ES

CONSEJO DE
LA UNIÓN EUROPEA

SECRETARÍA GENERAL

DG H

UE
Catálogo de Schengen

Volumen 2

Sistema de Información de Schengen, Sirene: Recomendaciones y prácticas más idóneas

Diciembre de 2002

UE
Catálogo de Schengen

Volumen 2

Sistema de Información de Schengen, Sirene: Recomendaciones y prácticas más idóneas

Diciembre de 2002

ÍNDICE

Prefacio de la Presidencia danesa

De conformidad con la decisión adoptada por el Consejo el 28 de mayo de 2001, el Grupo "Evaluación de Schengen" ha iniciado la elaboración de un Catálogo de recomendaciones y prácticas más idóneas para la correcta aplicación del acervo de Schengen.

El Catálogo tiene como finalidad aclarar y precisar el acervo de Schengen y ofrecer recomendaciones e indicar las prácticas más idóneas, con objeto de constituir así un ejemplo para los Estados que van a adherirse a Schengen y para los que aplican plenamente el acervo de Schengen. No se trata de definir de forma exhaustiva todo el acervo de Schengen, sino de presentar recomendaciones y prácticas más idóneas a la luz de la experiencia adquirida con la evaluación permanente de la aplicación correcta de dicho acervo en los Estados Schengen.

El primer volumen del Catálogo trata de las fronteras exteriores, la expulsión y la readmisión. Se aprobó y entregó a los países candidatos en el Consejo de 28 de febrero 2002.

Dinamarca, que ocupa la Presidencia del Consejo de la Unión Europea desde el 1 de julio de 2002, considera muy importante proseguir la labor de redacción del Catálogo. Durante la Presidencia danesa se ha redactado el segundo volumen del Catálogo, relativo al Sistema de Información de Schengen y a la aplicación del Manual SIRENE.

La Presidencia danesa quisiera agradecer a los Estados Schengen y a la Comisión la ayuda y la valiosa cooperación que han prestado en la elaboración del Catálogo; en este sentido, desea manifestar su especial gratitud a Noruega, país que ostenta la Presidencia del Comité Mixto, por ayudar a la Presidencia danesa presidiendo el subgrupo que ha redactado el Catálogo.

El Catálogo tiene una finalidad explicativa y no es jurídicamente vinculante. Se presenta en dos columnas: en una se exponen los aspectos a los que sería preciso atender para cumplir el acervo de Schengen; en la otra se indican las prácticas más idóneas observadas en algunos Estados miembros.

El Catálogo se entregará a los países adherentes y a los países candidatos. La Presidencia danesa confía en que constituirá, junto con otros, un instrumento útil para lograr la satisfactoria integración de los nuevos Estados miembros de la Unión Europea en el momento oportuno y de la forma adecuada.

Diciembre de 2002

CATÁLOGO SCHENGEN

INTRODUCCIÓN

1. En la sesión de 28 de mayo de 2001, el Consejo fijó como objetivo para la continuación de los trabajos del Grupo de Evaluación de Schengen "... destacar las prácticas más idóneas, en particular respecto al control en las fronteras con objeto de que sirvan de ejemplo a los Estados que se adhieran a Schengen, pero también a aquéllos que aplican el acervo de Schengen en su totalidad. Estas evaluaciones, además de la distinción de las prácticas más idóneas, servirán de inspiración para el establecimiento de unos criterios uniformes para definir la aplicación mínima del acervo de Schengen (…) en los grupos de trabajo correspondientes" (mandato otorgado al Grupo "Evaluación de Schengen") (8881/01 – SCH-EVAL 17, COMIX 371).

   En virtud de dicho mandato, el Grupo de Evaluación de Schengen definió los principios y el procedimiento para elaborar el Catálogo de recomendaciones y de prácticas más idóneas con miras a la correcta aplicación del acervo de Schengen, en adelante denominado Catálogo de recomendaciones y de prácticas más idóneas o Catálogo.

   El objetivo del Catálogo es aclarar el acervo de Schengen, profundizar en él y ofrecer recomendaciones y prácticas más idóneas, a fin de que sirva de ejemplo para los Estados candidatos a la adhesión a Schengen, pero también a los que aplican plenamente el acervo de Schengen. Desde esta perspectiva, el catálogo proporciona a los Estados candidatos a la adhesión a la Unión Europea (en adelante la UE) a petición de éstos una buena indicación sobre lo que se espera de ellos, en la práctica sobre todo para las cuestiones de Schengen. El objetivo no es definir de forma exhaustiva todo el acervo de Schengen, sino presentar las recomendaciones y prácticas más idóneas, conforme a la experiencia adquirida por el Grupo de Evaluación de Schengen en la verificación de la aplicación correcta del citado acervo en diversos países.

   El texto del Catálogo no tiene por objetivo introducir nuevas exigencias, pero sí debe permitir, también, señalar al Consejo, en su caso, la necesidad de modificar determinadas disposiciones del acervo de Schengen, de manera que la Comisión y, si procede, los Estados miembros tomen en consideración las recomendaciones y las prácticas más idóneas a la hora de presentar propuestas o iniciativas formales. Con este ejercicio el Consejo comienza a definir normas mínimas.

Por otra parte, el catálogo servirá como instrumento de referencia en las futuras evaluaciones que se hagan en los países candidatos. Así pues, servirá también a éstos como indicador de las misiones que se les asignen, para lo cual deberá leerse en relación con el Manual SIRENE.

2. El Grupo Evaluación de Schengen ha adoptado las siguientes definiciones para realizar el ejercicio:
Recomendaciones: conjunto no exhaustivo de medidas que debe permitir constituir la base para la correcta aplicación del acervo de Schengen, así como para el control de ésta.
Prácticas más idóneas: conjunto no exhaustivo de métodos de trabajo o de medidas ejemplares que deben considerarse la aplicación óptima del acervo de Schengen, lo que se entiende sin perjuicio de que puedan existir distintas prácticas idóneas para cada parte específica de la cooperación Schengen.

