PT

CONSELHO DA
UNIÃO EUROPEIA

SECRETARIADO-GERAL

DG H

UE
Inventário Schengen

Volume 2

Sistema de Informação de Schengen , Sirene: recomendações e melhores práticas

Dezembro 2002

UE
Inventário Schengen

Volume 2

Sistema de Informação de Schengen , Sirene: recomendações e melhores práticas

Dezembro 2002

ÍNDICE

Prefácio da Presidência Dinamarquesa

Em conformidade com uma decisão do Conselho tomada em 28 de Maio de 2001, o Grupo de Avaliação de Schengen iniciou a redacção de um inventário de recomendações para a aplicação correcta do acervo de Schengen.

O objectivo do Inventário é clarificar e aprofundar o acervo de Schengen e apresentar recomendações e exemplos de melhores práticas, para proporcionar um exemplo aos Estados que venham a aderir a Schengen, bem como aos Estados que já aplicam plenamente o acervo de Schengen. Não se trata de definir de maneira exaustiva todo o acervo de Schengen, mas de apresentar recomendações e exemplos de melhores práticas à luz da experiência adquirida na avaliação contínua da correcta aplicação do acervo nos Estados Schengen.

O primeiro volume do Inventário diz respeito às fronteiras externas e aos procedimentos de afastamento e de readmissão, tendo sido aprovado e apresentado aos países candidatos no Conselho de 28 de Fevereiro de 2002.

A Dinamarca, que assume a Presidência da União Europeia desde 1 de Julho de 2002, considera que é muito importante continuar a redigir o Inventário. Durante a Presidência dinamarquesa foi elaborado um segundo volume do Inventário. Este trata do Sistema de Informação de Schengen e da aplicação do Manual SIRENE.

A Presidência dinamarquesa agradece aos Estados Schengen e à Comissão todo o apoio e cooperação dados no âmbito da elaboração do Inventário e muito especialmente à Noruega que preside ao Comité Misto, pela ajuda facultada à Presidência Dinamarquesa ao presidir o subgrupo responsável pela redacção do Inventário.

O Inventário foi elaborado com o objectivo de prestar esclarecimento, não sendo juridicamente vinculativo. Colige, em duas colunas, por um lado, os níveis exigíveis para cumprir o acervo e, por outro, as melhores práticas que têm sido registadas em alguns dos Estados-Membros.

O Inventário será apresentado aos países que aderirem à UE e aos países candidatos. A Presidência Dinamarquesa ousa esperar que o Inventário venha a constituir mais um instrumento útil para garantir o êxito da integração atempada e adequada dos novos parceiros na União Europeia.

Dezembro de 2002

INVENTÁRIO SCHENGEN

INTRODUÇÃO

1. Na sua sessão de 28 de Maio de 2001, o Conselho definiu como objectivo para a continuação dos trabalhos do Grupo de Avaliação de Schengen "… destacar as melhores práticas, designadamente em matéria de controlo nas fronteiras, de modo a constituírem exemplos para os Estados que venham a aderir a Schengen, mas também para os Estados que já aplicam plenamente o acervo de Schengen. Essas avaliações e a identificação das melhores práticas servirão para inspirar a elaboração de normas para definir o nível mínimo de aplicação do acervo de Schengen (...) nos grupos competentes" (mandato conferido ao Grupo de Avaliação de Schengen, ver doc. 8881/01 – SCH–EVAL 17, COMIX 371).

   Com base neste mandato, o Grupo de Avaliação de Schengen desenvolveu os princípios e os procedimentos com vista à elaboração de um inventário de recomendações para a aplicação correcta do acervo de Schengen e melhores práticas, a seguir designado por Inventário de Recomendações e Melhores Práticas, ou Inventário.

   É objectivo do Inventário clarificar e aprofundar o acervo de Schengen, fazer recomendações e indicar melhores práticas, que possam servir de exemplo para os Estados aderentes a Schengen, mas também para os que aplicam plenamente esse acervo. Nesta óptica, o Inventário proporciona aos países candidatos à adesão à União Europeia (a seguir designada por UE), (a pedido dos mesmos), uma boa indicação sobre o que deles se espera, nomeadamente na prática, em matéria de Schengen. Não se visa definir de maneira exaustiva todo o acervo de Schengen, mas apresentar as recomendações e as melhores práticas, com base na experiência adquirida pelo Grupo de Avaliação de Schengen ao verificar a correcta aplicação do acervo de Schengen.

   O texto do Inventário não pretende introduzir novas exigências, mas antes chamar também a atenção do Conselho para a necessidade de eventualmente alterar algumas disposições do acervo de Schengen de forma a que a Comissão e, se for caso disso, os Estados-Membros tenham em conta as recomendações e melhores práticas ao apresentar propostas ou iniciativas formais. O exercício corresponde, nomeadamente, à primeira fase do processo que visa a definição de padrões mínimos pelo Conselho.

Acresce que o Inventário servirá de instrumento de referência nas futuras avaliações a efectuar nos países candidatos, servindo pois também como indicador das tarefas a atribuir--lhes, pelo que deve, a este respeito, ser lido em cotejo com o Manual SIRENE.

2. O Grupo de Avaliação de Schengen aprovou as seguintes definições para a realização do exercício:

Recomendações: conjunto não exaustivo de medidas que deverá permitir estabelecer a base da aplicação correcta do acervo de Schengen, e bem assim velar por essa mesma aplicação correcta.

Melhores práticas: conjunto não exaustivo de métodos de trabalho ou de medidas–modelo que deverão ser consideradas como as melhores para a aplicação do acervo de Schengen, ficando entendido que podem existir vários tipos de melhores práticas para cada parte específica da cooperação de Schengen.

3. Nos casos em que o Inventário refere os Estados-Membros que aplicam o acervo de Schengen, entende-se que se trata actualmente dos treze Estados-Membros da UE, indicados no artigo 1.º do Protocolo que integra o acervo de Schengen no âmbito da UE, anexo ao Tratado da União Europeia e ao Tratado que institui a Comunidade Europeia (a seguir designado por "Protocolo de Schengen"), a que se somam a Islândia e a Noruega, nos termos do Acordo celebrado pelo Conselho da União Europeia, a República da Islândia e o Reino da Noruega relativo à Associação destes Estados à Execução, à Aplicação e ao Desenvolvimento do Acervo de Schengen, assinado a 18 de Maio de 1999 (estes quinze Estados são a seguir designados por "Estados Schengen").

