas instalações onde está localizado o CS-SIS de salvaguarda.

Artigo 10.º

Suportes de dados e controlo dos bens

1. Os suportes móveis que contenham dados devem ser protegidos contra acessos não autorizados, utilização indevida ou corrupção dos dados, devendo a sua legibilidade ser assegurada ao longo de toda a vida útil dos dados.

2. Quando já não forem necessários, os suportes devem ser eliminados de forma segura, segundo os procedimentos pormenorizados estabelecidos na política de segurança.

3. Devem estar disponíveis inventários com informação sobre a localização dos dados arquivados, o período de conservação aplicável e as autorizações de acesso.

4. Todos os elementos importantes da infra-estrutura de comunicação devem ser identificados, para que possam ser protegidos de acordo com a sua importância. Deve ser mantido um registo actualizado do equipamento informático relevante.

5. A documentação actualizada relativa à infra-estrutura de comunicação deve estar disponível. Esta documentação deve ser protegida contra acessos não autorizados.

6. Os n.os 1 a 5 aplicam-se *mutatis mutandis* aos incidentes do SIS II Central. Nesse caso, as referências à infra-estrutura de comunicação devem ser entendidas como referências ao SIS II Central.

Artigo 11.º

Controlo do armazenamento

1. São tomadas medidas adequadas para assegurar o armazenamento adequado dos dados e a sua protecção contra acessos não autorizados.

2. Todos os equipamentos que contenham suportes de armazenamento devem ser verificados, para assegurar que os dados sensíveis foram retirados ou integralmente apagados antes da sua eliminação, ou são destruídos de forma segura.

Artigo 12.º

Controlo de palavras-passe

1. Todas as palavras-passe são mantidas em segurança e tratadas confidencialmente. Quando haja suspeitas de que uma palavra-passe foi divulgada, esta deve ser imediatamente alterada ou a conta em questão desactivada. Os nomes de utilizador devem ser únicos e individuais.

2. Os procedimentos para iniciar e terminar uma sessão são definidos na política de segurança para impedir quaisquer acessos não autorizados.

Artigo 13.º

Controlo de acessos

1. A política de segurança estabelece um procedimento de registo e supressão do registo do pessoal em actividade, destinado a conceder e revogar o acesso ao equipamento e ao *software* do SIS II para efeitos de gestão operacional. A atribuição e utilização de credenciais de acesso (palavras-passe ou outros meios adequados) são controladas através de um processo de gestão formal, em conformidade com a política de segurança.

2. O acesso ao equipamento e ao *software* do SIS II no CS-SIS deve:

i) Ser limitado às pessoas autorizadas;

ii) Ser limitado aos casos em que possa ser identificado um objectivo legítimo em conformidade com o artigo 45.º do Regulamento (CE) n.º 1987/2006 e o artigo 61.º da Decisão 2007/533/JAI, ou com o artigo 50.º, n.º 2, do Regulamento (CE) n.º 1987/2006 e o do artigo 66.º, n.º 2, da Decisão 2007/533/JAI;

iii) Não exceder a duração e âmbito necessários ao objectivo do acesso; e

iv) Ter lugar apenas nos termos da política de controlo de acesso a definir na política de segurança.

3. Só as consolas e *software* autorizados pelo responsável local pela segurança do SIS II Central podem ser utilizados no CS-SIS. A utilização de funções do sistema susceptíveis de ultrapassar os controlos do sistema e das aplicações é restringida e controlada. Devem ser criados procedimentos de controlo da instalação de *software*.

Artigo 14.º

Controlo da comunicação

A infra-estrutura de comunicação deve ser verificada a fim de assegurar a disponibilidade, integridade e confidencialidade das trocas de informações. Devem ser utilizados meios criptográficos para proteger os dados transmitidos através da infra-estrutura de comunicação.

Artigo 15.º

Controlo do registo de dados

As contas das pessoas autorizadas a aceder ao *software* do SIS II a partir do CS-SIS são controladas pelo responsável local pela segurança do SIS II Central. A utilização dessas contas, incluindo o tempo e a identidade do utilizador, é registada.

Artigo 16.º

Controlo do transporte

1. São definidas medidas adequadas na política de segurança para impedir a leitura, cópia, alteração ou supressão não autorizada dos dados pessoais durante a transmissão de ou para o SIS II ou durante o transporte dos suportes de dados. A política de segurança deve incluir disposições sobre os tipos admissíveis de envio ou transporte, bem como sobre os procedimentos de responsabilização pelo transporte desses elementos e pela sua chegada ao local de destino. Os suportes de dados não devem conter quaisquer dados para além dos que devem ser enviados.

