Guía para evaluar la seguridad en el manejo y emisión de documentos de viaje

Versión 3.4

Enero de 2010

Resumen ejecutivo

La integridad de los pasaportes y otros documentos de viaje es un componente clave de las estrategias nacionales e internacionales contra el crimen y el terrorismo. Debido a que los documentos de viaje pueden ser herramientas poderosas en manos de criminales y terroristas, controlar la seguridad y los procesos de emisión de documentos de viaje tiene un impacto directo no solamente en la seguridad nacional e internacional, sino también en el respeto internacional por la integridad del documento.

En años recientes, el desarrollo acelerado de nuevas tecnologías y técnicas de seguridad ha conllevado un giro en el fraude de documentos de viaje. En el pasado, quienes cometían fraudes se concentraban en el final de la cadena de producción del documento falsificando o alterando el documento físico. Hoy en día, concentran sus esfuerzos en el inicio de la cadena, a saber, en los sistemas de emisión de documentos, así como en cualquier registro del documento. De ahí que los países deban prestar particular atención a la seguridad en cuanto a los procesos de manejo y emisión, a fin de prevenir que se expidan documentos legítimos con identidades falsas a favor de terroristas o criminales.

Durante la reunión No. 17 del Grupo Técnico Asesor sobre Documentos de Viaje de Lectura Mecánica (TAG-MRTD 17), se aprobó un proyecto para producir una herramienta práctica de orientación común que ayude a los Estados Miembros de la OACI a autoevaluar o a apoyar la evaluación de la seguridad del sistema de manejo y emisión de documentos de viaje de otros países.

La Guía se divide en dos partes:

1) En la primera parte se recomiendan una serie de buenas prácticas para prevenir y mitigar las amenazas a la seguridad en cada paso del proceso de emisión de pasaportes.
2) En la segunda parte se expone una herramienta de evaluación exhaustiva en la forma de listas de verificación, que permitirá valorar las vulnerabilidades en el proceso de emisión.

Las medidas y prácticas que se presentan en este documento constituyen prácticas recomendadas, y como tales ningún país está en obligación de adoptarlas.
Esta guía fue elaborada y será periódicamente actualizada por el Grupo de Trabajo sobre Implementación y Fortalecimiento de Capacidades (ICBWG) de la Organización de Aviación Civil Internacional. Las preguntas, comentarios y observaciones sobre sus contenidos deben dirigirse al ese Grupo de trabajo a la dirección de correo ICBWG@icao.int.

Tabla de control de cambios introducidos a este documento

Número de versión	Fecha de emisión	Breve descripción de los cambios
1.1	07 enero 2008	Primer borrador
1.2	18 enero 2008	Modificaciones a la estructura/edición – envío al NTWG
1.3	10 abril 2008	Producido después de discusiones del NTWG en Christchurch, enviado al TAG
1.4	15 mayo 2008	Actualización después de Reunión del TAG 18
2.0	30 septiembre 2008	Incorporación de observaciones y modificaciones a la estructura; enviado a ICBWG
3.0	10 marzo 2009	Desarrollo Parte 2— Listas de verificación Revisión y adición de texto en todos los capítulos de la Parte I Harmonización de la Parte 1 y la Parte 2
3.1	29 junio 2009	Cambios editoriales
3.2	12 agosto 2009	Comentarios Post Tavira y La Haya
3.3	Octubre 2009	Observaciones finales del ICBWG a partir de Reunión de Cabo Verde.
3.4	Enero 2010	Observaciones de TAG/MRTD de Australia

Índice

Introducción

A) La función de los documentos de viaje en la seguridad nacional e internacional

Los pasaportes y otros documentos de viaje son documentos oficiales internacionalmente reconocidos que consignan la identidad y ciudadanía de una persona para efectos de facilitar los viajes al exterior. Son utilizados por las autoridades fronterizas y migratorias para determinar la admisibilidad y legitimidad de quienes deseen cruzar las fronteras internacionales e ingresar al territorio de otro país. También son utilizados por el país emisor para permitir el reingreso al territorio nacional. El pasaporte le permite al titular solicitar una visa de ingreso a los países que la requieran, a la vez que la autoridad hace la anotación en el pasaporte y registra las fechas de ingreso y de salida.

Además de los propósitos de viaje, el pasaporte es un documento de identidad de uso cada vez más frecuente para otros tipos de transacciones en el sector público y el privado, por ejemplo para la apertura de cuentas corrientes, como apoyo en la realización de transacciones financieras o para acceder a los servicios y beneficios que ofrece el Estado.

Los documentos de viaje, ya sea que fuesen debidamente obtenidos o no o que sean alterados, constituyen herramientas deseables para los criminales y delincuentes y grupos terroristas. En manos de criminales, pueden ser mal utilizados de forma organizada para financiar actividades ilícitas, facilitar la migración ilegal, el tráfico de migrantes y la trata de personas, así como el contrabando de bienes o el narcotráfico. Un pasaporte fraudulento puede ser utilizado para el espionaje, para cometer delitos financieros, para huir y evitar así el enjuiciamiento o para facilitar otros crímenes o delitos. También puede permitirle a un terrorista viajar – reclutar, trabajar en redes, movilizar, financiar y organizarse a escala internacional. Sin la capacidad de trasladarse libremente que da un documentos de viaje, los terroristas pueden verse impedidos, ser localizados, ver sus finanzas minimizadas e incluso cabe la posibilidad de que sean puestos "en cuarentena", por lo que su alcance e impacto se verán impedidos. En efecto, un pasaporte u otro documento de viaje puede ser la medida de seguridad que evite que los terroristas lleguen a su objetivo.

Los criminales y sus organizaciones están dispuestos a pagar cuantiosas sumas de dinero para obtener documentos de viaje de manera ilegal, así como para tener acceso a la información personal que sea recolectada, procesada y almacenada como parte del proceso de emisión del documento. Esto significa que la integridad del documento de viaje y su proceso de emisión pueden ser en extremo vulnerables al fraude, la manipulación y los actos ilegales.

Con los acelerados avances recientes en el campo tecnológico, los documentos de viaje en sí mismos son cada vez más seguros. Debido a que los documentos de viaje son más seguros y difíciles de alterar, los estafadores pasan de alterarlos, a procurar obtener documentos auténticos por otras vías ilícitas. Hoy en día se reconoce que los sistemas de emisión de documentos de viaje se convertirán en objetivo de la criminalidad, al igual que cualquier otro documento o registro que pueda ser considerado un documento madre o registro auténtico (esto es, registro de nacimiento). Por consiguiente, la Autoridad Emisora de Documentos de Viaje (AEDV), así como cualquier organización involucrada en la producción de documentos de viaje, debe preocuparse más por la seguridad en el proceso de manejo y emisión. Es posible que un país cuente con pasaportes sumamente seguros, pero si la identidad de una persona no puede establecerse más allá de toda duda o si un documento legítimo es expedido a favor de una persona que no tiene el derecho legítimo de portarlo, la calidad del documento será de muy poca importancia.

Las amenazas al proceso de emisión de documentos pueden desglosarse en varios tipos principales:

- El robo de documentos en blanco y de materiales para su producción para elaborar documentos fraudulentos (incluyendo el acceso no autorizado a las instalaciones de producción y emisión y/o el acceso no autorizado a los sistemas de procesamiento).
- La solicitud de un documentos de viaje bajo una identidad falsa utilizando un documento madre falsificado, robado o auténtico.
- La solicitud de un documento de viaje bajo una identidad falsa utilizando evidencia falsa manufacturada de la nacionalidad y/o la identidad.
- La solicitud de múltiples documentos de viaje de forma que un viajero pueda ocultar viajes anteriores que resulten sospechosos utilizando como evidencia visas y sellos de entrada y de salida obtenidos de personal de los cruces fronterizos.
- El uso de documentos de viaje falsamente declarados o no declarados como perdidos o robados.
- Comisión de actos ilegales por parte del personal.
- Solicitud de un documento de viaje con la intención de dárselo o vendérselo a una persona que no tenga derecho a utilizarlo y que se asemeje al titular auténtico.

Controlar la seguridad del proceso de emisión de pasaportes de un país no tiene solamente un impacto directo en la seguridad nacional e internacional, sino también en el respeto internacional de que goce la integridad del documento, integridad que es de fundamental importancia, en especial cuando éste es presentado por un ciudadano o ciudadana para solicitar una visa y en los cruces fronterizos. También puede incidir en los requisitos de ingreso de otras naciones. El nivel de seguridad y el prestigio de un pasaporte pueden tener serias repercusiones en la conveniencia y facilidad con que se efectúe el cruce de fronteras internacionales para los ciudadanos y ciudadanas de un país. La integridad del pasaporte y otros documentos de viaje es un componente clave de las estrategias nacionales e internacionales contra el crimen y el terrorismo.