O Reino Unido e a Irlanda formularam o desejo de participar em certas disposições do acervo de Schengen. As modalidades de participação do Reino Unido foram adoptadas na decisão do Conselho de 29 de Maio de 2000 (2000/365/CE) e as da Irlanda na decisão do Conselho de 28 de Fevereiro de 2002 (2002/192/CE). O Conselho ainda não decidiu sobre a aplicação dessas disposições.

O acervo de Schengen e as outras medidas tomadas pelas instituições no seu âmbito de aplicação são considerados, nos termos do artigo 8.º do Protocolo de Schengen, como um acervo que deve ser integralmente aceite por todos os Estados candidatos à adesão.

4. O acervo de Schengen foi integrado no âmbito da UE pelo Protocolo de Schengen. A extensão do acervo integrado na União Europeia está definida na Decisão do Conselho 1999/435/CE, publicada no JO L 176, de 10 de Julho de 1999.

   Desde a sua integração na UE, o acervo de Schengen tem aumentado e tem sido alterado, o que lhe confere um carácter evolutivo.

   O acervo de Schengen foi também enriquecido com os resultados das avaliações efectuadas no âmbito da Comissão Permanente de Aplicação e Avaliação do Acervo de Schengen, que actualmente se chama "Grupo de Trabalho da Avaliação de Schengen". Nos termos do mandato deste grupo, são apresentados relatórios ao Conselho a fim de verificar se estão reunidas as condições necessárias para a entrada em vigor das disposições do acervo de Schengen num Estado que deseje participar nessas disposições (ou em algumas delas) e, por outro lado, controlar a correcta aplicação do acervo de Schengen pelos Estados Schengen, nomeadamente detectando problemas e propondo soluções.

5. O primeiro volume do Inventário, que foi distribuído aos países candidatos no Conselho de 28 de Fevereiro de 2002, aborda essencialmente a questão das fronteiras e do afastamento. O segundo volume actual é consagrado ao Sistema de Informação de Schengen, nomeadamente à aplicação do Manual SIRENE. A livre circulação no interior do território dos Estados Schengen é uma liberdade que exige como contrapartida não apenas o reforço das fronteiras externas comuns e uma política eficaz e dissuasiva de afastamento dos nacionais de países terceiros em situação irregular, mas também o intercâmbio rápido e eficiente de informações, no âmbito dos controlos nas fronteiras e da cooperação policial. Por conseguinte, as medidas adoptadas neste quadro visam reforçar a integração europeia e, em especial, dar à UE a possibilidade de mais rapidamente se tornar num espaço de liberdade, de segurança e de justiça.

6. O Inventário actual inclui um capítulo consagrado ao SIS/SIRENE. Na parte "Generalidades", descrevem-se sucintamente os conceitos fundamentais subjacentes às recomendações e às melhores práticas, apresentadas sob forma de quadro, com as recomendações à esquerda e as melhores práticas à direita, em face das correspondentes recomendações.

* * *

PARTE III: SISTEMA DE INFORMAÇÃO DE SCHENGEN

RECOMENDAÇÕES E MELHORES PRÁTICAS NA ESPECIFICIDADE

GENERALIDADES

A lista de recomendações e melhores práticas que seguidamente se apresenta foi compilada essencialmente com base nos resultados das diversas avaliações efectuadas durante os últimos anos, tanto as avaliações do SIS nos vários países como as avaliações mais específicas do SIRENE.

O presente inventário foi elaborado independentemente do seu sistema técnico, ou seja, o SIS 1 + ou SIS II e destina-se sobretudo a ser utilizado na criação de bases de dados nacionais que, por seu turno, fornecerão informações ao SIS, assim como na preparação da secção nacional do SIS, seja qual for a forma assumida na arquitectura do SIS II.

De qualquer modo, recorda-se que, sempre que os utilizadores dos sistemas de TI de Schengen tratarem informações classificadas da UE, é aplicável a Decisão do Conselho 2001/264/CE que aprova as regras de segurança do Conselho (JO n.º L 101 de 11.04.2001, p. 1)

Quanto à introdução de indicações no SIS, o princípio de base que lhe está subjacente é de que se deve procurar um equilíbrio entre introduzir o maior número possível de indicações no SIS, nos termos do disposto na Convenção, e garantir que essas indicações sejam de boa qualidade, condições essenciais da eficiência e utilidade do SIS. Todas as indicações nacionais relacionadas com Schengen deverão, em princípio, ser introduzidas no SIS mas, para que se lhe possa dar execução, a indicação deverá ser correcta, tão completa quanto possível e de proveniência conhecida. Por último, é de ter presente que, quando um Estado Schengen dá execução a uma indicação, tem o direito de esperar que o Estado Schengen de emissão dê seguimento a essa resposta positiva. Se não o fizer sem uma justificação (jurídica) válida, isso terá um impacto negativo na predisposição das autoridades (locais) para utilizarem o SIS e explorarem todo o seu potencial.

O papel dos SIRENE no funcionamento do SIS é absolutamente essencial. Embora não se espere, nem seja necessário, que os SIRENE assumam a responsabilidade por toda e qualquer acção relacionada com o SIS, pode-se considerar que os SIRENE são a interface humana do SIS, o que significa que são o contacto de primeira linha, tanto para os outros Gabinetes SIRENE como para as autoridades nacionais e utilizadores finais. Conforme os casos, os SIRENE deverão estar preparados para os resolverem autonomamente ou para os remeterem para as autoridades ou serviços competentes. O pessoal dos SIRENE deverá, pois, ser competente e devidamente formado e ter boas relações com as autoridades nacionais e estrangeiras.

RECOMENDAÇÕES/MELHORES PRÁTICAS

RECOMENDAÇÕES	MELHORES PRÁTICAS
1. Secção nacional do SIS	
1.1 Sistemas e organização	
– Deverá ser criada uma secção nacional para o SIS que assegure um funcionamento permanente (24 horas por dia, 7 dias por semana) contando com suficiente apoio técnico a todo o momento – Garantir a integridade dos dados entre os N.SIS e quaisquer cópias técnicas nacionais, quando estas existam	– A fim de garantir o funcionamento 24 horas por dia, 7 dias por semana, deverão ser assumidos compromissos sobre o nível de manutenção e de qualidade do equipamento e do *software* – Sincronização em tempo real das cópias – Comparações regulares de bases de dados
1.2 Infra-estrutura de comunicação	
– Deverá existir uma rede nacional estável – Deverá ser garantido um tempo de resposta rápido às consultas – Os dados SIS disponíveis nos postos consulares têm de ser actualizados regularmente	– A fim de garantir uma grande disponibilidade da rede, deverão ser assumidos compromissos sobre o nível de manutenção e de qualidade do serviço – O tempo de resposta deverá ser inferior a 5 segundos – O ideal seria que os postos consulares tivessem acesso em linha aos dados pertinentes do SIS – Quando só está disponível o acesso *off-line*, as actualizações das bases de dados deverão ser enviadas de duas em duas semanas e deve-se proceder a um controlo telefónico adicional