3. Cuando el Catálogo menciona los Estados miembros que aplican el acervo de Schengen, queda entendido que se trata, en estos momentos, de los trece Estados miembros de la Unión Europea mencionados en el artículo 1 del Protocolo por el que se integra el acervo de Schengen en el marco de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea (en adelante el "Protocolo de Schengen"), a los que se añaden Islandia y Noruega, en virtud del Acuerdo de cooperación celebrado por el Consejo de la Unión Europea, la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen, firmado el 18 de mayo de 1999 (estos 15 Estados se denominan en adelante los "Estados Schengen").

El Reino Unido e Irlanda manifestaron el deseo de participar en algunas disposiciones del acervo de Schengen. El modo de participación del Reino Unido se estableció en la Decisión del Consejo de 29 de mayo de 2000 (2000/365/CE), y el modo de participación de Irlanda en la Decisión del Consejo de 28 de febrero de 2002 (2002/192/CE). El Consejo todavía no se ha pronunciado sobre la aplicación de estas disposiciones.

De acuerdo con el artículo 8 del Protocolo de Schengen, se considera que dicho acervo y las restantes medidas adoptadas por las instituciones en el ámbito del acervo han de aceptarse en su totalidad como acervo por todo Estado que sea candidato a la adhesión.

4. El acervo de Schengen se integró en el marco de la UE en virtud del Protocolo de Schengen. La delimitación del acervo está establecida en la Decisión del Consejo 1999/435/CE, publicada en el DO L 176, de 10 de julio de 1999.
   Desde su integración en la UE, el acervo de Schengen ha registrado novedades y modificaciones, es decir, está en evolución.
   El acervo de Schengen se ha enriquecido también con los resultados de las evaluaciones que se han venido realizando en la Comisión Permanente de Evaluación del Acervo de Schengen, hoy denominada "Grupo de Evaluación de Schengen". Con arreglo al mandato de dicho grupo, se presentan al Consejo informes para comprobar si se cumplen las condiciones exigidas para la aplicación de las disposiciones del acervo de Schengen en un Estado que desee participar en dichas disposiciones (o en algunas de ellas) y, asimismo, para velar por la correcta aplicación del acervo de Schengen por parte de los Estados Schengen, descubriendo los problemas y proponiendo soluciones.

5. El primer volumen del Catálogo, del que se hizo entrega a los países candidatos en el Consejo de 28 de febrero de 2002, abordaba principalmente cuestiones relativas a las fronteras y a la expulsión. Este segundo volumen del Catálogo trata del Sistema de Información de Schengen, en particular de la aplicación del Manual SIRENE. La libre circulación en el territorio de los Estados Schengen es una libertad que exige como contrapartida no sólo el refuerzo de las fronteras exteriores comunes y una política de expulsión de los nacionales de terceros países en situación irregular, sino también un intercambio de información rápido y eficaz en el contexto de los controles fronterizos y de la cooperación policial. Por ello, las medidas adoptadas en este sentido van encaminadas a impulsar la integración europea y, sobre todo, a permitir que la UE llegue a ser más pronto un espacio de libertad, seguridad y justicia.

6. El presente volumen del Catálogo está integrado por el capítulo relativo al SIS/SIRENE. En un breve apartado de observaciones generales se describen los conceptos fundamentales sobre los que se basan las recomendaciones y prácticas idóneas expuestas. Estas se presentan en forma de cuadro, con las recomendaciones a la izquierda y las prácticas más idóneas a la derecha de las recomendaciones correspondientes.

* * *

PARTE III: EL SISTEMA DE INFORMACIÓN DE SCHENGEN

PORMENORES DE LAS RECOMENDACIONES Y PRÁCTICAS MÁS IDÓNEAS

Observaciones generales

La lista de recomendaciones y prácticas más idóneas que figura más abajo se confeccionó principalmente sobre la base del resultado de diferentes evaluaciones llevadas a cabo durante los últimos años, tanto evaluaciones del SIS en distintos países como evaluaciones más específicas de los SIRENE.

El contenido del presente Catálogo fue elaborado de manera que fuera independiente del sistema técnico de base, ya sea el SIS 1+ o el SIS II. De hecho, está destinado a utilizarse para la creación de bases de datos nacionales que aporten información al SIS y para la preparación de la parte nacional del SIS, sea cual sea su forma en la arquitectura del SIS II.

Se recuerda que, en cualquier caso, en la medida en que los usuarios de sistemas de TI de Schengen manejen información clasificada de la UE, es de aplicación la Decisión 2001/264/CE del Consejo por la que se adoptan las normas de seguridad del Consejo (DO L 101 de 11.4.2001, p. 1).

Por lo que respecta a la introducción de descripciones en el SIS, el principio básico consiste en hallar un equilibrio entre la inclusión en el SIS de cuantas descripciones sea posible, en el marco de lo dispuesto en el Convenio, y la garantía de que las descripciones incluidas en el SIS sean de buena calidad. Ambos criterios son condición esencial para la eficacia y la utilidad del SIS. Cada descripción nacional que sea pertinente a los efectos de Schengen debería en principio ser introducida en el SIS. No obstante, para poder tomar medidas a raíz de una descripción es necesario que ésta sea correcta, lo más completa posible y que pueda hacerse un seguimiento de la misma. Por último, hay que tener presente que cuando un Estado Schengen toma medidas a raíz de una descripción, tiene derecho a esperar que el Estado Schengen de emisión dará seguimiento a la respuesta positiva. No hacerlo sin una razón jurídica válida afectará negativamente a la predisposición de las autoridades locales para utilizar el SIS y aprovechar al máximo sus posibilidades.

El papel del SIRENE en el funcionamiento del SIS es esencial. Aunque no se supone ni es necesario que el SIRENE sea responsable de cada una de las acciones en relación con el SIS, el SIRENE es la interfaz humana del SIS. Ello implica que desempeña un papel de contacto de primera línea tanto para los demás SIRENE como para las autoridades nacionales y los usuarios finales. En función de cada caso, el SIRENE debe poder atenderlos de manera independiente o remitirlos a las autoridades u organismos competentes. Por ello, el personal SIRENE debe ser competente, poseer una buena formación y tener establecidos buenos contactos con las autoridades nacionales y extranjeras.