Si bien la integridad del pasaporte es un elemento necesario para la seguridad nacional e internacional, las autoridades emisoras también enfrentan el desafío de encontrar el equilibrio correcto entre seguridad, servicio, privacidad y costos. Sin embargo, la prevención del fraude es sin duda alguna más eficiente y resulta mucho menos onerosa que enfrentar las consecuencias de un fraude exitoso.

Ningún país es inmune al fraude todavía y si bien es imposible eliminar en un 100 por ciento las amenazas y vulnerabilidades, una combinación de diversas características y métodos servirá para mitigar los riesgos, manteniéndolos en un nivel aceptable y suficiente para disuadir a quienes tengan potencialmente intereses criminales.

La presente guía es una herramienta de información para las organizaciones involucradas en el proceso de emisión de documentos de viaje. Aquí se esbozan las mejores prácticas en materia de seguridad y también se apoyan los esfuerzos para evaluar el desempeño del proceso de emisión desde el punto de vista de la seguridad.

B) La Organización de Aviación Civil Internacional (OACI)

La Organización de Aviación Civil Internacional (OACI) fue establecida mediante el *Convenio sobre Aviación Civil Internacional (Convenio de Chicago)* de 1944. La OACI desempeña desde hace muchos años un papel fundamental en la definición de normas, prácticas recomendadas y especificaciones para la emisión de documentos de viaje. En la Sección 3 del Anexo 9 (Facilitación) del Convenio de Chicago se presentan las normas y prácticas recomendadas con respecto a los pasaportes y otros documentos de viaje.

En 1984, el Secretario General de la OACI conformó el Grupo asesor técnico sobre los documentos de viaje de lectura mecánica (TAG/MRTD), el cual está conformado por expertos provenientes de varios Estados Miembros de la OACI. Este grupo asesor tiene a su cargo el desarrollo y adopción de especificaciones para los Documentos de Viaje de Lectura Mecánica

(DVLM) y los pasaportes de lectura mecánica electrónicos (PLM-e), las cuales están contenidas en el Documento 9303. El TAG/MRTD también publica materiales de orientación para apoyar a los Estados Miembros en la implementación de sus especificaciones, además de informes técnicos y documentos informativos. Dos grupos de trabajo se conformaron bajo la rectoría del TAG/MRTD: el Grupo de trabajo sobre nuevas tecnologías (NTWG) y el Grupo de Trabajo sobre Implementación y Fortalecimiento de Capacidades (ICBWG).

La propuesta de una Guía para evaluar las normas de seguridad para el manejo y emisión de documentos de viaje se presentó durante la séptima reunión del TAG/MRTD celebrada en marzo del 2007, cuando obtuvo el aval de los participantes.

Recursos en Internet:

- ⇒ Programa OACI DVLM: http://www2.icao.int/en/MRTD/Pages/default.aspx
- ⇒ Documento 9303 (Este documento debe ser solicitado a la OACI): http://icaodsu.openface.ca/mainpage.ch2

C) Propósito de la Guía

La importancia de garantizar el proceso de emisión de documentos de viaje es bien conocida, aunque la existencia de lineamientos para la adopción de medidas recomendadas de prevención y mitigación es limitada. "¿Es nuestro sistema de emisión seguro?"; "¿cuáles medidas de seguridad son las más efectivas y eficientes?"; "¿por dónde debemos empezar?" son solo algunas de las interrogantes que los países y organizaciones involucradas en el proceso de emisión de documentos de viaje se plantean. En respuesta, esta Guía ofrece una referencia completa y sencilla sobre el tema de la seguridad. En ella se presentan las mejores prácticas en materia de seguridad para prevenir y mitigar las amenazas y ataques al proceso de emisión. Además, contiene una herramienta de autoevaluación para ayudar a las organizaciones a identificar sus vulnerabilidades.

Esta Guía fue escrita desde la perspectiva de la emisión de pasaportes en los países sin cédula u otro documento nacional de identidad u otras disposiciones universales para el registro de identidad de sus nacionales. En los países en que las disposiciones relativas al registro civil incluyen un sistema de inscripción universal y/o un régimen de cédulas de identidad o similares, la emisión de pasaportes puede gestionarse como un proceso simplificado que dependa de la integridad de la inscripción anterior para obtener la cédula nacional de identidad o similar. En estos casos, los controles descritos aquí para gestionar la emisión de pasaportes continúan siendo esenciales, pero se llevan a cabo antes de que se solicite el pasaporte, en un proceso aparte del registro civil. Por lo tanto, el contenido de esta Guía sigue siendo relevante para todos los sistemas de emisión de pasaportes, aunque es posible que las secciones sobre inscripción y verificación de la identidad tengan que leerse como si aplicaran al registro civil así como a la emisión de pasaportes.

Aunque esta publicación puede ser utilizada por los estados para evaluar la seguridad en la manejo y emisión de sus documentos de viaje e introducir mejoras en los casos en que se identifiquen deficiencias, el ICBWG de la OACI recomienda firmemente el uso de evaluadores calificados. El ICBWG puede recomendar evaluadores que estén familiarizados con esta Guía y que tengan experiencia en todos los aspectos relevantes del proceso relacionado con los documentos de viaje. Los evaluadores realizan un análisis objetivo y exhaustivo del proceso de emisión de documentos de viaje del Estado en cuestión y redactan un informe confidencial para el Gobierno solicitante. La participación de evaluadores calificados es esencial en los casos en que el Estado planee utilizar el informe para procurar asistencia para el desarrollo de capacidades.

Varias organizaciones nacionales e internacionales han tenido una participación activa en todo el mundo en las actividades de divulgación y desarrollo de capacidades destinadas a mejorar la seguridad de los documentos de viaje y sus procesos de emisión. En esta Guía se reconoce el

trabajo de estas organizaciones y se hace un inventario de sus actividades y logros. En particular, con el auspicio de Subgrupo de Expertos sobre Migraciones (SGEM) se elaboró un documento con el título de "Normas mínimas de seguridad para la manejo de DVLM y otros pasaportes", posteriormente adoptado como el Anexo informativo III de la Sección III del Documento 9303. Este valioso documento, en que se aborda primordialmente el fraude en el ámbito interno, sirvió de base para la elaboración de la presente Guía.

Público meta

Esta Guía tiene por objetivo:

- orientar a los encargados de la formulación de políticas de los organismos emisores y/o involucrados en la producción de documentos de viaje para que evalúen su propia situación;
- apoyar al ICBWG de la OACI y a otras organizaciones internacionales con propósitos de divulgación, asistencia para el desarrollo de capacidades y realización de auditorías;
- prestar asistencia a los gobiernos para que evalúen a otros Estados; esto es, aquéllos que estén siendo considerados para optar por el programa de exención de visas.

Alcance

Esta Guía ofrece las mejores prácticas y recomendaciones relacionadas con el proceso de emisión de pasaportes y otros documentos de viaje. La mayoría de las prácticas y recomendaciones aplican por igual a otros documentos de identidad. Las prácticas aplican tanto a organismos gubernamentales como no gubernamentales e instalaciones involucradas en todas las etapas del proceso de emisión de pasaportes.

Las medidas y prácticas expuestas en este documento constituyen recomendaciones y, como tales, ningún país está en la obligación de adoptarlas. Depende de cada país determinar, de acuerdo a su propio marco jurídico, administrativo y de políticas, además de sus usos y costumbres, las prácticas que ha de adoptar.

Esta Guía aborda primordialmente el primer paso del ciclo de vida del pasaporte, a saber el proceso de emisión. Este incluye:

- recepción de las solicitudes;
- los procesos de toma de decisiones y de negocios para establecer la identidad, ciudadanía y restricciones de viaje de un individuo;
- la producción; y
- la entrega del documento.

Es importante anotar que las medidas adoptadas para mejorar la seguridad del proceso de emisión podrían tener también un impacto directo o indirecto en otros pasos del ciclo de vida del pasaporte como la autenticación, validación y rechazo.

Estructura

Parte 1: Buenas prácticas sobre la emisión segura de documentos de viaje. En esta sección se recomiendan las prácticas más recomendadas desde el punto de vista de la seguridad para cada paso del proceso de emisión de pasaportes. Se divide en 12 capítulos.

Parte 2: Guía para la evaluación. En esta sección se presenta una herramienta de evaluación exhaustiva para valorar las vulnerabilidades en el proceso de emisión, siguiendo las recomendaciones y organización por capítulos de la Parte 1.

Guía para evaluar la seguridad en la manejo y emisión de documentos de viaje

PARTE 1: BUENAS PRÁCTICAS SOBRE LA EMISIÓN SEGURA DE DOCUMENTOS DE VIAJE

1. Autoridad Emisora de Documentos de Viaje: estructura organizativa, seguridad interna y prácticas generales sobre seguridad
2. Procesos de solicitud
3. Procesos de verificación de la titularidad
4. Tratamiento de los materiales y libretas en blanco
5. Personalización y entrega
6. Seguridad de los documentos
7. Seguridad de las instalaciones
8. Seguridad informática
9. Integridad del personal e interna
10. Documentos de viaje perdidos y robados
11. Emisión de documentos en el exterior
12. Actores clave nacionales e internacionales

1 La autoridad emisora de documentos de viaje: estructura organizativa, seguridad interna y prácticas generales de seguridad

1.1 Resumen

En general, la Autoridad Emisora de Documentos de Viaje (AEDV) supervisa la recepción y procesamiento de las solicitudes, la verificación de la titularidad de las personas solicitantes, así como la producción y emisión de los documentos de viaje.