RECOMENDAÇÕES	MELHORES PRÁTICAS
2. SIRENE	
2.1 Estrutura nacional	
– Deverá ser criado um SIRENE, que é designado como único ponto de contacto para cada Estado Schengen para as indicações SIS e o procedimento a seguir na sequência de uma resposta positiva – Deverá ser respeitado e aplicado o princípio de que as indicações Schengen prevalecem sobre as indicações Interpol	– O acesso a todos os serviços responsáveis pela cooperação policial internacional deverá ser feito através de um único ponto de contacto, deverá estar integrado na mesma estrutura de gestão e situado no mesmo local – A indicação Interpol deverá incluir uma nota para os Estados Schengen, indicando o número de identificação Schengen da indicação
2.2 Organização e sistema	
– O SIRENE deverá garantir a cobertura permanente da comunicação com todos os outros SIRENE e as autoridades nacionais	– Continuidade da gestão, aspectos técnicos e relativos ao pessoal
– Todo o pessoal, incluindo os que é destacado para trabalhar fora das horas de expediente, deverá ter competências e experiência para fornecer os serviços necessários aos outros SIRENE e tratar quaisquer indicações que dêem entrada	– Flexibilidade da organização do trabalho
– Além do pessoal administrativo e operacional, há uma clara necessidade de pessoal de apoio TI – Os SIRENE têm de estar equipados com um sistema eficaz e efectivo de gestão do fluxo de trabalho	– A fim de garantir um funcionamento permanente, deverão ser assumidos compromissos sobre o nível de manutenção e de qualidade do equipamento e do *software* – Os sistemas electrónicos de gestão do fluxo de trabalho e dos processos para os operadores SIRENE têm a vantagem de melhorar a qualidade do trabalho e reduzir o risco de erros

RECOMENDAÇÕES	MELHORES PRÁTICAS
	– O sistema de gestão electrónica do fluxo de trabalho e dos processos deverá interagir com a aplicação N.SIS e os sistemas nacionais no que respeita à gestão das indicações que entram e saem, o que inclui os avisos automáticos • de que foi aditado ou suprimido um marcador requerido • de quando se alterou uma indicação • da entrada de uma nova indicação nos termos do artigo 95.º
– Os SIRENE deverão ter a possibilidade de transmitir imagens rápida e eficazmente, como por exemplo fotografias e impressões digitais	– A fim de garantir a recepção de imagens utilizáveis, é preferível a sua transmissão electrónica – Para essa transmissão electrónica, deverá ser utilizada a norma ANSI/NIST–CLS 1–1993 ou as suas versões posteriores
2.3 Recrutamento e formação	
– Os SIRENE deverão dispor de mão-de-obra apta a funcionar por iniciativa própria, a fim de garantir que os casos sejam tratados com eficiência	– Deverá ser possível recorrer a um apoio à gestão, incluindo o acesso a serviços de consultoria jurídica ou outros serviços de especialistas fora do horário de expediente, a fim de permitir uma delegação de responsabilidades – Deverá ser dada especial atenção à gestão dos recursos humanos, tendo em vista garantir uma continuidade em termos de pessoal, o que constitui uma vantagem para a melhoria da qualidade do trabalho dos SIRENE – Dever-se-á criar um sistema de formação em matéria de gestão do fluxo de trabalho dos SIRENE
– Todos os operadores deverão possuir bons conhecimentos sobre questões jurídicas nacionais, sobre a execução das leis nacionais (incluindo um conhecimento teórico das actividades policiais), sobre os sistemas administrativos judiciais e de imigração nacionais e, no mínimo, conhecimentos básicos sobre questões jurídicas internacionais	

RECOMENDAÇÕES	MELHORES PRÁTICAS
– Deverão ser recrutadas pessoas com conhecimentos especializados a nível jurídico, bons conhecimentos sobre a legislação nacional e internacional, um conhecimento aprofundado da Convenção de Schengen e da respectiva regulamentação, bem como um conhecimento teórico das actividades policiais	– Os serviços jurídicos especializados podem ser prestados através do recrutamento a nível interno de consultores jurídicos ou da organização de cursos de formação jurídica para o pessoal dos SIRENE
– Será necessário recrutar pessoal com formação a nível de execução da lei, cuja experiência se tem revelado muito vantajosa e que contribui para reduzir o período de formação	
– Estabelecer normas e um entendimento comuns	
	– Formação comum, pelo menos uma vez por ano – Intercâmbio regular de operadores, a iniciar antes da utilização operacional do SIS
– Os níveis de recrutamento deverão ter em conta o número de indicações nacionais e a revisão dessas indicações no fim do seu período de validade, bem como o número de respostas positivas no território nacional	
– A estratégia de recrutamento dos SIRENE deverá prever a validação dos ficheiros do artigo 95.º, antes da utilização operacional do SIS	
– O pessoal existente deverá ter conhecimentos linguísticos suficientes	– Este deverá ser um aspecto crucial do recrutamento e da formação em exercício do pessoal SIRENE – O pessoal SIRENE deverá ter prioridade em matéria de formação linguística – O intercâmbio de formulários na língua do país de emissão e em inglês é a prática corrente

RECOMENDAÇÕES	MELHORES PRÁTICAS
– Para uma maior eficácia da comunicação bilateral, deverão ser utilizadas línguas conhecidas por ambas as partes	– É obviamente da maior conveniência à que os operadores tenham bons conhecimentos das línguas mais faladas, tendo em vista a comunicação directa e a capacidade de utilizar documentação, na falta de apoio a nível da tradução