RECOMENDACIONES Y PRÁCTICAS MÁS IDÓNEAS

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
1. Parte nacional del SIS	
1.1 Sistemas y organización	
– debe establecerse una parte nacional del SIS que tenga un funcionamiento las 24 horas del día y los siete días de la semana con suficiente apoyo técnico en todo momento	– deberían asumirse compromisos a nivel de mantenimiento y funcionamiento del equipo y de la programación para garantizar un funcionamiento las 24 horas del día y los siete días de la semana
– garantía de la integridad de los datos entre los N.SIS y cualquier copia técnica nacional, en caso de existir	– sincronización de las copias en tiempo real – comparaciones periódicas de la base de datos
1.2 Infraestructura de comunicación	
– debería disponerse de una red nacional estable	– deberían asumirse compromisos apropiados a nivel de mantenimiento y funcionamiento para garantizar una alta disponibilidad de la red
– debería garantizarse un plazo breve de respuesta a las consultas	– el plazo de respuesta debería ser inferior a 5 segundos
– los datos del SIS disponibles en las oficinas consulares deben actualizarse periódicamente	– lo mejor sería que las oficinas consulares tuvieran acceso en línea a los datos pertinentes del SIS – cuando sólo pueda facilitarse acceso fuera de línea, deberían enviarse actualizaciones de la base de datos cada dos semanas y debería realizarse un control adicional por teléfono

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
2. SIRENE	
2.1 Estructura nacional	
– debe establecerse un SIRENE y designarse como punto de contacto único para cada Estado Schengen por lo que respecta a las descripciones del SIS y al procedimiento subsiguiente a una respuesta positiva	– todas las oficinas responsables de la cooperación policial internacional deberían poder ser contactadas mediante un punto de contacto único, hallarse integradas en una misma estructura de gestión y estar ubicadas en el mismo lugar
– debería respetarse y aplicarse el principio de que las descripciones de Schengen tienen preferencia sobre las descripciones de Interpol	– la descripción de Interpol debería incluir una nota para los Estados Schengen en la que se indicara el número de identificación Schengen de la descripción
2.2 Organización y sistema	
– el SIRENE debe proporcionar una cobertura las 24 horas del día y los siete días de la semana para la comunicación con el resto de oficinas SIRENE y autoridades nacionales	– continuidad de los aspectos de gestión, personal y técnicos
– todo el personal, incluido aquel que tenga asignado trabajo fuera de las horas de oficina, debería poseer la competencia y la experiencia suficientes para prestar el servicio necesario a las demás oficinas SIRENE y ocuparse de cualquier entrada de descripciones	– flexibilidad de las normas de trabajo
– además del personal administrativo y operativo, existe una necesidad específica de personal de apoyo de TI	– deberían asumirse compromisos a nivel de mantenimiento y funcionamiento del equipo y de la programación para garantizar un funcionamiento las 24 horas del día y los siete días de la semana
– el SIRENE debe estar equipado de un sistema eficiente y efectivo de gestión del trabajo	– se ha diseñado un sistema informatizado de seguimiento del trabajo y gestión de casos para los operadores SIRENE que aumenta la calidad del trabajo y reduce la posibilidad de errores

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
	– el sistema informatizado de seguimiento del trabajo y gestión de casos debería interactuar con los sistemas nacionales y la aplicación N.SIS por lo que respecta a la gestión de las descripciones recibidas y emitidas; dicha interacción debería incluir indicaciones automáticas • sobre si se ha añadido o suprimido un indicador de validez requerido • sobre el momento en que se haya modificado una descripción • sobre la llegada de una nueva descripción a los efectos del artículo 95
– el SIRENE debería contar con la posibilidad de transmitir imágenes rápida y eficientemente, p. ej. fotografías e impresiones dactilares	– es preferible la transmisión electrónica de imágenes para garantizar la transmisión de imágenes utilizables – para tales transmisiones electrónicas debería utilizarse la norma ANSI/NIST-CLS 1-1993 o posteriores revisiones
2.3 Contratación y formación	
– el SIRENE debería tener un personal capaz de actuar a iniciativa propia para garantizar que los casos sean tratados de forma eficiente	– debería contarse con apoyo de gestión, incluido el acceso fuera de horas de servicio a asesoramiento jurídico especializado y de otro tipo, para permitir la delegación de responsabilidades – debería prestarse especial atención a la gestión de los recursos humanos para garantizar la continuidad del personal, que constituye una de las claves para mejorar la calidad del trabajo SIRENE – debería disponerse de un sistema de formación en el seguimiento del trabajo SIRENE
– todos los operadores deberían tener buenos conocimientos de las cuestiones jurídicas nacionales, de la aplicación de las leyes nacionales (incluido un conocimiento teórico de las actividades policiales), del sistema judicial y de inmigración nacional y al menos unos conocimientos básicos sobre cuestiones jurídicas internacionales	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– debería disponerse de asesoramiento jurídico, con un buen conocimiento de la legislación nacional e internacional, un conocimiento detallado del Convenio de Schengen y de normativas conexas, y conocimientos teóricos sobre las actividades policiales	– el asesoramiento jurídico puede obtenerse mediante la contratación de asesores jurídicos internos u organizando formación jurídica para el personal SIRENE
– se requiere personal con formación policial que aporte una experiencia que ha demostrado ser muy beneficiosa y reduce el tiempo de formación	
– establecer normas comunes y un entendimiento mutuo	– formación común, al menos una vez al año – intercambio periódico de operadores, comenzando antes del uso operativo del SIS
– los niveles de contratación deberían tener en cuenta el número de descripciones nacionales y el examen ulterior de dichas descripciones al final de su periodo de validez, así como el número de respuestas positivas en el territorio nacional	
– la estrategia de contratación del SIRENE debería prever la validación de los archivos existentes relativos al artículo 95 antes del uso operativo del SIS	
– el personal debería tener suficientes conocimientos lingüísticos	– este debería ser un elemento clave en el procedimiento de contratación y en la formación en curso del personal SIRENE – el personal SIRENE debería tener prioridad en la formación lingüística – la práctica común consiste en intercambiar formularios en la lengua del país emisor y en inglés

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– para lograr la máxima eficacia en la comunicación bilateral su utilizarán las lenguas que sean familiares para ambas partes	– es desde luego deseable que los operadores conozcan las lenguas habladas más frecuentemente, tanto para la comunicación directa como para poder gestionar documentación a falta de apoyo de traducción