En cada capítulo se cubre un aspecto, paso o fase en particular del continuo. Esta sección se centra en la estructura organizativa general y el marco de políticas en el que se realizan las actividades de emisión de documentos de viaje. Esto es lo básico de un entorno organizativo que apoye la seguridad. Asimismo, se analizan las prácticas de seguridad que han de aplicarse en todos los pasos del proceso de emisión, específicamente la realización regular de evaluaciones de riesgos y amenazas y auditorías.

1.2 Estructura organizativa

1.2.1 Mandato, responsabilidades y legislaciones

La AEDV debe ser un organismo (o dependencia) gubernamental independiente cuyo trabajo se centre exclusivamente en la emisión de pasaportes, documentos de viaje y otros documentos gubernamentales. Es importante que haya solamente una AEDV a cargo de todos los documentos de viaje que emita el Estado. Ésta debe ser responsable ante un nivel ejecutivo superior dentro del gobierno, el cual debe estar activamente involucrado en garantizar que el mandato y responsabilidades de la AEDV se cumpla debidamente.

Se requiere una debida ejecución de las leyes o reglamentos para establecer el mandato, responsabilidades y los límites de autoridad de la AEDV, sus altos funcionarios y el personal. Muchos gobiernos convierten los requisitos generales de las leyes en reglamentos específicos con fuerza de ley, que a la vez ofrecen una orientación más detallada tanto a los solicitantes como al personal de la autoridad emisora en cuanto a lo que puede permitirse, así como los casos en que puede haber un margen de flexibilidad. Las leyes y reglamentos establecen límites en cuanto a lo que el solicitante puede esperar recibir y lo que el personal puede legítimamente ofrecer bajo su propia autoridad. Las autoridades en el ámbito nacional, en el regional y en el local deben estar claramente definidas. A continuación se indican las áreas que han de regularse:

- la autoridad básica para emitir, revocar, retener, recuperar, cancelar y rechazar documentos de viaje;
- quién puede solicitar un documento de viaje;
- los requisitos que la persona solicitante deba cumplir para obtener el documento;
- los cargos por los servicios prestados por la autoridad emisora;
- los requisitos del sistema de registro;
- la protección de la privacidad;
- el período de validez del documento de viaje;
- información que se indicará en el documento de viaje
- instrucciones sobre su uso; y

- mecanismos para llevar a juicio casos de falsificación, uso indebido de documentos de viaje, falsa representación –uso del documento de otra persona– y mutilación del documento de viaje.

Debido a sus implicaciones de seguridad e interrelaciones con las funciones de las autoridades de control fronterizo e inmigración, la función de emisión de documentos de viaje debe estar incluida en el marco de seguridad nacional de todo país y reconocerse su impacto significativo en la seguridad nacional e internacional. Un resultado deseable de este reconocimiento es que las responsabilidades de seguridad de la autoridad emisora tengan el respaldo adecuado y que el gobierno la dote de los recursos adecuados. La AEDV y su personal deben participar en la planificación de la seguridad estatal y ser concientes del impacto global de sus responsabilidades en cuanto a la seguridad.

1.2.2 Estructura del proceso de emisión [centralizada o descentralizada]

Es necesario que cada gobierno llegue a su propia conclusión en cuanto a cuál es la estructura más apropiada a utilizar en su proceso de emisión –ya sea centralizada o descentralizada– a partir de consideraciones como la carga de trabajo, geografía, situación social, seguridad, nivel requerido de atención al cliente, entre otras.

Es altamente recomendable establecer un proceso de solicitud y emisión uniforme en todos los puntos donde se personalizarán los documentos de viaje, a fin de que el mismo sea estandarizado y transparente. El uso de formularios, procedimientos y configuraciones de software y hardware estandarizadas permite garantizar un nivel mínimo de calidad, cumplimiento, seguridad y control. Independientemente de la estructura por la que se opte, la supervisión y el control de todos los aspectos del proceso de emisión deben estar centralizados. Las revisiones y auditorías de rutina en todas las organizaciones e instalaciones involucradas en el proceso de emisión de pasaportes resultan de importancia crítica.

1.2.3 Uso de socios [públicos o privados]

En la actualidad muchos países recuren al uso de socios (bien sean gubernamentales o proveedores externos de prestigio) para llevar a cabo algunas de las funciones de emisión de documentos de viaje, como se menciona a continuación:

- producción de las libretas (o los materiales empleados en su producción);
- recepción de las solicitudes de documentos de viaje;
- impresión; y/o
- entrega.

Las decisiones sobre la titularidad de las personas solicitantes NUNCA deben subcontratarse.

Al momento de decidir si se recurre a socios en el sector público o el privado, varios factores han de tenerse en cuenta. En la siguiente tabla se presentan algunas consideraciones clave. Cada autoridad emisora debe llegar a sus propias conclusiones dependiendo de su situación particular.

Factores	Comentarios
Costos	Los costos de las funciones pueden variar dependiendo de si éstas se llevan a cabo internamente o si son subcontratadas.
Disponibilidad de recursos	Es posible que la autoridad emisora no disponga de los recursos internos (humanos, instalaciones, equipos) para llevar a cabo

	algunas de las funciones.
Accesibilidad del servicio	Dependiendo del territorio cubierto por la autoridad emisora, es posible que los servicios sean más accesibles para la población si son provistos por socios.
Control de los datos, materiales y procesos	La subcontratación puede resultar menos deseable desde la perspectiva del control, a menos que éste quede específicamente en manos de la autoridad emisora o que sea regulado en el marco de un acuerdo contractual.
Localización, nacionalidad de las compañías subcontratadas	Es necesario tomar en cuenta la legitimidad política y el contexto económico y de seguridad.
Transporte	La seguridad de los documentos de viaje/materiales mientras estos se encuentran en tránsito resulta de importancia crucial.
Implementación de medidas de seguridad en las instalaciones	Todas las instalaciones involucradas en el proceso de emisión deben contar con medidas adecuadas y salvaguardas de seguridad en el sitio.

Antes de sacar a concurso la elaboración de un nuevo documento de viaje, o bien los sistemas de producción y emisión u otros servicios se requiere una planeación cuidadosa de todos los aspectos del proyecto. En muchos casos, el éxito del proyecto en su conjunto depende del trabajo preliminar durante la fase de planificación.

Son muchos los beneficios que pueden obtenerse de una investigación previa a la realización del proyecto. En este sentido, es importante contactar a otros países que ya hayan implementado el sistema o servicio que se esté considerando, a fin de aprender a partir de sus experiencias. Otra práctica recomendable consiste en hacer una Solicitud de Información (SDI) para establecer los tipos de sistemas y tecnologías actualmente disponibles, y así determinar en forma óptima las necesidades de la autoridad emisora. Antes de suscribir un acuerdo con un socio potencial es recomendable realizar un Evaluación de Amenazas y Riesgos (EAR) de éste, con miras a garantizar su confiabilidad y seguridad. Una vez seleccionado el socio, se requiere realizar auditorías de rutina mientras dure la relación de trabajo.

Además, es necesario que existan contratos o memorandos de entendimiento en que se definan los derechos y responsabilidades de todos las partes involucradas, así como las penas en caso de que éstos no sean respetados. La AEDV debe realizar auditorías y evaluaciones regulares de sus socios para asegurarse de que estos apliquen las medidas y salvaguardas de seguridad apropiadas. Es recomendable realizar evaluaciones de riesgo en todas las instalaciones con regularidad.

1.3 Marco de seguridad

Un marco de seguridad incluye las estrategias, políticas, prácticas y controles que contribuyan a que el proceso de emisión de documentos de viaje sea más seguro. Así, por ejemplo, el fin de la presente Guía es en realidad evaluar el marco de seguridad de una AEDV, el cual promueva una mejor coordinación, estandarización y coherencia de los conceptos y prácticas de seguridad dentro de la organización y de la cadena de producción de los documentos. Algunos aspectos básicos deben estar resueltos para garantizar que exista un marco de seguridad, que sea efectivo, conocido y cumplido por el personal y por la gerencia. En esta sección se presentan estos aspectos básicos, a saber: un equipo de seguridad exclusivo, políticas y lineamientos documentados, apoyo financiero y de la gerencia, además de herramientas y actividades de capacitación y concienciación.