RECOMENDAÇÕES	MELHORES PRÁTICAS
3. Utilizadores finais	
3.1 Consulta e interface utilizador	
– Será necessário proceder a consultas ou a investigações que vão além da concordância exacta	– Como por exemplo consultas fonéticas, consultas com caracteres polivalentes, consultas segundo uma lógica difusa (*fuzzy*) e "soundex"
– A consulta única dos sistemas nacional e internacional é o modo mais eficaz de garantir a consulta sistemática do SIS.	– Dever-se-á garantir que a legislação nacional não impeça essa consulta única – Dever-se-á garantir que a consulta única seja rápida e fácil
– É preferível o acesso directo	– A fim de possibilitar as consultas directas, os utilizadores finais deverão poder dispor do maior número possível de instrumentos de consulta de dados
– As informações relativas às indicações nacionais e internacionais deverão aparecer simultaneamente	
– O utilizador final deverá poder dispor no primeiro ecrã da informação de que a pessoa é considerada perigosa e/ou está armada	
– Ao inserir as indicações nacionais, a inserção da indicação no SIS deverá ser programada como uma função por defeito, a fim de evitar operações adicionais ao utilizador final	– As indicações deverão ser controladas previamente na base de dados nacional e daí transferidas para o N.SIS de forma automatizada
– Antes do carregamento inicial dos dados relativos às indicações nacionais para o SIS, deverá ser verificada a correcção e a relação com Schengen dos dados nacionais pré-existentes	
– Indicar claramente as informações e instruções sobre as operações que o utilizador final tem de realizar, em caso de resposta positiva	– Em caso de usurpação de identidade, mostrar claramente no ecrã o procedimento a seguir para o tratamento de uma resposta positiva relativa a uma usurpação de identidade e as investigações a realizar posteriormente para verificar se a pessoa é a vítima ou o autor da usurpação

RECOMENDAÇÕES	MELHORES PRÁTICAS
– As aplicações deverão ser desenvolvidas de modo a serem de utilização fácil, a fim de permitir a utilização de meios rápidos e eficazes para a realização das tarefas relativas ao SIS	– Sempre que necessário, a consulta do SIS poderia ser combinada com sistemas de consulta existentes – Ao inserir um nome durante uma consulta, o sistema deverá verificar tanto os dados relativos a pessoas como os dados relativos a documentos – A interface utilizador deverá permitir e favorecer a inserção em simultâneo do nome e, se for caso disso, do número do documento, e a aplicação deverá verificar ambos na mesma consulta
3.2 Formação	
– Garantir a sensibilização das partes interessadas no SIS: polícia e outros serviços (de execução da lei), magistrados e autoridades competentes para a investigação e o exercício da acção penal	– Prever a formação contínua das partes interessadas – Colocar um sistema de formação à disposição dos utilizadores finais – Assegurar um contacto estreito entre as partes interessadas e os SIRENE, através de agentes de ligação – Promover a sensibilização através dos grupos de trabalho competentes (cooperação policial, controlo fronteiriço, Grupo Operacional dos Chefes das Polícias, cooperação judicial, terrorismo) ou através da CEPOL – As autoridades responsáveis pela segurança pública poderiam ser (mais) sensibilizadas para a possibilidade de inserir indicações ao abrigo da alínea b) do n.º 2 do artigo 96.º
– A formação sobre o SIS deveria ser integrada na formação inicial dos utilizadores finais, bem como na formação contínua, ainda antes da utilização operacional do SIS	– Explicar as consequências da supressão dos controlos fronteiriços internos para o trabalho da polícia – Explicar a utilização do SIS como instrumento policial quotidiano – A formação deverá abranger tanto as consultas do sistema como a inserção de indicações – O pessoal SIRENE deverá participar na formação SIS das escolas de polícia

RECOMENDAÇÕES	MELHORES PRÁTICAS
– Deverão ser elaborados manuais sobre os procedimentos internos – Deverão ser publicadas instruções actualizadas que incluam as novas funções – Antes de iniciar o trabalho no âmbito de Schengen, deveria ser organizada uma formação em cascata – Deverão ser previstos cursos de reciclagem logo que os utilizadores finais adquiram uma certa experiência	– A Intranet da polícia ou outros meios de comunicação deveriam colocar manuais à disposição dos agentes, incluindo o Manual SIRENE, assim como informação, material de formação e de reciclagem – Antes da utilização operacional do SIS, um boletim informativo sobre a situação do projecto destinado aos utilizadores finais poderá reforçar e garantir o seu interesse – A implementação do SIS deverá ser uma extensão fluida dos actuais métodos de consulta nacionais, de modo a reduzir as necessidades em matéria de formação

RECOMENDAÇÕES	MELHORES PRÁTICAS
4. Tratamento de dados	
4.1 Inserção / alteração / supressão de indicações	
- Ao serem inseridas, todas as indicações deverão satisfazer os critérios que garantem que será dado seguimento à indicação	- Informar as autoridades que inserem indicações no SIS acerca das consequências dessas inserções e, em especial, da obrigação de dar seguimento a uma resposta positiva - Instaurar procedimentos nacionais que definam as responsabilidades pela apresentação cabal dos pedidos de extradição ou de localização de veículos furtados...
- Analisar os ficheiros das indicações ,os termos do artigo 95.º existentes, antes de serem disponibilizadas ao utilizador final	- Garantir que o sistema SIRENE de gestão do fluxo de trabalho emite um aviso automático quando é inserida uma nova indicação ao abrigo do artigo 95.º - ainda que não tenha sido possível validar antecipadamente todos os ficheiros sobre indicações ao abrigo do artigo 95.º, as indicações deverão ser disponibilizadas aos utilizadores finais, assim que o sistema lhes seja aberto, sem aguardar o resultado da análise do formulário A pelos SIRENE; neste caso, têm de ser instaurados procedimentos para assegurar uma análise rápida do ficheiro, se a indicação for executada
- As regras de prioridade e incompatibilidade deverão ser respeitadas	- Os operadores dos SIRENE deverão ser autorizados a suprimir manualmente as indicações que não respeitem as regras de prioridade e incompatibilidade - As indicações "secundárias" sobre uma pessoa deverão continuar disponíveis para poderem ser inseridas quando expirar a primeira indicação sobre a pessoa, que era incompatível com a indicação "secundária"

RECOMENDAÇÕES	MELHORES PRÁTICAS
	- A legislação nacional deveria permitir todas as acções, designadamente os "controlos específicos" ao abrigo do artigo 99.º.
- Antes de se prorrogar a validade de uma indicação, dever-se-á reapreciar o seu prazo de validade e relevância - Os números de identificação Schengen não deviam ser reutilizados	
- O intervalo de tempo entre o incidente e a inserção de uma indicação no SIS devia ser reduzido ao mínimo	- A inserção das indicações devia efectuar-se de preferência em tempo real - Descentralizar tanto quanto possível a inserção das indicações (em especial sobre objectos) para evitar demoras devidas aos trâmites administrativos internos, como o envio das indicações para centros de inserção de dados - Sempre que não seja possível a introdução directa, deverão ser disponibilizados meios de transmissão rápidos para enviar a informação do nível local ao nível da inserção dos dados, em especial nas indicações sobre menores desaparecidos e veículos furtados
- A inserção das indicações que preenchem os critérios de Schengen no SIS deverá ser, na medida do possível, automatizada: o facto de os SIRENE terem de copiar manualmente essas indicações dos sistemas nacionais para as inserir no SIS causa frequentemente atrasos	
- Deverão ser tomadas medidas em matéria de qualidade dos dados para evitar que as indicações do SIS afectem pessoas a elas alheias	- O número de matrícula de um veículo não deverá voltar a ser utilizado enquanto for objecto de uma indicação do SIS - É prática normal uma indicação ser suprimida do SIS e mantida apenas na base de dados nacional quando, nos casos previstos na lei nacional, se apura que um veículo furtado foi adquirido licitamente por um comprador de boa fé