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
3. Usuarios finales	
3.1 Consulta e interfaz de usuario	
– es preciso que la consulta o la búsqueda vaya más allá de la correspondencia exacta	– los ejemplos en este sentido incluyen consultas fonéticas, consultas con caracteres comodines, lógica difusa, *soundex*
– una consulta única tanto para el sistema nacional como para el internacional es la forma más eficaz de garantizar una consulta sistemática al SIS	– debería verificarse que dicha consulta única no es contraria a la legislación nacional – debería garantizarse que la consulta única sea rápida y fácil
– es preferible el acceso directo	– debería proporcionarse a los usuarios finales el mayor número posible de dispositivos de consulta de datos para permitir consultas directas
– debería mostrarse simultáneamente la información sobre las descripciones nacionales y las internacionales	
– el usuario final debería disponer en la primera pantalla de la información acerca de si la persona se considera peligrosa o va armada	
– al introducir descripciones nacionales, la inclusión de la descripción en el SIS debería establecerse como función por defecto para que no sea necesaria ninguna otra acción por parte del usuario final	– las descripciones deberían verificarse previamente en la base de datos nacional y desde ella transferirse al N.SIS de forma automática
– deberían verificarse los datos nacionales que existan previamente por lo que respecta a su relevancia a los efectos de Schengen y a su corrección antes de proceder a la carga de datos inicial de descripciones nacionales en el SIS	
– presentar información e instrucciones claras sobre las acciones que ha de llevar a cabo el usuario final en caso de respuesta positiva	– en caso de usurpación de identidad, presentar claramente en la pantalla el procedimiento para hacer frente a una respuesta positiva de identidad usurpada y las ulteriores indagaciones que deberían realizarse para establecer si la persona es la víctima o el autor de la usurpación

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– las aplicaciones deberían desarrollarse de forma que su utilización sea fácil, permitiendo que se lleven a cabo las tareas del SIS de manera rápida y efectiva	– si fuera oportuno, la consulta al SIS podría combinarse con la consulta a sistemas existentes – al introducir un nombre en una consulta, el sistema debería verificar tanto los datos sobre personas como sobre documentos – la interfaz de usuario debería permitir y fomentar que el nombre y, en su caso, el número de documento se introduzcan simultáneamente y la aplicación debería hacer la búsqueda de ambos en la misma consulta
3.2 Formación	
– asegurarse de que las partes interesadas conocen las posibilidades del SIS: policía y otros organismos policiales, jueces y fiscales	– facilitar formación permanente a dichas partes – poner a disposición de los usuarios finales un sistema de formación – asegurar un estrecho contacto de las partes interesadas con el SIRENE mediante funcionarios de enlace – fomentar el conocimiento del SIS mediante los grupos pertinentes (cooperación policial, control fronterizo, grupo de jefes de policía, cooperación judicial, grupo sobre terrorismo) o por medio de la CEPOL – podría darse más a conocer a las autoridades responsables de la seguridad pública la posibilidad de introducir descripciones en virtud de la letra b) del apartado 2 del artículo 96
– la formación sobre el SIS debería incluirse en la formación inicial de los usuarios finales y en la formación continua, antes del uso operativo del SIS	– explicar las consecuencias de la supresión de los controles en las fronteras interiores para el trabajo policial – explicar el uso del SIS como instrumento policial cotidiano – la formación debería abarcar tanto la consulta al sistema como la introducción de descripciones – el personal SIRENE debería participar en la formación sobre el SIS en las escuelas de policía

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– deberían elaborarse manuales sobre procedimientos internos – deberían formularse instrucciones actualizadas que reflejen nuevas funciones – antes de poner en marcha Schengen debería organizarse una formación en cascada – deberían proporcionarse cursos de reciclaje una vez que los usuarios finales hayan adquirido cierta experiencia	– en la intranet policial o por otros medios deberían ofrecerse manuales, incluido el manual SIRENE, información, formación y material para ponerse al día – con anterioridad al uso operativo del SIS, un boletín que informe a los usuarios finales de la situación del proyecto puede asegurar y garantizar su interés – la implantación del SIS debería hacerse como una ampliación homogénea de los actuales métodos nacionales de consulta para reducir así la necesidad de formación

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
4. Tratamiento de los datos	
4.1 Introducción, modificación y supresión de descripciones	
– al introducirlas, todas las descripciones han de cumplir los criterios, para garantizar una acción consecutiva a las respuestas positivas (*hit*)	– informar a las autoridades que introducen descripciones en el SIS de las consecuencias de dichas introducciones y, en particular, de la obligación de emprender una acción consecutiva a las respuestas positivas (*hit*) – establecer procedimientos nacionales de determinación de competencias para el envío de solicitudes de extradición y la recuperación de vehículos robados
– estudiar los ficheros relativos a descripciones existentes con arreglo al artículo 95 antes de que estén disponibles para el usuario final	– velar por que el sistema de seguimiento del trabajo de SIRENE emita una advertencia automática al introducir nuevas descripciones con arreglo al artículo 95 – si no ha sido posible validar previamente todos los ficheros relativos a descripciones con arreglo al artículo 95, éstas, sin embargo, se pondrán a disposición de los usuarios finales tan pronto como el sistema se haya abierto a los usuarios finales, sin esperar el resultado del examen del impreso A por parte de SIRENE; en tal caso, han de establecerse procedimientos que garanticen un examen fluido del fichero cuando se ejecute una descripción
– deben respetarse las normas de prioridad y de incompatibilidad	– permitir a los operadores de SIRENE que supriman manualmente las descripciones que no se ajusten a las normas de prioridad y de incompatibilidad – las descripciones “secundarias” sobre una persona han de mantenerse disponibles, de modo que puedan introducirse cuando expire la primera descripción sobre la misma persona, descripción con la que la descripción “secundaria” resultaba incompatible.