1.3.1 El equipo (o dependencia) dedicado a la seguridad

Es importante que la AEDV cuente con un equipo o sección que tenga a su cargo y esté dedicada a desarrollar, supervisar y garantizar el cumplimiento del marco de seguridad. Este grupo debe ser independiente de las operaciones y su personal debe contar con los recursos adecuados y con capacitación actualizada en materia de seguridad. Sus responsabilidades y actividades han de estar debidamente planificadas y ser informadas a la alta gerencia. A continuación se mencionan algunas, si bien la siguiente no es una lista exhaustiva:

- definir el marco de seguridad –estrategias, políticas, prácticas y controles;
- realizar evaluaciones documentadas de la seguridad, evaluaciones de riesgo y auditorías de todas las instalaciones y procesos, así como de las organizaciones que trabajen en forma asociada a todas las instalaciones y;
- garantizar la integridad del proceso de emisión del documentos de viaje;
- garantizar la seguridad y calidad de los documentos de viaje;
- facilitar conocimientos y experiencia en materia de fraudes;
- desarrollar programas de capacitación y concienciación en materia de seguridad;
- realizar investigaciones internas en caso de incidentes de seguridad; y
- consultar a los actores clave en el sector gubernamental, por ej., sobre controles fronterizos, inmigración, aplicación de la ley o seguridad.

1.3.1..1 Gerencia de controles internos

Todo cambio organizativo, actualización tecnológica, modificación al proceso de solicitud y método operativo puede tener consecuencias para la seguridad del proceso de emisión. Por lo tanto, resulta importante designar un funcionario(a) a la gerencia en el ámbito nacional (sede), así como en cada sitio de producción (oficina de campo), para asegurarse de que las consideraciones desde el punto de vista de la seguridad y de los controles internos sean tomadas en cuenta en las decisiones gerenciales.

Estos funcionarios(as) deben contar con independencia de la cadena operativa de mando y en última instancia rendir cuentas ante la dirección de la autoridad emisora. La razón para tal independencia de las operaciones es que la responsabilidad primordial de la oficina de operaciones es emitir los documentos de viaje, prevenir atrasos y cumplir con la carga de trabajo. Si bien esto no excluye involucrarse en los controles internos, no será su preocupación primordial.

- En el ámbito nacional, la persona designada para los controles internos debe ocupar un alto cargo gerencial y participar en la planificación y toma de decisiones de la organización.
- A nivel de las oficinas de campo, es importante designar a un alto funcionario(a) a cargo de los controles internos, de preferencia alguien que conozca el trabajo en detalle pero que no tenga autoridad en la solicitud o procesamiento de las solicitudes. Una administración exitosa del programa de controles internos del sitio deberá ser un elemento crítico en la evaluación de desempeño de ese funcionario(a).

1.3.1..2 Equipo antifraude

Es recomendable que la AEDV establezca un equipo cuya labor primordial sea la prevención de fraudes y que este equipo tenga al menos un representante en cada oficina emisora de pasaportes.

Las tareas del equipo antifraude han de ser las siguientes:

- coordinar las operaciones antifraude;
- ofrecer recursos de capacitación;
- ofrecer asesoría sobre trabajo en casos difíciles;

- trabajar en enlace con otras entidades gubernamentales que produzcan documentos madre y documentación de apoyo; y
- trabajar en enlace con otros organismos gubernamentales encargados de enjuiciar casos de fraude una vez detectados.

1.3.2 Políticas de seguridad documentadas

Las políticas, prácticas, lineamientos y estrategias de seguridad que desarrolle la sección de seguridad y que conformen el marco de seguridad organizativo deben quedar consignadas por escrito y documentadas. Deben incluir los procedimientos y controles internos que hayan sido desarrollados para minimizar las vulnerabilidades en todos los aspectos de las operaciones de la AEDV, e implementarse plena y sistemáticamente en todas las instalaciones y organizaciones asociadas para la emisión de documentos de viaje.

En las políticas, prácticas y lineamientos deben definirse las responsabilidades de todas las personas con respecto a la seguridad de los activos y hacerse énfasis en el apoyo de la gerencia al programa de seguridad. Tales políticas, prácticas y procedimientos deben comunicarse a todo el personal, de forma que sean bien conocidos. Debe ser fácil remitirse a ellas y ser además de fácil comprensión. Se requiere un monitoreo estrecho y estricto en cuanto al cumplimiento con las políticas.

La información en cada uno de los capítulos subsiguientes puede servir de base para las políticas y procedimientos sobre seguridad.

1.3.3 Apoyo gerencial y financiero

1.3.3..1 Apoyo gerencial

Ningún programa de seguridad funcionará de manera adecuada si no tiene el apoyo de la alta gerencia. Es necesario que quienes tengan a su cargo la toma de decisiones estén dispuestos a comprometer tiempo y recursos para el desarrollo, implementación y mantenimiento de un sistema eficaz de controles. Es posible que poner en marcha dicho sistema requiera reorganizar el flujo de trabajo, introducir cambios en la administración del personal, revisar otros aspectos de las operaciones y organizar sesiones de capacitación y concienciación, entre otros. Asimismo, se considera vital que la alta gerencia dé el ejemplo a las políticas de seguridad y otras medidas que defina el equipo de seguridad, cumpliendo con éstas y sin pedir favores especiales.

1.3.3..2 Apoyo financiero

Es necesario contar con recursos exclusivos, tanto monetarios como humanos, para proteger la integridad del proceso de emisión, lo cual puede plantear dificultades a una autoridad emisora que funcione con un presupuesto reducido. Sin embargo, es importante percatarse de que el no prever los recursos adecuados para mantener un programa eficaz de controles internos puede traducirse en última instancia en costos significativos, como se menciona a continuación:

- La posibilidad de incurrir en una vergüenza para el país en caso de que sus documentos de viaje sean utilizados para cometer actos terroristas.
- Las dificultades que enfrentarán los ciudadanos del país en sus viajes internacionales si sus documentos de viaje son inspeccionados más rigurosamente por las autoridades fronterizas y relacionadas con las visas.
- Los costos sustanciales que supone la realización de investigaciones, enjuiciamientos y encarcelaciones como resultado de actividades criminales facilitadas mediante el fraude de documentos de viaje.

Un documento de calidad expedido con un alto nivel de integridad representará un gran avance para prevenir este tipo de abusos. El costo de la prevención a través de un proceso de emisión altamente seguro y controlado suele ser mucho menor que el costo de hacer frente a los resultados de un proceso inseguro.

Es recomendable que al establecer los cargos por los servicios de emisión de documentos de viaje se tome en cuenta el costo real de ofrecer tales servicios, incluyendo el costo necesario de la seguridad en todas sus formas, a saber el personal, capacitación, software, hardware, materiales, seguridad física, papelería, folletos, materiales de comunicación y mantenimiento de equipos.

1.3.4 Establecimiento de una cultura de seguridad [Capacitación y concienciación]

Es importante que la organización promueva la seguridad entre su personal con miras a desarrollar una cultura organizativa que propicie la implementación y el respeto por las políticas y prácticas de seguridad. Los siguientes son algunos ejemplos de técnicas que la gerencia podría utilizar para desarrollar una cultura de seguridad y hacer conciencia sobre el tema entre su personal:

- ofrecer regularmente capacitaciones, sesiones informativas y de refrescamiento;
- recordar con frecuencia al personal sus responsabilidades en cuanto a la seguridad;
- desarrollar un código de conducta y valores y lineamientos éticos (Capítulo 9);
- realizar campañas de comunicación y publicidad sobre políticas de seguridad;
- publicar los resultados de las evaluaciones y auditorías sobre seguridad;
- organizar reuniones mensuales sobre el tema de la seguridad;
- producir y distribuir boletines de inteligencia;
- utilizar intranets;
- recurrir al refuerzo positivo y recompensar o premiar las buenas prácticas de seguridad; y
- aplicar sanciones y medidas disciplinarias por incumplimiento o negligencia.

Resulta importante ofrecer capacitación de manera regular, a fin de mantener un nivel adecuado de conciencia sobre el tema entre los empleados. Dependiendo del cargo que ocupen, éstos también han de recibir capacitación sobre medidas específicas de seguridad que apliquen a sus funciones, por ejemplo documentación de abusos, alteración de documentos y otros aspectos del fraude. Asimismo, la capacitación debe abarcar el manejo de información personal y la privacidad, además de la seguridad informática. Debe verificarse que el personal comprenda los conceptos y prácticas sobre seguridad y las razones en que se sustentan. Si el personal carece de información o no comprende la necesidad de todos los pasos de seguridad que abarcará el proceso, es posible que intente buscar atajos en los procedimientos para facilitarse el trabajo. Asimismo, debe alentársele a sugerir posibles mejoras a las prácticas de seguridad.

1.3.5 Estándares de desempeño

Las descripciones de funciones de todos los miembros del personal deben incluir un estándar de desempeño que imponga como requisito conocer y cumplir con los controles internos. La evaluación de todo el personal debe incluir el desempeño desde el punto de vista de los controles internos y las medidas disciplinarias en caso de negligencia en cuanto a las obligaciones o responsabilidades de seguridad.