RECOMENDAÇÕES	MELHORES PRÁTICAS
– A inserção sistemática das indicações no SIS deveria ser melhorada e deveriam ser fixados critérios nacionais para tal inserção – Ao efectuar-se a inserção, dever-se-á verificar se não há dupla indicação	– O sistema devia procurar automaticamente eventuais indicações duplas, através de uma busca que fosse além da correspondência exacta
4.2 Seguimento das respostas positivas	
– Os SIRENE têm de ser os únicos pontos de contacto e o canal único para a transmissão de toda a informação relacionada com o procedimento pós-resposta positiva – Para as indicações ao abrigo do artigo 95.º, os SIRENE têm de ser o único ponto de contacto e são responsáveis pela troca de informação pós resposta positiva, pelo menos até ao início do processo oficial de extradição – Deverá ser enviada no prazo fixado uma resposta, ou pelo menos uma resposta preliminar, sobre a situação do processo.	– Toda a troca de informação que não exija carta rogatória deverá processar-se através dos SIRENE – Sempre que possível e/ou oportuno, os SIRENE poderão facilitar todas as novas trocas de informação subsequentes à detenção – Dever-se-á garantir que também as autoridades responsáveis pelos nacionais de países terceiros estejam permanentemente disponíveis ou organizadas de forma que permita respeitar os prazos para dar informações suplementares: podia autorizar-se o acesso dos SIRENE às bases de dados dessas autoridades

RECOMENDAÇÕES	MELHORES PRÁTICAS
– Devia ser suprimida do SIS, uma indicação assim que deixasse de haver necessidade da mesma	– As indicações ao abrigo do artigo 95.º deviam ser suprimidas, uma vez concretizada a extradição – As indicações ao abrigo do artigo 96.º não deviam ser suprimidas após uma resposta positiva – As indicações ao abrigo do artigo 97.º, sobre adultos que não é necessário colocar sob protecção internacional, deverão ser suprimidas após uma resposta positiva – Outras indicações ao abrigo do artigo 97.º deviam ser suprimidas quando são executadas as medidas de protecção – Uma indicação sobre um veículo furtado (seja ela dupla) deverá ser suprimida logo após a resposta positiva, para evitar problemas na devolução do veículo
– Deviam ser definidos procedimentos para garantir que as acções sobre objectos extraviados sejam rapidamente executadas	– Definir os papéis e responsabilidades das partes interessadas
– Fornecer estatísticas sobre as respostas positivas	– Há uma resposta positiva quando um Estado Schengen reage a uma indicação emitida por outro Estado Schengen – Todas a respostas positivas deverão ser escrupulosamente registadas, incluindo as respostas às indicações ao abrigo do artigo 96.º – As respostas positivas deviam ser classificadas por artigo

RECOMENDAÇÕES	MELHORES PRÁTICAS
4.3 Medidas relativas à qualidade dos dados	
– Inserção automatizada dos dados SIS, através de uma ligação entre as bases de dados nacionais pertinentes e a base de dados N.SIS – A par da inserção automatizada das indicações deverá haver uma alteração/supressão automatizada, em tempo real, no SIS, na sequência da alteração/supressão no sistema nacional	– Considera-se executado quando a inserção no SIS está fixada como escolha por defeito, como recomendado no Capítulo 3.1
– As indicações deverão ser o mais completas possível	– Os dados contidos na indicação deviam ser cotejados, de preferência de forma automatizada, com os registos nacionais – As indicações deverão ser actualizadas com a informação suplementar que vá ficando disponível, como o número de um documento emitido ou o número de identificação de um veículo furtado – O SIRENE do país de origem de um objecto furtado deverá facultar informações suplementares para actualizar a indicação

RECOMENDAÇÕES	MELHORES PRÁTICAS
– Os SIRENE deveriam funcionar como gestores da garantia de qualidade – Os SIRENE têm de validar todas as indicações ao abrigo do artigo 95.º	– Os SIRENE deviam possuir competência interna e meios operacionais e técnicos para garantir a qualidade dos dados, incluindo a de ter acesso às bases de dados nacionais, e efectuar amostragens de todas as categorias de indicações – Os SIRENE deviam ser implicados na formação dos utilizadores – As lista de respostas positivas deviam ser cotejadas com as listas de respostas positivas suprimidas – O quociente indicações/respostas positivas devia ser revisto e estudado – Dever-se-ia apurar periodicamente junto das autoridades locais se é necessário manter uma indicação sobre um menor desaparecido
– Deverão ser respeitadas as regras de transliteração	– Devia ser disponibilizada aos utilizadores finais informação específica sobre regras de transliteração
– Os utilizadores finais deverão receber formação sobre qualidade dos dados	– Não é permitido inserir informação impossível de despistar, inscrevendo por exemplo "desconhecido" em campos obrigatórios, ou deixando em branco campos facultativos em vez de inscrever "desconhecido" ou "?"

RECOMENDAÇÕES	MELHORES PRÁTICAS
5. Segurança	
5.1. Organização dos trabalhos em matéria de segurança de dados	
– A determinação da política de segurança para os sistemas informáticos Schengen (N.SIS, C.SIS, SIRENE e sistemas destinados ao utilizador final) deverá constituir parte integrante de toda a política de segurança desenvolvida pelas autoridades ligadas a esses sistemas. – A política de segurança deverá ser documentada por escrito pelas autoridades competentes. – É essencial atribuir os recursos necessários à elaboração e manutenção das medidas de segurança. – Haverá que estabelecer a nível nacional os procedimentos e as competências que assegurem a actualização e revisão constante das medidas de segurança. – Na medida do possível, as medidas de segurança deverão ser actualizadas ou revistas uma vez por ano, por forma a que estejam correctas e em qualquer momento reflictam a situação efectiva. – Além disso, proceder-se-á à actualização ou à revisão, na sequência de ocorrências significativas/graves ou alterações de sistema com implicações para a segurança de dados.	