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
	– la legislación nacional ha de permitir todas las actuaciones, en particular los controles específicos a tenor del artículo 99
– antes de ampliar una descripción, ha de volver a examinarse si se mantiene su validez y pertinencia – no reutilizar los números de identificación Schengen – reducir al mínimo el tiempo transcurrido entre el incidente y la introducción de una descripción en el SIS – introducir en lo posible de manera automática en el SIS las descripciones que cumplan los criterios Schengen: si el SIRENE tiene que copiarlas manualmente de los sistemas nacionales para introducirlas en el SIS, esto a menudo provoca retrasos	– de preferencia, efectuar la introducción de descripciones en tiempo real – descentralizar en lo posible la introducción de descripciones (especialmente sobre objetos) para evitar los retrasos debidos a procedimientos administrativos internos, como el envío de las descripciones a centros de introducción de datos – cuando no sea posible la introducción directa, proveer modos rápidos de transmisión para enviar la información del nivel local al nivel en que se introduzcan los datos, en particular para las descripciones sobre menores desaparecidos y vehículos robados

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– adoptar medidas de calidad de los datos para evitar que las descripciones SIS se refieran a personas ajenas a ellas	– no volver a asignar un número de matrícula de vehículo mientras sea objeto de una descripción SIS – es práctica habitual que las descripciones se supriman del SIS y se mantengan únicamente en la base de datos nacional al comprobarse, si así lo prevé la legislación nacional, que un vehículo robado ha sido adquirido legalmente por un comprador que ha actuado de buena fe
– fomentar en lo posible la introducción sistemática de descripciones en SIS y establecer criterios nacionales al respecto – en el momento de la introducción, verificar que no se trate de una descripción repetida	– el sistema deberá verificar automáticamente la posible existencia de descripciones repetidas mediante búsquedas que vayan más allá de las correspondencias exactas
4.2 Seguimiento de las respuestas positivas	
– el SIRENE debe ser el único punto de contacto y el conducto de transmisión de toda la información relacionada con el procedimiento subsiguiente a una respuesta positiva – para las descripciones correspondientes al artículo 95, el SIRENE debe ser el único punto de contacto y encargarse del intercambio de información subsiguiente a una respuesta positiva al menos hasta que comience el procedimiento de extradición oficial	– el intercambio de toda información que no requiera una comisión rogatoria se hará a través de SIRENE – cuando sea posible o conveniente, el SIRENE podrá facilitar cualquier nuevo intercambio de información subsiguiente a la detención

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– enviar dentro de los plazos establecidos una respuesta, al menos provisional sobre el estado del caso	– garantizar una disponibilidad las 24 horas del día y los siete días de la semana incluso de las autoridades competentes para tratar con los nacionales de terceros países, u organizarla de tal modo que puedan respetarse los plazos para el suministro de información adicional: podría darse acceso al SIRENE a la base de datos de dichas autoridades
– suprimir las descripciones del SIS cuando desaparezca el motivo de su existencia	- suprimir las descripciones con arreglo al artículo 95 una vez efectuada la extradición - no suprimir las descripciones con arreglo al artículo 96 después de una respuesta positiva - suprimir después de una respuesta positiva las descripciones con arreglo al artículo 97 sobre adultos que no necesiten protección - suprimir las otras descripciones con arreglo al artículo 97 una vez ejecutadas las medidas de protección - suprimir rápidamente las descripciones sobre vehículos robados (incluidas las descripciones repetidas) después de una respuesta positiva para evitar problemas al devolver el vehículo
– establecer procedimientos tendentes a garantizar la rápida ejecución de las actuaciones relativas a objetos perdidos	– determinar las funciones y competencias de las partes interesadas
– facilitar estadísticas sobre las respuestas positivas (*hits*)	– un *hit* es una respuesta positiva obtenida en un Estado Schengen a una descripción emitida en otro Estado Schengen – registrar con precisión todas las respuestas positivas, incluso las relativas a descripciones con arreglo al artículo 96 – clasificar las respuestas positivas por artículo

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
4.3 Medidas acerca de la calidad de los datos	
– introducción automatizada de los datos de SIS, mediante un enlace a las bases de datos nacionales pertinentes y a la N.SIS. – realizar la introducción automática de las descripciones acompañadas de una modificación y supresión automatizadas en tiempo real en el SIS tras cualquier modificación y supresión efectuada en los sistemas nacionales	– esto se cumple cuando la introducción en el SIS está definida como opción por defecto, como se recomienda en el apartado 3.1
– introducir descripciones lo más completas posible	– cotejar los datos de las descripciones, de preferencia de forma automatizada, con los que se conservan en los registros nacionales – actualizar las descripciones, incorporando información adicional, como el número de documento de un documento expedido o el número del bastidor de un vehículo robado, tan pronto como se conozca – el SIRENE del país de origen de un objeto robado ha de facilitar información adicional para actualizar la descripción

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– SIRENE ha de hacer las veces de gestor de garantía de la calidad de los datos – SIRENE debe validar toda descripción introducida con arreglo al artículo 95	– el SIRENE dispondrá de la competencia nacional y los medios técnicos y operativos para garantizar la calidad de los datos, lo que incluirá el acceso a las bases de datos nacionales, efectuará un muestreo encapsulado dual en línea (*dip-sample*) de todas las categorías de descripciones – el SIRENE participará en la formación de los usuarios – cotejar la lista de respuestas positivas con la de descripciones suprimidas – revisar y estudiar el coeficiente de descripciones y respuestas positivas – consultar periódicamente con las autoridades locales la necesidad de mantener las descripciones sobre menores desaparecidos
– respetar las normas de transliteración	– facilitar a los usuarios finales información específica sobre normas de transliteración
– formar a los usuarios finales en relación con las medidas de calidad de los datos	– no permitir la introducción de información que no pueda detectarse, p. ej. escribir la palabra “desconocido” en las casillas obligatorias o dejar en blanco las optativas en lugar de escribir “desconocido” o “?”