1.3.6 Anticipación y planeamiento de la carga de trabajo

La AEDV debe anticipar aumentos repentinos en el número de solicitudes de documentos de viaje y planificar en consecuencia para disponer de los recursos financieros y humanos. Es posible

hacer proyecciones de la carga de trabajo mediante el uso de datos históricos y tomando en cuenta los elementos conocidos que puedan incidir en la demanda de documentos, por ej., los períodos tradicionales de mayor frecuencia de viajes como feriados escolares, acontecimientos de importancia, la economía, y los requisitos de ingreso de otros países, entre otros.

La autoridad emisora ha de hacer todos los esfuerzos necesarios para establecer un nivel adecuado de personal para satisfacer la demanda proyectada de trabajo. Además, es importante elaborar planes de contingencia para enfrentar situaciones de exceso de enfermedades, por ej. en casos de pandemias. La capacidad no debe incrementarse con demasiada rapidez a fin de no quedar con una cantidad importante de empleados recién capacitados. La AEDV debe mantener un grupo de funcionarios(as) previamente autorizados(as) o cuyo historial haya sido previamente investigado a los cuales pueda convocarse en situaciones de exceso de trabajo o de escasez de personal.

Los controles internos tienen más importancia que nunca cuando aumenta la carga de trabajo, ya que el personal a cargo de atención al cliente y de enfrentar los atrasos en las solicitudes puede verse tentado a recurrir a atajos o pasar por alto procedimientos de control interno que sienta que enlentecen el flujo del trabajo. Al encontrarse sometidos a la presión de una carga de trabajo excesiva, la gerencia deben resistirse al impulso de dejar de lado los controles internos.

1.4 Prácticas generales de seguridad

Algunas prácticas de seguridad aplican a todo el proceso de emisión de documentos de viaje: las evaluaciones de amenazas y riesgos y auditorías deben aplicarse habitualmente a todos los pasos, funciones, activos e instalaciones involucradas en el proceso de emisión. Estas prácticas se explican en la presente sección, en lugar de reiterar su importancia en cada uno de los capítulos subsiguientes.

1.4.1 Evaluaciones de amenazas y riesgos

Es recomendable que la AEDV tome las acciones apropiadas para gestionar las vulnerabilidades, amenazas y riesgos a la seguridad de su sistema de emisión. La gestión de riesgos es el proceso de planificación, organización, conducción y control de los recursos para garantizar que el riesgo de funcionamiento de un sistema se mantenga dentro de los límites aceptables a un costo óptimo. Debido a que resulta prohibitivo –y probablemente imposible– salvaguardar la información y los activos contra todas las amenazas el 100% de las veces, las prácticas modernas de seguridad se basan en una evaluación de las amenazas y vulnerabilidades con respecto al grado de riesgo que cada una presente, para seleccionar luego las salvaguardas que resulten más efectivas desde el punto de vista de los costos.

Es importante aplicar evaluaciones de amenazas y riesgos de manera regular, ya que estas ayudan a determinar las amenazas actuales al sistema de emisión y los activos y áreas que se encuentran en mayor riesgo dentro del proceso. A partir de las evaluaciones se recomiendan medidas para prevenir y mitigar los riesgos, las cuales disminuirán los riesgos para dejarlos en niveles aceptables. Las evaluaciones de amenazas y riesgos involucran los siguientes pasos:

- establecer los alcances de la evaluación;
- determinar las amenazas y valorar las probabilidades e impacto de que se materialicen;
- evaluar los riesgos con base en la suficiencia de las salvaguardas existentes y las vulnerabilidades; e
- implementar cualquier salvaguarda complementaria para disminuir el riesgo a un nivel aceptable.

Es posible que surjan diferencias significativas de un país a otro, e incluso de una región a otra, en términos de las amenazas y las razones subyacentes a los intentos de fraude. Es por ello que las evaluaciones de amenazas y riesgos deben realizarse en todas las instalaciones donde se emitan documentos de viaje y en todas las etapas del proceso de emisión, en colaboración con las autoridades encargadas de la aplicación de leyes. Resulta importante anotar que las amenazas también provienen de fuentes internas y que la AEDV debe asegurarse de que los procesos y sistemas de apoyo al personal y de gestión de los riesgos por mala conducta y corrupción queden cubiertos.

Las personas que saben mejor cuáles son las vulnerabilidades son las que trabajan con los sistemas y procedimientos. Resulta aconsejable preguntar al personal periódicamente cuáles consideran que son las vulnerabilidades y lo que debe hacerse para minimizarlas. Es importante alentársele a comunicar sus inquietudes y reconocerse adecuadamente a quienes identifiquen los problemas. Es una buena práctica mantener las estadísticas sobre amenazas o riesgos que se materializan, a fin de dirigir recursos hacia la introducción de cambios en el proceso para prevenir incidentes o ataques de algún tipo en particular en el futuro.

La organización debe monitorear de forma continua para identificar cualquier cambio en el ambiente en términos de las amenazas, y hacer los ajustes del caso para mantener un nivel aceptable de riesgo y un balance entre las necesidades operativas y la seguridad. Para mayor información remítase al Estándar Australiano/Neozelandés ASNZS 4360/2004, que en la actualidad está transformándose en la norma ISO 31000 (http://www.iso.org/iso/catalogue_detail.htm?scnumber=43170).

Al analizar los riesgos y vulnerabilidades la AEDV debe desarrollar también un Plan de Continuidad del Negocio que garantice que, de materializarse un ataque o amenaza de importancia, las operaciones de pasaportes puedan continuar. Esto es de particular importancia para los Estados con un sitio primario dedicado a la emisión. Para mayor información sobre la planificación de la continuidad del negocio, remítase al material de orientación sobre buenas prácticas y normas del Business Continuity Institute (http://www.thebci.org/).

1.4.2 Auditorías

Uno de los medios más eficaces para garantizar que el personal conozca y cumpla con las reglas establecidas para prevenir el fraude es contar con un sistema de auditorías formalmente requeridas. Es importante que se realicen periódicamente auditorías internas en forma *ad hoc,* y que éstas estén a cargo de organizaciones externas independientes.

1.4.2..1 Auditorías internas

Es necesario realizar auditorías formales y en forma *ad hoc* con regularidad en todas las instalaciones y para todos los pasos del proceso de emisión, a fin de garantizar el cumplimiento con las políticas y reglas.

Las auditorías internas formales y las evaluaciones de cumplimiento deben ser realizadas por altos funcionarios que revisen la gestión de las operaciones y la suficiencia del programa de controles internos. El equipo de inspección debe producir un informe formal de los hallazgos, cuyas recomendaciones de mejoras sean enviadas al alto funcionario(a) ejecutivo(a) ante el cual la AEDV sea responsable. Es importante que exista un proceso de cumplimiento que garantice la implementación de los cambios necesarios.

Estas auditorías formales deben complementarse con una evaluación activa del trabajo en marcha por parte de la gerencia, el cual debe ser revisado en forma aleatoria para asegurarse de que las

reglas establecidas se cumplan. Esto aplica en todo momento, pero en particular en períodos de mucho trabajo cuando el personal y la gerencia quizás se vean tentados a buscar atajos y dejar de lado algunos controles internos. Para las revisiones internas debe requerirse que los altos funcionarios(as) de todas las instalaciones analicen un porcentaje de las solicitudes de mayor urgencia, otras solicitudes que se encuentren en trámite, además de las solicitudes de documentos de viaje ya emitidos, con el fin de verificar que se hayan seguido los procedimientos adecuados; que las pruebas adjuntas o registradas sean adecuadas; que las anotaciones se encuentren completas; que las acciones dirigidas puedan justificarse y que se hayan cancelado los cargos correspondientes.

1.4.2..2 Auditorías externas

Una entidad externa e independiente como la dependencia gubernamental dedicada a las auditorías, debe llevar a cabo también y en forma periódica auditorías de desempeño para evaluar las prácticas de seguridad de la AEDV. Estas entidades independientes por lo general emiten sus recomendaciones y son responsables de monitorear su implementación. Las auditorías externas han demostrado ser sumamente eficaces, ya que no desconocen las prácticas usuales dentro de la organización, no se ven influenciadas por los requisitos de operación y toman en cuenta las amenazas de seguridad y otras medidas efectivas instituidas en otras organizaciones.

2 Los procesos de solicitud

2.1 Resumen

Para obtener un documento de viaje, la persona solicitante debe seguir un proceso determinado de solicitud, que incluye llenar formularios, presentar evidencia documental y fotografías y en algunos casos indicadores biométricos secundarios. La información y documentación que aporte permitirá al personal de la AEDV corroborar la titularidad del solicitante al documento de viaje.

La información que el solicitante presente debe estar protegida durante todo el proceso de emisión y una vez expedido el documento de viaje. Así, la privacidad y la protección de los datos son elementos esenciales para garantizar la seguridad del proceso de emisión del documento de viaje.