RECOMENDAÇÕES	MELHORES PRÁTICAS
5.2. Organização da segurança	
– Os trabalhos em matéria de segurança de dados deverão, se for caso disso, ser efectuados no âmbito de uma estrutura de segurança que poderá envolver uma ou mais autoridades.	
– Deverão estar bem definidas as responsabilidades e competências das pessoas que trabalham no sector da segurança de dados, eventualmente mediante uma descrição das tarefas individuais. – Será conveniente documentar num organigrama a organização dos trabalhos em matéria de segurança.	
5.3. Controlo dos activos	
– Haverá que assegurar que todos os elementos essenciais (activos) dos sistemas sejam conhecidos, para assegurar a sua protecção, em função da sua importância. – Dever-se-á, portanto, manter um registo permanente do equipamento informático relevante. – Além disso, deverá existir uma documentação actualizada de redes e sistemas que identifique, nomeadamente, a conexão ou funcionalidade dos diferentes elementos dos sistemas.	
5.4. Segurança a nível do pessoal	
– O acesso a dados e equipamento do SIS, utilizado para o tratamento de dados SIS, deverá ser exclusivamente restringido a pessoas que tenham uma autorização específica. – O acesso aos dados SIS só será permitido quando tal for necessário para o cumprimento das tarefas atribuídas à pessoa	– Controlos de segurança do pessoal como parte integrante do processo de recrutamento, repetidos de cinco em cinco anos

em causa. – A descrição das tarefas do pessoal que tem acesso a dados e equipamento para tratamento de dados SIS deverá incluir uma informação sobre as responsabilidades em matéria de segurança.	
– As práticas de recrutamento de pessoal deverão privilegiar os conhecimentos no domínio da segurança de dados. – Deverá ser ministrada a esse pessoal a formação necessária, nomeadamente sobre as regras vigentes em matéria de segurança de dados. – O pessoal que não pertença a nenhuma autoridade nacional deverá estar sujeito a regras de sigilo e confidencialidade. – O pessoal em causa deverá dispor da necessária habilitação ou certificação e – Ter acesso aos dados do SIS apenas na medida do necessário para o desempenho das suas tarefas. – Haverá que definir vias de comando e procedimentos para notificar com a possível brevidade ocorrências reais ou suspeitas, com implicações para a segurança. – Todo o pessoal interno e externo deverá ter conhecimento deste procedimento. – Haverá que implementar procedimentos de retorno por forma a assegurar que os resultados sejam tidos em conta, uma vez tratada e encerrada a ocorrência. – O não cumprimento das regras de segurança deverá ser devidamente sancionado, de acordo com a legislação nacional.	

5.5. Segurança física	
– As instalações de tratamento de dados SIS (N.SIS, C.SIS e SIRENE) e outros recursos sensíveis, nomeadamente os arquivos electrónicos, deverão estar situadas em zonas seguras, protegidas e delimitadas com barreiras físicas adequadas e sujeitas a medidas de controlo do acesso.	– Será conveniente estabelecer uma área de segurança de classe II, tal como definida na Decisão do Conselho de 19 de Março de 2001 [1], para o tratamento de todos os dados SIS (na medida em que as instalações de tratamento de dados SIS lidam com informações confidenciais da UE, será necessária, de qualquer modo pelo menos uma área de segurança de classe II) – Computadores instalados nas caves – Zonas de segurança diferenciadas – Cartões de acesso – Guardas – Controlo por televisão em circuito fechado (CCTV)
– Os espaços deverão ser adequadamente protegidos contra toda e qualquer forma de intrusão. – Os muros exteriores deverão ter uma construção sólida e as portas de acesso deverão estar devidamente protegidas para impedir o acesso de pessoas não autorizadas, mediante, por exemplo, mecanismos de controlo, dispositivos de bloqueio, alarmes e fechaduras. – Os edifícios ou locais onde se encontram as instalações de tratamento de dados do SIS deverão dispor de uma área de recepção com pessoal, ou ser dotadas de outros meios que permitam o controlo do acesso físico.	
– O acesso às zonas protegidas onde se encontram as instalações de tratamento de dados e de arquivo electrónico do SIS deverá estar sujeito o controlos e ser restringido às pessoas autorizadas.	– Controlo das entradas e saídas
– Pessoas estranhas que entram nas zonas protegidas deverão estar sujeitas a vigilância	

[1] Decisão do Conselho 2001/264/CE que aprova as regras de segurança do Conselho (JO n.º L 101 de 11.04.2001, p. 1)

ou passar por um controlo de segurança. – Estas pessoas só deverão ter acesso para uma finalidade específica, sujeita a autorização. – O pessoal de manutenção externo só deverá ter um acesso restrito às zonas protegidas se for estritamente necessário – Esse acesso deverá ser devidamente autorizado e vigiado.	
5.6. Segurança de equipamento	
– Todo o equipamento utilizado no tratamento e arquivo de dados SIS deverá ser protegido contra danos ou perdas acidentais e acesso não autorizado.	
5.6.1. Equipamento de tratamento de dados SIS	
– O equipamento de tratamento de dados SIS será colocado num local de acesso limitado – Haverá uma vigilância permanente, a fim de minimizar o risco de potenciais ameaças, nomeadamente ataques criminosos ou terroristas, incêndio, sobreaquecimento devido a uma avaria no sistema de climatização, desmoronamento das estruturas na sequência de uma explosão e infiltrações de água. – Para assegurar a alimentação contínua de energia deverá estar disponível, sujeito a controlo e testes periódicos, o seguinte equipamento: ● Alimentação ininterrupta de energia (UPS) que assegure o funcionamento das funcionalidades mais importantes ● Um gerador de apoio que permita continuar o tratamento de dados em caso de falha prolongada de enérgia.	– Sistemas de detecção de incêndios, calor e fumo – Sistemas automáticos de extinção de incêndios – Ar condicionado adequado