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
5. Seguridad	
5.1 Planificación del trabajo relativo a la seguridad de los datos	
– la definición de una política de seguridad para los sistemas de TI de Schengen (N.SIS, C.SIS, SIRENE y sistemas destinados a usuarios finales) debería ser parte integrante de la definición de la política de seguridad global de las autoridades que se ocupan de dichos sistemas – las autoridades competentes deben documentar por escrito la política de seguridad adoptada – es crucial asignar los recursos necesarios para preparar y mantener medidas de seguridad – a nivel nacional, deberían establecerse procedimientos y ámbitos de responsabilidad para garantizar que todas las medidas de seguridad se actualicen y revisen continuamente – la actualización o revisión debería llevarse a cabo, en la medida de lo posible, cada año, para que se adecuen constantemente y reflejen las condiciones existentes – además, deberían realizarse actualizaciones y revisiones tras incidentes significativos/graves o a raíz de modificaciones del sistema que tengan consecuencias para la seguridad de los datos	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
5.2 Organización de la seguridad	
– cuando sea conveniente, deberían planificarse esfuerzos para garantizar la seguridad de los datos en el marco de una organización de seguridad, que puede incluir una o varias autoridades	
– deberían definirse claramente las responsabilidades y la autoridad delegada a las personas implicadas en la seguridad de los datos, posiblemente en relación con las especificaciones del trabajo para las personas de que se trate – en principio, será conveniente facilitar documentación de la organización de los trabajos de seguridad mediante un cuadro organizativo	
5.3 Control de las partes importantes	
– hay que garantizar que se conocen todas las partes importantes de los sistemas, para que puedan protegerse en función de su importancia – por ello, debería llevarse un registro del equipo TI pertinente de forma continua – además, debería disponerse de documentación actualizada de la red y los sistemas que ponga de manifiesto, por ejemplo, la conexión y la funcionalidad de los elementos específicos del sistema	
5.4 Seguridad del personal	
– sólo podrán tener acceso a los datos del SIS y a los equipos utilizados para procesar los datos del SIS personas con autorización específica – sólo se podrá acceder al SIS cuando sea preciso para llevar a cabo las tareas de las que sea responsable el usuario	– investigación del personal como parte del procedimiento de selección y posteriormente cada 5 años

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– las descripciones de los trabajos del personal que puede acceder a los datos del SIS y a los equipos utilizados para procesar datos del SIS deberían incluir información sobre las responsabilidades relativas a la seguridad	
– las prácticas de selección de personal deberían valorar los conocimientos sobre seguridad de datos – este personal debe recibir el correspondiente programa de formación del usuario, que ha de incluir todas las disposiciones actuales sobre seguridad de datos – se celebrarán acuerdos de confidencialidad y secreto con todas las personas que no pertenezcan a una autoridad nacional – dichas personas deberán tener la autorización o certificación necesaria – sólo deberían tener acceso a los datos del SIS cuando sea preciso para la realización de sus cometidos – deben definirse cadenas de mando y procedimientos para garantizar que se comuniquen cuanto antes los incidentes o las sospechas de incidentes relativos a la seguridad – todo el personal interno y los contratistas externos deben conocer el procedimiento – deben llevarse a cabo consultas para garantizar que se ha comunicado la información relativa a los resultados cuando un incidente haya sido tratado y haya finalizado – cualquier infracción de las normas de seguridad se sancionará en la medida necesaria, en conformidad con la legislación nacional	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
5.5 Seguridad física	
– las instalaciones de tratamiento de datos SIS (N.SIS, C.SIS y SIRENE) y demás recursos fundamentales o sensibles del SIS, como las zonas de almacenamiento de soportes, deben estar ubicadas en zonas seguras, cada una protegida por un perímetro de seguridad definido con barreras físicas y controles de entrada apropiados	– es deseable una zona de seguridad de clase II según la definición de la Decisión del Consejo de 19 de marzo de 2001 [1] por lo que respecta al manejo de todos los datos del SIS (en la medida en que en las instalaciones de tratamiento de datos del SIS se maneje información confidencial de la UE, es necesaria en cualquier caso al menos una zona de seguridad de clase II) – ubicación subterránea de ordenadores – diferentes zonas de seguridad – tarjetas de acceso – vigilantes – control mediante circuito cerrado de televisión
– la zona debe estar adecuadamente protegida contra todo tipo de intrusión	
– la construcción de los muros externos debe ser sólida y las puertas de acceso deben estar convenientemente protegidas contra el acceso no autorizado, por ejemplo con mecanismos de control, barreras, alarmas y cerraduras	
– el edificio o el lugar en el que se encuentren las instalaciones de tratamiento de datos SIS debe disponer de una zona de recepción atendida o de otros medios de control del acceso físico	
– el acceso a las zonas de seguridad en las que se encuentren las instalaciones de tratamiento de datos SIS y de almacenamiento de soportes debe estar controlado y restringido a las personas autorizadas	– control de las entradas y salidas

[1] Decisión del Consejo 2001/264/CE por la que se adoptan las normas de seguridad del Consejo, publicada en el DO L 101 de 11.04.2001, p. 1.