2. Os serviços prestados por terceiros que impliquem o acesso, tratamento, comunicação ou gestão das instalações de tratamento de dados ou o fornecimento de bens ou serviços a essas instalações devem incluir controlos de segurança integrados adequados.

Artigo 17.º

Segurança da infra-estrutura de comunicação

1. A infra-estrutura de comunicação deve ser gerida e controlada adequadamente, a fim de a proteger contra as ameaças e garantir a segurança da própria infra-estrutura de comunicação e do SIS II Central, incluindo dos dados transmitidos por essa via.

2. As características de segurança, os níveis de serviço e os requisitos de gestão de todos os serviços de rede devem ser identificados no acordo de serviços de rede com o fornecedor de serviços.

3. Além da protecção dos pontos de acesso ao SIS II, qualquer serviço adicional utilizado pela infra-estrutura de comunicação deve igualmente ser protegido. As medidas adequadas são definidas na política de segurança.

Artigo 18.º

Acompanhamento

1. Os registos da informação referida no artigo 18.º, n.º 1, do Regulamento (CE) n.º 1987/2006 e no artigo 18.º, n.º 1, da Decisão 2007/533/JAI relativa a todos os acessos e trocas de dados pessoais no CS-SIS, são conservados em segurança e estão acessíveis nas instalações onde estão localizados os CS-SIS principal e de salvaguarda durante o período referido no artigo 18.º, n.º 3, do Regulamento (CE) n.º 1987/2006 e no artigo 18.º, n.º 3, da Decisão 2007/533/JAI.

2. Os procedimentos de controlo da utilização das instalações de tratamento de informação ou das suas deficiências são definidos na política de segurança e os resultados das actividades de controlo são revistos regularmente. Se necessário, são tomadas as medidas adequadas.

3. Os registos e respectivos suportes são protegidos contra a manipulação indevida e o acesso não autorizado, para respeitarem os requisitos relativos à recolha e ao período de conservação dos dados.

Artigo 19.º

Medidas criptográficas

São utilizadas medidas criptográficas adequadas para a protecção da informação. A sua utilização, objectivos e condições devem ser previamente aprovados pelo responsável pela segurança do sistema.

CAPÍTULO IV

SEGURANÇA DOS RECURSOS HUMANOS

Artigo 20.º

Perfis dos membros do pessoal

1. A política de segurança define as funções e responsabilidades das pessoas autorizadas a aceder ao SIS II Central.

2. A política de segurança define as funções e responsabilidades de pessoas autorizadas a aceder à infra-estrutura de comunicação.

3. Os papéis e responsabilidades a nível de segurança do pessoal da Comissão, dos contratantes e do pessoal implicado na gestão operacional são definidos, registados e comunicados às pessoas em causa. A descrição das funções e os objectivos definem os papéis e responsabilidades do pessoal da Comissão, sendo os mesmos definidos nos contratos ou acordos de nível de serviço quanto aos contratantes.

4. São celebrados acordos de confidencialidade e sigilo com todas as pessoas não abrangidas pelas regras da função pública da União Europeia ou dos Estados-Membros. O pessoal que trabalhe com dados do SIS II deve ter a necessária autorização ou certificação, em conformidade com os procedimentos pormenorizados a estabelecer na política de segurança.

Artigo 21.º

Informação ao pessoal

1. Todos os membros do pessoal e os contratantes recebem formação adequada sobre segurança, requisitos legais, políticas e procedimentos, na medida em que as suas funções o exijam.

2. Relativamente à cessação da relação laboral ou do contrato, a política de segurança define as responsabilidades do pessoal e dos contratantes inerentes à mudança de funções ou à cessação de emprego, bem como os procedimentos para gerir a devolução dos bens e a supressão dos direitos de acesso.

CAPÍTULO V

DISPOSIÇÃO FINAL

Artigo 22.º

Aplicabilidade

1. A presente decisão é aplicável a partir da data fixada pelo Conselho nos termos do artigo 55.º, n.º 2, do Regulamento (CE) n.º 1987/2006 e do artigo 71.º, n.º 2, da Decisão 2007/533/JAI.

2. Os artigos 1.º, n.º 1, 2.º, n.º 1, 2.º n.º 3, alíneas b), d), f) e i), 3.º, 6.º, n.º 5, 7.º, n.º 5, 9.º, n.º 6, 10.º, n.º 6, 13.º, n.ºs 2 e 3, 15.º, 18.º e 20.º, n.º 1, caducam quando a autoridade de gestão assumir funções.

Feito em Bruxelas, em 4 de Maio de 2010.

Pela Comissão

O Presidente

José Manuel BARROSO