RECOMENDAÇÕES	MELHORES PRÁTICAS
- Os cabos de telecomunicações deverão ser devidamente protegidos. - O equipamento das redes electrónicas deverá estar instalado em espaços ou armários fechados à chave. - A reparação e manutenção só podem ser confiadas a pessoal autorizado. - Sistema de apoio separado, controlos periódicos da ligação entre o sistema de apoio e o sistema operacional	- Sítios de reserva frios/quentes e sítios espelho - Em locais afastados de modo a que um acidente que afecte um dos sítios não tenha repercussões no outro
5.6.2 Terminais e PC	
- Os terminais, os PC e as impressoras deverão dispor de mecanismos que impeçam que pessoas não autorizadas leiam os dados. - Deverão ser instituídos procedimentos para vigiar as impressões feitas a partir do ecrã e as listas de dados SIS - As sessões em PC e terminais deverão cessar automaticamente após um período de inactividade ou ser protegidas por mecanismos de bloqueio, senhas ou outro tipo de controlo, quando não estão a ser utilizadas. - Os terminais e os PC, incluindo as impressoras que se encontrem em locais acessíveis ao público, deverão estar sob vigilância permanente.	
5.7 Gestão das comunicações e do funcionamento	
5.7.1 Procedimentos operacionais e responsabilidades	
- Os procedimentos operacionais estabelecidos por cada um dos Estados-Membros deverão ser documentados e constantemente actualizados - Deverão incluir, no mínimo, os seguintes elementos:	

RECOMENDAÇÕES	MELHORES PRÁTICAS
• Procedimentos relativos à gestão quotidiana, como por exemplo, cópias de segurança, actualização de programas antivírus, vigilância da rede, etc. • Procedimentos relativos à gestão de suportes de dados e outros activos • procedimentos relativos às restrições de acesso • Instruções em caso de erro ou outras circunstâncias excepcionais • Contactos de apoio, em caso de dificuldades técnicas ou de funcionamento imprevistas • Procedimentos para o relançamento e reinstalação do sistema em caso de avaria - Deverá ser assegurado um controlo satisfatório de todas as alterações das instalações e dos sistemas de tratamento de dados SIS, nomeadamente a nível de equipamento, *software* ou procedimentos - As responsabilidades e os procedimentos de gestão das mesmas deverão estar claramente definidas.	
5.7.2 Procedimento em caso de incidentes	
- Deverão existir planos de emergência e procedimentos escalonados de intervenção no caso de incidentes susceptíveis de interromper o funcionamento do sistema e de impedir total ou parcialmente o acesso aos sistemas informáticos Schengen - Deverão existir procedimentos específicos para detectar e actuar em caso de incidentes que, embora não impossibilitando o acesso a todo o sistema, comprometam a segurança dos dados.	

RECOMENDAÇÕES	MELHORES PRÁTICAS
5.7.3 Protecção contra software malévolo	
- A protecção da integridade do *software* e dos dados exige uma série de medidas de segurança que permitam prevenir e detectar a introdução de *software* malévolo e que contribuam para a subsequente reinstalação do sistema. - Estas medidas deverão incluir controlos para a protecção contra vírus, vermes, cavalos de Tróia e outras formas de *software* malévolo - Deverão ainda abranger, no mínimo, os seguintes elementos: • Uma política formal que exija o respeito das licenças de *software* e proíba a utilização e software não autorizado • Deverão ser instalados programas antivírus e programas de reparação em todos os PC, com actualização periódica de definições dos vírus e varrimento dos servidores, PC e computadores portáteis. As eventuais excepções deverão ser documentadas. • Todos os anexos a mensagens de correio electrónico e todos os ficheiros descarregados deverão ser verificados para detectar *software* malévolo antes da sua utilização. Deverá ser indicado onde é efectuado este controlo, por exemplo, nos servidores de correio electrónico ou no acesso à rede • Deverão existir procedimentos estabelecidos de reacção a incidentes relacionados com vírus	- Proibir os anexos com ficheiros exe., cifrados, com macros ou senhas,…
5.7.4 Cópias de segurança	
- Há que fazer regularmente cópias de segurança dos dados SIS, dos ficheiros de configuração e das aplicações	- Fazer cópias diariamente

RECOMENDAÇÕES	MELHORES PRÁTICAS
- Todos os sistemas de cópias de segurança serão testados periodicamente para garantir que cumpram as exigências do plano de funcionamento	
- Os dados das cópias de segurança deverão beneficiar da protecção física necessária e ser colocados em diferentes localizações geográficas	- Guardar as cópias em pelo menos dois locais diferentes
- Os procedimentos de reinstalação deverão ser controlados e testados regularmente	- Semestralmente
5.7.5 Gestão da rede	
- A transmissão nacional de dados SIS deverá processar-se exclusivamente em rede protegida contra o acesso não autorizado	- Rede cifrada/ rádio / fax
- A rede deverá estar sob vigilância permanente	
- Deverão ser tomadas medidas que assegurem a confidencialidade dos dados SIS quando são transmitidos através de redes de comunicações.	- Securizar as comunicações entre o SIRENE e as agências no terreno/agentes operacionais no que diz respeito ao intercâmbio de dados pessoais
- Não pode haver acesso aos dados SIS a partir de redes públicas como a Internet	- Evitar que se aceda à Internet através da rede da polícia
- A transmissão de senhas e de outros elementos de segurança deverá ser protegida por meio de métodos de cifragem	
5.7.6 Gestão dos suportes electrónicos	
- O número de cópias técnicas de dados SIS deverá limitar-se ao mínimo necessário (cf. n.º 2 do artigo 102.º)	
- Deverão ser definidos procedimentos que regulem a gestão e o arquivo de dados SIS, por forma a proteger esses dados contra a transmissão não autorizada ou a utilização abusiva.	
- Estes procedimentos deverão incluir as seguintes disposições:	

RECOMENDAÇÕES	MELHORES PRÁTICAS
• O acesso aos arquivos electrónicos que contêm dados SIS deverá ser restringido a pessoas autorizadas.	
• Todos os suportes de dados SIS deverão ser devidamente assinalados e suficientemente protegidos durante a transmissão.	- As actualizações da base de dados do SIS deverão ser enviadas para os postos consulares através de suportes cifrados e por correio diplomático
• Os suportes que sejam obsoletos ou deixem de ser necessários deverão ser tornados inutilizáveis e, em caso de reutilização, ser tratados por forma a eliminar todos os dados SIS.	- Prevenir a distribuição errada de dados devido a uma reciclagem incorrecta de materiais, inclusive papel - Substituição dos suportes efectuada por autoridades competentes ou empresas aprovadas/sujeitas a controlo de segurança - Procedimentos de armazenagem e destruição de materiais/, política da "secretária limpa"
- Os arquivos deverão ser protegidos - O acesso aos arquivos deverá ser controlado e restringido ao pessoal designado para o efeito - Esse acesso deverá ser vigiado e registado - Os arquivos deverão ser geridos de forma a garantir que são aplicadas políticas de supressão	- Os arquivos electrónicos proporcionam as melhores garantias de segurança, incluindo o registo de acesso e de utilização dos ficheiros e instrumentos de controlo - Os arquivos electrónicos poderão incluir funções automáticas de limpeza e de supressão - No caso dos arquivos físicos, considerou-se que a combinação de um cartão magnético e de um código pessoal seria a melhor solução - Será de evitar impressões feitas a partir de arquivos electrónicos, mas se tal for necessário, deverão ser destruídas após a utilização
5.8 Controlo do acesso dos utilizadores	
- Estabelecer-se-á um procedimento de registo e de anulação do registo dos utilizadores para efeitos de acesso aos diferentes sistemas e serviços. Este procedimento deverá incluir os seguintes elementos:	- Validação das consultas por amostragem