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– deberían supervisarse o someterse a autorización las visitas a las zonas de seguridad – sólo debería permitirse el acceso de visitantes con objetivos específicos y autorizados – el personal de los servicios de asistencia de terceras partes sólo debería tener acceso restringido a las zonas de seguridad en caso de necesidad – dicho acceso debe someterse a autorización y supervisarse	
5.6 Seguridad de los equipos	
– todos los equipos utilizados para procesar o almacenar datos del SIS deben estar protegidos contra daños y pérdidas no intencionados y acceso no autorizado	
5.6.1 Equipos de tratamiento de datos del SIS	
– los equipos de tratamiento de datos del SIS deben estar ubicados en una zona en la que el acceso esté reducido al mínimo – deben realizarse supervisiones continuas para reducir al mínimo el riesgo de amenazas potenciales, incluidos los atentados criminales o terroristas, el incendio, el recalentamiento por fallo en el control de la climatización, el derrumbamiento de la estructura tras una explosión y la inundación – para lograr la continuidad del suministro de energía, debe disponerse de los siguientes equipos, que se verificarán y comprobarán periódicamente: • un suministro de energía ininterrumpido (UPS) que mantenga activas las funciones esenciales • un generador auxiliar para el proceso continuado en caso de interrupción prolongada del suministro de energía	– sistemas de detección de incendio, calor y humo – sistema automático de extinción de incendios – aire acondicionado suficiente
– los cables de telecomunicación deben estar protegidos en la medida necesaria	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– los equipos de red electrónica deben estar instalados en salas cerradas o despachos cerrados – únicamente el personal de mantenimiento autorizado puede llevar a cabo las reparaciones y el mantenimiento de los equipos – sistema de seguridad separado, control periódico del conmutador entre sistema de seguridad y sistema operativo	– reserva activa y pasiva o duplicación simultánea exacta – en una ubicación remota para que un siniestro que se produzca en un lugar no afecte al otro
5.6.2 Terminales y puestos de trabajo en ordenadores personales	
– los terminales**,** puestos de trabajo en ordenadores personales e impresoras deben estar ubicados de modo que se garantice que personas no autorizadas no puedan leer los datos que contienen deberían establecerse procedimientos para controlar las impresiones de pantallas y de listas de datos del SIS. – las sesiones con ordenadores personales y terminales deben terminar automáticamente tras un período de inactividad y estar protegidos con dispositivos de cierre, claves de acceso u otras medidas de control cuando no estén siendo utilizados – los terminales, puestos de trabajo en ordenadores personales e impresoras que estén instalados en salas a las que tenga acceso el público en general deben encontrarse constantemente bajo control	
5.7 Gestión de las comunicaciones y del funcionamiento	
5.7.1 Procedimientos de funcionamiento y responsabilidad	
– los procedimientos de funcionamiento establecidos por cada Estado Schengen deben documentarse y actualizarse continuamente – como mínimo, deben incluir lo siguiente:	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
• procedimientos para las medidas de funcionamiento diario como la salvaguarda, la actualización anti-virus, la supervisión de la red, etc. • procedimientos para el tratamiento de los soportes de datos y demás partes esenciales • procedimientos relativos a las restricciones de acceso • instrucciones sobre cómo tratar los errores u otras condiciones excepcionales • contactos de asistencia en caso de funcionamiento imprevisto o de dificultades técnicas • procedimientos para reiniciar y restaurar el sistema tras cualquier fallo del mismo – debería garantizarse un control satisfactorio de todas las modificaciones de las instalaciones y los sistemas de tratamiento de datos SIS, incluyendo los equipos, programas o procedimientos – deben existir instrucciones relativas a la responsabilidad y procedimientos claros para su tratamiento	
5.7.2 Procedimientos para la gestión de incidentes	
– deben existir planes de emergencia y procedimientos de cadena de alerta que se utilizarán para resolver incidentes que puedan interrumpir potencialmente el funcionamiento del sistema y causar una inaccesibilidad total o parcial de los sistemas de TI de Schengen – deben definirse procedimientos para la detección y el tratamiento de incidentes que aunque no den lugar a una inaccesibilidad total del sistema, comprometan la seguridad de los datos	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
5.7.3 Protección contra programas nocivos	
– para proteger la integridad de la programación y de los datos, debería tomarse una serie de medidas de seguridad para prevenir y detectar la intrusión de programas nocivos y contribuir a restaurar posteriormente los sistemas – entre dichas medidas deberían figurar medidas de control para la protección contra los virus, parásitos, programas disimulados y demás programas nocivos – como mínimo, deberían incluirse los siguientes elementos: • una política formal que requiera el cumplimiento de las licencias de programas y la prohibición del uso de programas no autorizados • se ha de instalar en todos los ordenadores personales un programa de detección anti-virus y de reparación con actualizaciones periódicas de definición de virus y escaneado en servidores, ordenadores personales y ordenadores portátiles; si hay excepciones, deberán ilustrarse • se verificarán todos los archivos que se adjunten en correos electrónicos y las descargas de la red antes de su utilización por lo que respecta a programas nocivos; debería precisarse dónde se llevará a cabo esta verificación: por ejemplo, en los servidores de correo electrónico o al entrar en la red • debe disponerse de procedimientos formales para reaccionar contra incidentes relacionados con virus	– prohibir los archivos adjuntos que sean archivos .exe, que estén codificados, que contengan macros o palabras clave, …
5.7.4 Copia de seguridad	
– se realizarán periódicamente copias de seguridad de los datos SIS, archivos de configuración y aplicaciones	– hacer copias diarias

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– todos los sistemas de seguridad debe comprobarse periódicamente para garantizar su conformidad con los requisitos de los planes operativos	
– los datos de las copias de seguridad deben estar sometidos a la protección física requerida y estar situados en lugares geográficamente distintos	– guardar copias al menos en dos lugares distintos
– debe controlarse y comprobarse periódicamente los procedimientos de restauración	– dos veces al año
5.7.5 Gestión de la red	
– la transmisión nacional de datos del SIS sólo puede utilizar redes que estén protegidas contra el acceso no autorizado	– red/radio/fax codificados
– debe supervisarse constantemente las redes	
– hay que adoptar medidas para proteger la confidencialidad de los datos del SIS durante la transmisión por redes de comunicación	– comunicaciones seguras entre las oficinas SIRENE y sobre el terreno / funcionarios operativos para el intercambio de datos de carácter personal
– no debe ser posible acceder a los datos del SIS desde redes públicas como Internet	– evitar que sea posible acceder a Internet a través de la red policial
– debe protegerse la transmisión de claves de acceso y demás elementos de seguridad mediante métodos de cifrado	
5.7.6 Tratamiento de los soportes de datos	
– debe restringirse al mínimo necesario el número de copias técnicas de datos del SIS (véase el apartado 2 del artículo 102)	
– deben establecerse procedimientos para el tratamiento y almacenamiento de datos del SIS, con objeto de proteger dichos datos de retransmisiones no autorizadas o usos indebidos	
– dichos procedimientos deberían incluir:	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
• sólo debería tener acceso a los soportes informáticos de almacenamiento que contengan datos del SIS el personal autorizado • deben marcarse adecuadamente todos los soportes que contengan datos del SIS y protegerse adecuadamente durante su transporte • los soportes obsoletos o que hayan dejado de ser necesarios deben inutilizarse o, en caso de volver a ser utilizados, tratarse de forma que se eliminen todos los datos del SIS – los archivos deberían disponer de medidas de seguridad – el acceso a los archivos debería estar controlado y restringido al personal autorizado – dicho acceso debería controlarse y quedar registrado – los archivos deberían estar gestionados de modo que se garantice el cumplimiento de las normas de supresión	– las actualizaciones de la base de datos del SIS que se remitan a las oficinas consultares deberían enviarse en soportes codificados y por valija diplomático – evitar la difusión de datos por error debido a un reciclado inadecuado del material, incluido el papel – sustitución de soportes por parte de las autoridades competentes o empresas autorizadas y controladas – procedimientos para el almacenamiento y la destrucción de material / política de mesa limpia – los archivos electrónicos ofrecen las mayores garantías de seguridad, dotados de una clave para el acceso y la utilización de los mismos, así como facilidades para la auditoría – los archivos electrónicos pueden incluir funciones automáticas de depuración y supresión – en el caso de los archivos físicos, se estimó que la mejor solución sería la combinación de una tarjeta magnética y un código personal de acceso a los archivos – debería evitarse hacer impresiones de los archivos electrónicos, que deben destruirse en cualquier caso tras ser utilizadas
5.8 Control del acceso de los usuarios	
– debe existir un procedimiento de registro y de "desregistro" del usuario para conceder acceso a los distintos sistemas y servicios – dicho procedimiento debe incluir:	– validación de las consultas por muestreo