2.2 Procesos de solicitud y requisitos

2.2.1 Uniformidad de los procesos

Independientemente de la estructura organizativa de la AEDV, es decir, de si es centralizada o descentralizada, e independientemente de la información y documentación que deba presentar el solicitante, todas las solicitudes deben pasar por un proceso uniforme en toda la AEDV. Todos los formularios de solicitud deben ser estandarizados y los requisitos para el solicitante deben ser los mismos en todo el país. Además, las políticas y procedimientos relativos a cómo y dónde hacer la solicitud deben ser de fácil acceso para el público y todo el proceso de solicitud debe ser transparente. Las políticas y procedimientos sobre el trámite de las solicitudes deben estar documentadas y encontrarse fácilmente disponibles para el personal de la AEDV.

2.2.2 Factores que influyen en el proceso

Los procesos y requerimientos de solicitud presentan sin duda variantes de un país a otro, y será cuestión para que cada Estado decida, por ej. si las solicitudes deberán hacerse en persona, por correo, en línea, etc. Además de la seguridad, varios factores han de tomarse en cuenta al momento de establecer los procesos de solicitud, entre ellos los siguientes:

Factores	**Comentarios**
Primera solicitud o renovación	La primera solicitud debe pasar por un escrutinio más minucioso. Es posible que el solicitante que ya haya tenido un pasaporte no deba presentarse en persona o presentar los mismos documentos –esto es, los documentos madre– que quien solicita por primera vez, pero por lo general debe adjuntar a su solicitud el pasaporte (o documento de viaje) anterior. Sin embargo, si este pasaporte anterior corresponde a una identidad falsa, la renovación automática sin una verificación adicional perpetuará el problema.
Accesibilidad del servicio	Dependiendo del territorio que cubran las oficinas de la AEDV, la opción de enviar por correo la solicitud o de presentarla en las oficinas de algún socio puede derivar en una mayor accesibilidad del servicio para la población.
Confirmación de la identidad	Requerir que el solicitante se apersone ante algún funcionario gubernamental mejora las posibilidades de confirmar la identidad de una amplia gama de solicitantes. Primero permite confirmar que la persona esté viva todavía; pueden compararse las fotografías con respecto a la persona propiamente, pueden hacerse preguntas directamente al solicitante, además de que puede observarse su comportamiento.
Historial de documentos de viaje perdidos o robados	Si el solicitante tiene un historial de documentos de viaje perdidos o robados, podría requerirse que presente la solicitud en persona. (Capítulo 10).

Recolección de datos biométricos secundarios	La captura de datos biométricos requiere que el solicitante se apersone al menos en una ocasión.
Seguridad del sistema de correos	Si el servicio de correo, sea público o privado, no es fiable, el proceso de solicitud debe hacerse personalmente.
Tecnología	Gracias al desarrollo de nuevas tecnologías es posible que algunas partes del proceso de solicitud se hagan en línea o a distancia, por ejemplo la impresión de formularios, transmisión de datos, transmisión de fotografías digitales, entrevistas telefónicas o por teleconferencia.
Servicio urgente o expreso	Las solicitudes que requieran tramitarse con urgencia pueden requerir que el solicitante se apersone en las oficinas de la AEDV.

Muchos países requieren que el solicitante se presente personalmente para hacer toda solicitud de un documento de viaje, incluyendo las renovaciones, aunque el que esto sea necesario es algo que depende de de las salvaguardas en todo el proceso de solicitud y emisión. Algunos países requieren que solamente quienes solicitan el documento por primera vez, las personas menores de edad y las que no puedan presentar su documento de viaje anterior más reciente se apersonen para solicitar uno nuevo. Los adultos cuya identidad ya haya sido autenticada pueden ser debidamente identificados asociando/matching su antiguo pasaporte a una fotografía nueva (y a las características biométricas) y puede no ser necesario que se presenten personalmente. Desde el punto de vista de la seguridad, requerir la presencia personal contribuye a reforzar la seguridad del proceso. Sin embargo, otros recursos para verificar la identidad pueden atenuar de forma efectiva los riesgos de seguridad hasta un nivel aceptable.

Si es que forman parte del proceso, las funcionarias y funcionarios encargados de aceptar las solicitudes de documentos de viaje deben estar capacitados y contar con una orientación escrita detallada sobre cómo identificar a quienes solicitan un pasaporte, cómo anotar los documentos de identificación en la solicitud del pasaporte y qué hacer en caso de no quedar satisfechos con los documentos de identidad presentados. El personal debe recibir capacitación en otras destrezas que contribuyan a evidenciar otras señales o indicadores de solicitud fraudulenta, por ejemplo: destrezas para la realización de entrevistas, de reconocimiento de lenguaje corporal, verificación de documentos madre, además de la capacidad para reconocer incoherencias en la presentación y documentos del el(la) solicitante en su conjunto.

En muchos países, las solicitudes de documentos de viaje son aceptadas por socios fuera de la autoridad emisora, los cuales fungen sencillamente como casillas de correo y llevan a cabo verificaciones muy básicas a fin de garantizar que la solicitud se llene en su totalidad, que se cancelen los cargos correspondientes y que se adjunte la prueba documental requerida. Si esta función no está en manos de la autoridad emisora, es recomendable que se le asigne a instituciones gubernamentales que estén familiarizadas con los procesos y trámites legales, por ejemplo tribunales, agencias de policía, oficinas de correo u otras dependencias gubernamentales acostumbradas a trabajar con el público como oficinas de impuestos o bibliotecas públicas. Los socios de la autoridad emisora deben contar con la capacitación para verificar los documentos madre, además de tener la capacitación básica en materia de detección de fraude y sus características. En situaciones de duda, los casos han de referirse a la AEDV.

2.3 Fotografías

La emisión de documentos de viaje requiere que la persona solicitante presente fotografías, las cuales pueden ser tomadas por un fotógrafo comercial, un socio de confianza o un funcionario(a) nacional. Solamente las fotografías que cumplan con las especificaciones indicadas en el Documento 9303 de la OACI deben ser aceptables. Respetar estas especificaciones facilita la labor de verificación de la identidad del titular por parte de la AEDV y en la frontera, y también permite el uso de tecnología de reconocimiento facial. Para garantizar el cumplimiento con las especificaciones de la OACI estas deben ponerse a disposición de los fotógrafos comerciales y del público en general.

Los siguientes son ejemplos de especificaciones de la fotografía publicadas:

EE.UU.: http://travel.state.gov/passport/guide/guide_2081.html
Nueva Zelanda: http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Passports-Photographic-Requirements
Canadá: http://www.pptc.gc.ca/cdn/photos.aspx?lang=eng

Con el desarrollo de nuevas tecnologías es posible que algunos países comiencen a aceptar solicitudes en línea y fotografías digitalizadas o electrónicas. Estas fotografías deben ser tomadas por un socio o funcionario nacional fiable y ser transmitidas de forma segura desde el punto de la captura hasta la autoridad emisora sin que haya oportunidad de alteración. Para minimizar el riesgo de alteración en las diversas etapas del proceso de solicitud, es importante requerir una fotografía impresa además de la digitalizada.

2.4 Características biométricas secundarias

Muchos países requieren o requerirán la recolección de huellas digitales como parte del proceso de emisión de documentos de viaje. Las características biométricas, entre ellas las huellas digitales o el iris, pueden recolectarse por distintas vías: la autoridad emisora, otros funcionarios gubernamentales, otros agentes fiables designados por el gobierno u otro medio seguro y de confianza. El manejo de los registros biométricos y de los métodos de recolección de información biomética son cuestiones que cada país debe decidir. Sea cual sea el método seleccionado, es imperativo que respete la privacidad y que pueda demostrarse su seguridad y confiabilidad. El país debe decidir si requerirá la recolección de características biométricas solamente para la primera solicitud o para todas las solicitudes, incluyendo las renovaciones.

2.5 Tratamiento y protección de la información personal

Para cumplir de manera eficaz con su mandato, la AEDV procesa y almacena inmensas cantidades de información personal de solicitantes. Esta información debe ser rigurosamente salvaguardada ya que los criminales buscarán acceder a ella y utilizarla con propósitos ilegales como robo de identidad, obtención de beneficios financieros u otros tipos de fraude de identidad, los cuales son cada vez más frecuentes y son en la actualidad un tema de gran preocupación para la sociedad.

Una vez completado, el formulario de solicitud contiene alguna información personal que suele estar protegida por leyes de privacidad y en ningún caso debe ser revelada a terceros que no tengan la autoridad apropiada. El personal de la AEDV ha de contar con la capacitación y documentación sobre las distintas leyes sobre la información y la privacidad que se encuentren en vigor en el país y la gerencia debe velar por su cumplimiento. Además del aspecto de la privacidad, la comunicación no autorizada de esta información a terceros ajenos a la AEDV puede derivar en fraudes de identidad.