RECOMENDAÇÕES	MELHORES PRÁTICAS
• Deverão utilizar-se códigos de identificação inequívocos dos utilizadores, que permitam registar as diversas operações efectuadas, podendo os utilizadores ser responsabilizados pelas mesmas; por conseguinte, não se deverá autorizar a utilização de códigos de identificação colectivos. • O utilizador individual deverá dispor apenas dos direitos de acesso mínimos, indispensáveis ao cumprimento normal das suas tarefas.	
• Deverão ser imediatamente anulados os direitos de acesso aos dados SIS, assim que os seus utilizadores tenham deixado de exercer as funções que justificavam esse acesso • Deverá verificar-se periodicamente se o nível de acesso atribuído corresponde ao perfil do utilizador.	- A aplicação poderá incluir uma função técnica que encerre automaticamente a ficha de um utilizador que não tenha sido usada durante duas semanas, por exemplo
• Os códigos de identificação e as fichas dos utilizadores supérfluos deverão ser periodicamente verificados e apagados.	- A identificação e a ficha do utilizador poderão ser automaticamente ligadas ao estatuto pessoal
- A atribuição e gestão de senhas deverá ser controlada mediante um procedimento formal que assegure que: • Os utilizadores recebam instruções e conheçam as suas obrigações em relação à respectiva senha, • As senhas sejam comunicadas de uma forma segura ao utilizador,	
• Os utilizadores deverão alterar regularmente as respectivas senhas e não deverá ser permitida a repetição de senhas, • As senhas em caso algum deverão ser guardadas no sistema informático sem protecção.	– A senha deverá ser alterada de dois em dois ou de três em três meses
- Deverá ser estabelecido um procedimento que assegure a revisão periódica de todos os direitos de acesso dos utilizadores.	

RECOMENDAÇÕES	MELHORES PRÁTICAS
5.9 Vigilância do acesso e utilização do sistema	
– A utilização a nível nacional dos sistemas informáticos Schengen deverá ser vigiada a fim de detectar actividades não autorizadas - A transmissão de dados pessoais deverá ser registada em conformidade com o artigo 103.ºda Convenção Schengen - Durante o período previsto no artigo 103.º, deverá ser mantido um registo das entradas dos utilizadores no sistema e, na medida do possível, das saídas; das tentativas de conexão ou das conexões falhadas, assim como das tentativas de utilização não autorizada de dados - Os dados registados deverão incluir a identificação do utilizador, a data ou a hora do incidente e, se possível, a identificação e localização do terminal.	- As conexões e pistas de auditoria relativas às fichas SIRENE deverão ser vigiadas de forma proactiva e conservadas durante um período suficientemente longo, em conformidade com o direito nacional - Os sistemas electrónicos de gestão do fluxo de trabalho e dos processos constituem a melhor maneira de garantir que todos os movimentos relativos a uma ficha SIRENE são registados e controlados
5.10 Desenvolvimento e manutenção	
- A fim de minimizar o risco de danos nos sistemas operacionais deverão ser estabelecidas medidas de controlo dos dados e programas	

RECOMENDAÇÕES	MELHORES PRÁTICAS
- Será sobretudo necessário assegurar que a actualização dos sistemas operacionais, nomeadamente das bibliotecas de programas, só se efectue mediante autorização prévia. - Antes de ser autorizada, a actualização deverá ter sido suficientemente testada e documentada - Deverá ser encontrado um sistema de teste, diferente do ambiente de produção, que permita ensaiar as alterações antes que estas se tornem operacionais e sem introduzir dados relativos ao teste no sistema operacional - Deverá ser evitada a utilização de dados SIS reais para efeitos do teste, a menos que estes tenham sido tornados anónimos.	
5.11 Plano de emergência	
- Cada Estado Schengen deverá estabelecer e implementar um plano de emergência adequado, nomeadamente para as seguintes situações: • Ser constatada uma impossibilidade de acesso aos N.SIS ou à rede • Alguns ou todos os utilizadores ficarem impossibilitados de pesquisar dados SIS, na sequência de problemas a nível da infra--estrutura TI nacional - Os planos de emergência deverão basear-se numa avaliação das ameaças que possam tornar o sistema inacessível e no impacto dessas ameaças sobre os restantes Estados Schengen. - Os planos de emergência deverão, no mínimo, incluir os seguintes elementos:	

RECOMENDAÇÕES	MELHORES PRÁTICAS
• As condições para accionar os planos e as medidas que deverão ser imediatamente tomadas para avaliar a situação • Procedimentos escalonados de intervenção, de acordo com os procedimentos acordados para os Estados Schengen, tendo em vista informar as autoridades nacionais de gestão, o C.SIS e os restantes Estados Schengen • Procedimentos de emergência, com descrição das medidas a tomar, na sequência de um incidente que comprometa a acessibilidade do sistema • Procedimentos de recurso, com descrição das medidas a tomar para transferir temporariamente as operações N.SIS mais importantes para servidores alternativos • Procedimentos de reinstalação, com descrição das medidas a tomar para repor o funcionamento normal. - Deverá proceder-se periodicamente à actualização dos planos de emergência e a testes das rotinas seguidas pelo pessoal	
5.12 Controlo	
- Deverão ser estabelecidos procedimentos que assegurem um controlo permanente do cumprimento de todas as regras e disposições aplicáveis a nível nacional e a nível da UE.	- Controlos de segurança periódicos, realizados por pessoas exteriores ao departamento de TI.

O objectivo do Inventário é clarificar e aprofundar o acervo de Schengen, de forma a que possa servir de exemplo para os Estados aderentes a Schengen e para os que já aplicam plenamente esse acervo.
O primeiro volume do Inventário foi publicado em Fevereiro de 2002 e aborda as questões do controlo das fronteiras externas e do afastamento e readmissão.

O actual segundo volume do Inventário aborda especificamente o Sistema de Informação de Schengen e o SIRENE. Este volume fornece indicações úteis aos países candidatos à adesão à União Europeia sobre o que deles se espera, nomeadamente em termos práticos, relativamente a Schengen.