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
• utilizar claves de identificación del usuario únicas, para que las actuaciones de los usuarios individuales puedan contabilizarse y se pueda responsabilizar a los usuarios de sus actuaciones; por ello, no se debe permitir la utilización de claves de identificación de grupo • cada usuario debe disponer únicamente de una serie mínima de derechos de acceso necesarios para la ejecución normal de su cometido	
• supresión inmediata de los derechos de acceso a los datos del SIS siempre que los respectivos usuarios dejen de ejercer funciones que impliquen la necesidad de dicho acceso	– la aplicación puede incluir una función técnica para cerrar automáticamente la cuenta de un usuario cuando no se haya hecho uso de ella p. ej. en dos semanas
• verificación periódica de que el nivel de acceso concedido es acorde con el perfil del usuario	
• verificación periódica y supresión de las claves de identificación y cuentas de usuario redundantes	– la clave de identificación y la cuenta pueden vincularse automáticamente a la categoría del personal
– la asignación y administración de claves de acceso debe controlarse mediante un procedimiento formal que garantice que: • los usuarios estén informados sobre sus obligaciones relativas a sus claves de acceso y sean conscientes de las mismas • las claves de acceso se comuniquen a los usuarios de un modo seguro	
• se pida a los usuarios que cambien periódicamente sus claves de acceso y se rechace la reutilización de claves de acceso	– la clave de acceso debería cambiarse cada 60-90 días
• nunca se almacenen claves de acceso en el sistema informático sin protección	
– se establecerá un procedimiento para garantizar la revisión periódica de todos los derechos de acceso de los usuarios	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
5.9 Control del acceso al sistema y de su utilización	
– la utilización nacional de los sistemas de TI de Schengen debe supervisarse con objeto de garantizar la detección de actividades no autorizadas – la transmisión de datos de carácter personal deberá registrarse de conformidad con el artículo 103 del Convenio de Schengen – registro de las conexiones del usuario y, en la medida de lo posible, de las desconexiones; los intentos de conexión o conexiones fallidas y los intentos de utilización no autorizada de datos deberían almacenarse durante el periodo que establece el artículo 103 – los datos registrados deberían incluir la clave de identificación del usuario, la fecha y la hora del incidente y, si es posible, la identidad y la ubicación del terminal	– los registros de actuaciones y de auditoría relativos a los archivos SIRENE deberían supervisarse constantemente como medida preventiva y conservarse durante un periodo suficientemente largo, según el Derecho interno – un sistema informatizado de seguimiento del trabajo y gestión de casos ofrece los mejores medios para asegurarse de que cada acción llevada a cabo en un archivo SIRENE queda registrada y auditada
5.10 Desarrollo y mantenimiento	
– para reducir al mínimo el riesgo de daño a los sistemas operativos, deben establecerse medidas de control de seguridad para datos y programas	
– debería garantizarse que, por ejemplo, la actualización de los sistemas operativos, incluyendo la colección de programas, sólo se ejecute con aprobación previa – antes de que se conceda la aprobación, debe garantizarse que la actualización se ha ensayado y documentado satisfactoriamente	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
– debe disponerse de un sistema de pruebas separado del entorno de producción, para que los cambios puedan ensayarse antes de que sean operativos y para que no se introduzcan en el sistema operativo datos que no hayan sido ensayados – debería evitarse cualquier utilización de datos reales del SIS a efectos de prueba, a menos que se hayan convertido en anónimos	
5.11 Planes de emergencia	
– cada Estado Schengen debe establecer y aplicar medidas planificadas de emergencia adecuadas, teniendo en cuenta, por ejemplo, las situaciones siguientes: • se constata la inaccesibilidad de un N.SIS o de la red • algunos usuarios o los usuarios en su totalidad no pueden consultar los datos del SIS a causa de problemas en la infraestructura TI nacional – los planes de emergencia deben basarse en una evaluación del riesgo de amenazas que puedan desembocar en una inaccesibilidad del sistema y de las repercusiones de esas amenazas en los demás Estados Schengen – como mínimo, los planes de emergencia deben incluir lo siguiente:	
• criterios para la ejecución de los planes y medidas que se han de tomar inmediatamente para evaluar la situación • procedimientos de cadena de alerta, con arreglo a los procedimientos acordados para los Estados Schengen, con vistas a informar a las autoridades nacionales de gestión, al C.SIS y a los demás Estados Schengen	

RECOMENDACIONES	PRÁCTICAS MÁS IDÓNEAS
• procedimientos de emergencia que describan las medidas que se han de adoptar tras un incidente que interfiera en la accesibilidad del sistema • procedimientos auxiliares que describan las medidas que se han de adoptar para desviar las operaciones esenciales del N.SIS a servidores temporales alternativos • procedimientos de restauración que describan medidas que se han de adoptar para restaurar el funcionamiento normal – los planes de emergencia deben actualizarse periódicamente, al igual que los procedimientos rutinarios del personal	
5.12 Control	
– deben establecerse procedimientos para garantizar el control continuo del cumplimiento de todas las normas aplicables nacionales y de la UE	– auditorías de seguridad periódicas llevadas a cabo por personal externo al departamento de TI

La finalidad del Catálogo es aclarar y detallar el acervo de Schengen, dar un ejemplo a los Estados que se adhieran a Schengen y a los que ya están aplicando en su totalidad el acervo de Schengen.

El primer volumen del Catálogo se publicó en febrero de 2002, y trata sobre los controles en las fronteras exteriores y la expulsión y readmisión. Este segundo volumen aborda específicamente el Sistema de Información de Schengen y SIRENE, y ofrece a los países candidatos a la adhesión a la Unión Europea una buena indicación de lo que se espera de ellos, especialmente en términos prácticos, por lo que respecta a Schengen.