Toda solicitud debe ser registrada al momento de ser recibida y actualizarse su estado a lo largo de la cadena de procesamiento. Toda persona involucrada en las distintas etapas del proceso de manejo de solicitudes debe quedar identificada en la bitácora de estado de los trámites y dar el caso por concluido cuando la solicitud pase a la siguiente etapa. Ello permite una supervisión de alto nivel para determinar quién ha tenido acceso al expediente, además de controlar el estado de la solicitud en todo momento, algo que resulta de particular importancia para los expedientes de "personas de mucha importancia" (VIP). Todos los formularios y la documentación presentados deben archivarse bajo llave o en el menor de los casos, mantenerse en un lugar seguro en todo

momento, incluyendo cuando estén siendo tramitados. Se considera esencial que el trabajo pendiente quede bajo llave fuera de horas normales de trabajo, de forma que el personal de vigilancia del edificio, otros empleados o el personal de limpieza no tengan acceso a la información privada de los solicitantes. El personal debe estar en posibilidad de dar cuenta de todo documento de solicitud y sus copias en todo momento. Tal documentación no debe salir nunca de las instalaciones de la AEDV.

La información de las solicitudes que se lleve en registros informáticos debe estar protegida mediante las normas adecuadas de seguridad informática (Capítulo 8) y nunca debe ser salvaguardada o compartirse en una red no protegida, mediante conexiones de Internet o en equipos o aparatos portátiles que puedan sacarse de las instalaciones de la AEDV.

Han de utilizarse bitácoras electrónicas para controlar y rastrear el acceso al archivo. Para lograr una mayor seguridad, cabe la posibilidad de utilizar características tales como los controles biométricos o las tarjetas de identidad personalizadas para acceder a un sistema o base de datos.

La información personal de las solicitudes que se mantenga en registros computarizados debe protegerse mediante estándares adecuados de seguridad informática (Capítulo 8) y nunca debe salvaguardarse o compartirse a través de una red no protegida, conexiones de Internet o aparatos portátiles que puedan sacarse de las instalaciones de la autoridad emisora. Es importante llevar registros de acceso electrónico para controlar y rastrear el acceso a los archivos. Si se requieren medidas adicionales de seguridad, cabe la posibilidad de introducir controles biométricos o carnets de identidad personalizados para acceder a un sistema o base de datos.

Una vez concluido el trámite de la solicitud, todos los materiales que contengan información personal del solicitante (incluyendo los documentos de solicitud, registros computarizados, imágenes y datos del documento madre, imágenes de la página de datos, así como el contenido de los chips en el caso de los PLM-e) deben quedar cuidadosamente almacenados en forma segura para que facilitar su referencia futura, en archivadores bajo llave o en habitaciones protegidas y en bases de datos con protección de seguridad. El acceso a los registros archivados debe estar sujeto a estrictos controles en cuanto a los permisos y registros y rastreos del acceso. Cuando la información no se requiera más, debe ser destruida mediante máquinas trituradoras o equipos para la destrucción de documentos, en cumplimiento con todas las leyes gubernamentales y políticas de la AEDV sobre mantenimiento de registros.

2.5.1 Sistemas automatizados

El uso de tecnologías para automatizar los procesos de emisión de pasaportes puede incrementar la seguridad y la precisión de dichos procesos. El registro de datos, escaneo, impresión, almacenamiento, envío por correo y elaboración de informes de la gerencia son todos procesos que pueden automatizarse hasta cierto punto. Esto limita la manipulación manual de los datos, y podría aumentar la rapidez para detectar información fraudulenta o cuestionable. Los sistemas automatizados pueden incluir una función de chequeo aleatorio de seguridad que requiera que la solicitud sea vista por un supervisor(a) antes de que su emisión sea autorizada.

3 Procesos de verificación de la titularidad

3.1 Resumen

En la mayoría de los países hay tres elementos necesarios que un gobierno debe establecer antes de emitir un documento de viaje: evidencia de la identidad de la persona solicitante, esto es, si se trata de una identidad verdadera y si ésta es de hecho quien afirma ser; prueba de su ciudadanía; y verificar si dicha persona está sujeta a restricciones de viaje, por ej. debido a su hoja de antecedentes penales, historial de documentos de viaje perdidos y robados, falta de pago de su pensión alimenticia, entre otros. Son varias las herramientas y técnicas que se utilizan para verificar la titularidad de los documentos de viaje. Los usos de tales herramientas y técnicas varían de un país a otro. No hay un único método para establecer firmemente la identidad, aunque sí hay varias formas de corroborarla con un grado razonable de certeza. Para verificar la identidad y la ciudadanía, normalmente la AEDV requiere presentar pruebas documentales. Otras estrategias incluyen la recolección de características biométricas, verificación de la huella social, uso de un garante, además de referencias, entrevistas, etc.

Las restricciones de viaje aplicables que no permiten ni restringen los viajes a determinados individuos suelen ser verificadas examinando las solicitudes contra bases de datos con listas de observación que contengan información proveniente de la AEDV y de distintas organizaciones asociadas.

Es importante que la AEDV cuente con políticas y procedimientos documentados para verificar la identidad y titularidad de la persona solicitante a un pasaporte. Estas políticas y procedimientos deben encontrarse a disposición del personal de la AEDV y su cumplimiento debe vigilarse.

Todas las decisiones sobre la titularidad del solicitante deben ser tomadas por personal de la AEDV debidamente capacitado.

3.2 Tratamiento de primeras solicitudes versus *renovaciones*

En algunos países el proceso de solicitud y verificación de la titularidad es distinto para quienes solicitan por primera vez y quienes buscan renovar su documento de viaje. La información y documentación requerida puede ser diferente, así como las verificaciones a que se sometan. Los países que utilizan procesos diferentes deben contar con una política en la que se definan claramente las condiciones bajo las que puede presentarse una solicitud de renovación, por ejemplo el vencimiento del pasaporte anterior menos de un año antes de que se presente la solicitud.

(Ejemplo: Trámite simplificado de renovación en:
www.passportcanada.gc.ca/cdn/ren.aspx?lang=eng)

Las solicitudes presentadas por primera vez deben someterse a un examen más minucioso. Los países que permiten que las solicitudes de renovación sean presentadas mucho tiempo (más de dos años) después de que venza el documento anterior deben examinar estas solicitudes más de cerca. En el caso de todas las renovaciones, los datos presentados en la solicitud deben compararse con los del documento de viaje anteriormente expedido a favor de ese individuo. Además, en el caso de las renovaciones, si el documento anterior fue expedido a favor de una identidad falsa la renovación automática perpetúa el problema, de tal manera que es importante realizar verificaciones adicionales, por ejemplo en las bases de datos y de referencias para asegurarse de que esto no ocurra.

3.3 Solicitudes para niños

Las solicitudes de documentos de viaje de niños o niñas deben ser presentadas por al menos uno de los padres u otra persona con una responsabilidad parental sobre el niño. Debe aportarse prueba de nacimiento y evidencias de la huella social, junto con una posible comparación con otros documentos de apoyo si el niño o niña tiene edad suficiente para calificar para ello. El(los) padre(s) u otra persona con responsabilidad parental que presente la solicitud deben establecer su propia identidad. Los niños no han de incluirse en el pasaporte de las personas adultas, sino que cada cual debe tener su propio pasaporte, incluyendo los recién nacidos.

3.4 Evidencia documental

Confirmar la identidad de la persona solicitante resulta fundamental en términos de la integridad del documento de viaje. Para identificarse, ésta utiliza un documento o combinación de documentos. Además de la identidad, la evidencia documental debe permitir comprobar su ciudadanía.

Resulta crucial establecer que la identidad que el solicitante afirma tener es una identidad verdadera, que corresponde a una persona viva y que de hecho no corresponde a una persona fallecida o del todo ficticia. La identidad de una persona fallecida puede ser mal utilizada por impostores para solicitar un documento de viaje fraudulento. Es importante tomar medidas para garantizar que la identidad afirmada corresponda a la persona viva que afirma tenerla.

La evidencia documental para verificar la titularidad del solicitante mediante los requisitos de identidad y ciudadanía puede combinarse en un único carnet o documento:

- certificado de nacimiento
- certificado de matrimonio
- certificado de ciudadanía
- certificado de naturalización
- pasaporte u otro documento de viaje vigente
- cédula nacional de identidad o similar

Estos documentos reciben el nombre de documentos madre. Los documentos madre son aquellos que contienen información de identificación y nacionalidad y son emitidos por una fuente gubernamental confiable u otra fuente oficial. Ya han sido objeto de un nivel de verificación lo suficientemente alto por parte de personal de confianza antes de ser expedidos. Deben contener características básicas de seguridad, entre ellas un número único y quizás una fotografía autorizada o con indicadores biométricos. Sin estas características, la AEDV estará vulnerable al robo del cédula de identidad o similar, tanto de personas vivas como fallecidas. Empero, este tipo de documentación puede contribuir a la evidencia general de identidad cuando se presenta junto con otras formas de documentación. En estos casos, se pedirá a la persona solicitante que aporte documentación de apoyo para confirmar, por ejemplo, que se trata de una persona viva, residente en una dirección específica. A continuación se presentan algunos ejemplos de documentación de apoyo:

- cédula de identidad o similar
- registro de electores
- registro censal
- expediente médico
- expediente del seguro social y tributario

- registro de empleo
- licencia de conducir
- registro de propiedad de vehículos automotores
- registros financieros

Es necesario contar con procedimientos especiales para los solicitantes que tengan los documentos madre y la documentación de apoyo en forma limitada, por ejemplo un certificado de nacimiento más antiguo, que no tengan licencia de conducir, etc. En estos casos resulta de particular importancia contar con otros recursos y técnicas para validar la identidad.

La persona solicitante debe presentar su evidencia documental junto con la solicitud. Los documentos originales deben ser entregados, escaneados por la AEDV y almacenarse en una base de datos centralizada de forma que puedan ser verificados en una auditoría no anunciada en cualquier momento durante el proceso de corroboración de la titularidad y emisión del documento o al momento de su renovación. La evidencia documental es posteriormente devuelta a la persona solicitante junto con el documento de viaje. En el caso de las renovaciones, algunos países no piden a la persona solicitante que presente nuevamente la documentación, salvo por el pasaporte anterior –u otro documento de viaje– y la verificación se hace utilizando la información y documentos escaneados que ya se encuentran en la base de datos de la AEDV.

En muchos países, la evidencia documental utilizada (documentos madre o documentación de apoyo) se emite, almacena y recupera por separado. A menudo es emitida por autoridades locales o regionales con poco o ningún nivel de estandarización o control. Tal documentación a menudo contiene pocas características de seguridad. Quienes buscan obtener documentos de viaje bajo una falsa identidad pueden valerse de muchos métodos para obtener documentos madre: pueden recurrir al robo de identidad, aprovecharse de procedimientos laxos de solicitud, crear una falsa identidad a partir de personas fallecidas o de copias de documentos aceptables, completarlas y presentarlas como si fuesen documentos auténticos. Es importante prestar especial atención a verificar la autenticidad de los documentos presentados por quien solicita el documento de viaje.

Es recomendable que la identidad del reclamante sea verificada contra registros de fallecimientos electrónicos o impresos.

La Norma de autenticación del Gobierno de Nueva Zelanda es una referencia útil en este sentido: http://www.e.govt.nz/services/authentication/standards/index.html

3.4.1 Verificación de la autenticidad del documento

3.4.1..1 Verificación de las características de seguridad

El personal encargado de aceptar las solicitudes y decidir sobre la titularidad debe estar capacitado tanto en cuanto a las características y elementos de seguridad de los documentos auténticos como en cuanto a la identificación de documentos falsos. Es probable que los documentos madre, que a menudo son certificados de nacimiento, se presenten en muchas formas distintas dentro de un mismo país, lo cual complica el proceso de identificación para la emisión de documentos de viaje.

Lo ideal es que el personal de la autoridad emisora que esté capacitado y que cuente con las debidas autorizaciones de seguridad lleve a cabo la verificación, pero cuanto más grande sea el país y mayor sea la cantidad de localidades en que se reciban solicitudes, mayores serán las probabilidades de que la autoridad emisora se asocie con otras organizaciones que tengan una buena representación local. Los socios de la AEDV deben también estar capacitados para verificar los documentos madre. Los casos dudosos deben remitirse al personal de la AEDV para obtener su asesoría y orientación. Quizás sea necesario que las solicitudes que vengan acompañadas de evidencias de ciudadanía/identidad menos confiables sean rutinariamente referidas a un

supervisor y a la unidad de fraude para su revisión y para el examen del documento. Todos los examinadores deben conocer los elementos mínimos de seguridad recomendados.

3.4.1..2 Bases de datos de documentos

Existen bases de datos tanto gubernamentales como comerciales que contienen ejemplos de diversos documentos madre o documentos de viaje auténticos. Éstas pueden utilizarse para verificar la autenticidad de los documentos presentados por la persona solicitante. Ejemplos de bases de datos gubernamentales que se encuentran a disposición de cualquier autoridad emisora el mundo con el pago de una tarifa son la DISCS en el caso de los documentos madre y la EDISON en el caso de los pasaportes.

3.4.1..3Referencia a los registros oficiales

Siempre que las posibilidades lo permitan, ha de procurarse el acceso electrónico directo a registros gubernamentales apropiados y seguros, en lugar de a los documentos impresos.

Una revisión automatizada de cada solicitud puede ser una ayuda significativa para detectar y prevenir el fraude. Ejemplos de herramientas automatizadas son la verificación en línea con los organismos primarios donde se encuentran los documentos madre, como es el caso de los registros de nacimientos y ciudadanía, las bases de datos de nacimientos y de fallecimientos, los registros de licencias comerciales, padrones electorales, registros de propiedad y/o registros de propiedad de vehículos automotores. Esto ayudará a confirmar la legitimidad de los documentos y a identificar de manera rápida los fraudulentos.

Cuando no existan los vínculos electrónicos, es recomendable que la AEDV contacte al emisor de documentos madre con regularidad, en forma aleatoria o en casos dudosos, a fin de verificar la integridad de los documentos presentados por la persona solicitante.

3.5 Otros medios para identificar al solicitante

También es recomendable recurrir a otros medios de identificación de individuos, ya que ello reafirmará la confianza para confirmar la identidad.

3.5.1 Entrevista

Si la AEDV requiere que el solicitante se presente personalmente o si existen dudas con respecto a la integridad de la información y la documentación facilitada, puede resultar útil realizarle una entrevista. En estos casos, el personal de la AEDV debe estar capacitado para determinar su identidad a primera vista y valorar sus gestos personales y la confianza en sí mismo. Puede verificarse el parecido del solicitante con las fotos presentadas junto a la solicitud. Asimismo, pueden hacérsele preguntas personales para verificar si hay incoherencias entre la solicitud y las respuestas que dé durante la entrevista.

3.5.2 Garante

En los casos en que la entrevista no se realice o no sea posible realizarla, un método útil que se ha aplicado con éxito en algunos países para respaldar la identidad afirmada consiste en designar a profesionales como médicos, abogados, miembros del clero, entre otros, para que refrenden la

solicitud dando fe de la identidad del solicitante. Si el profesional conoce al solicitante personalmente desde hace muchos años, este puede resultar un medio de verificación eficaz. Las profesiones elegidas con este fin deben llevar registros de sus miembros mediante una asociación reconocida, y es conveniente que estos registros a su vez puedan ser verificados por la AEDV. Sin embargo, esta opción tiene el inconveniente de que es difícil que la autoridad emisora lleve el control de todas las personas autorizadas a dar su refrendo.

Algunos países recurren a garantes que no sean miembros de asociaciones reconocidas pero que sean titulares de documentos de viaje. Con este método resulta fácil verificar la información personal del garante, información que ha de ser incluida en la base de datos de la AEDV. El garante titular debe conocer al solicitante personalmente desde hace mucho tiempo y estar de acuerdo en dar fe de su identidad por escrito y bajo juramento, so pena de incurrir en perjurio.

El garante no ha de recibir ningún pago de el(la) solicitante por fungir como garante. Esta política debe indicarse en el formulario de solicitud y requerirse al garante que acepte conocerla consignando su firma. Una de las fotografías de el(la) solicitante debe presentarse firmada y fechada por el garante, como indicación de que refleja la verdadera apariencia del primero.

Para verificar sus afirmaciones, el garante es contactado de manera regular por la AEDV o, en caso de duda, con respecto a la identidad del solicitante. Por razones de seguridad no es recomendable que el garante sea un pariente cercano del solicitante, por ejemplo su padre, madre, hijos o hijas u otros parientes cercanos.

3.5.3 Referencias

Adicionalmente, o en caso de que no se recurra a un garante, puede recurrirse a las referencias de personas independientes y no relacionadas con el(la) solicitante pero que le conozcan desde hace mucho tiempo. Un mínimo de dos referencias es lo recomendable. Estas personas podrán ser contactadas por la AEDV para verificar la identidad indicada por el(la) solicitante.

3.5.4 Huella social

La huella social es la impresión que todo individuo deja en su comunidad mediante su participación personal en los acontecimientos o en sus interacciones con la sociedad. Incluso quienes tengan un perfil sumamente bajo dejarán algún tipo de impresión en la sociedad actual. Resulta difícil falsificar este tipo de información, que por lo general se construye en el transcurso de un período largo de tiempo y mediante una combinación de fuentes variadas. En la medida en que sea posible o práctico, la AEDV debe intentar establecer la marca que deje en la sociedad toda persona solicitante. La tecnología facilita cada vez más el uso de cualquier tipo de información disponible para establecer referencias cruzadas de los datos con el fin de corroborar los antecedentes de la identidad afirmada. Algunas áreas útiles de indagación para respaldar una identidad afirmada son el uso de agencias de referencia, otros registros/información financiera, detalles sobre el padre y/o la madre, registros de salud o educativos (primaria/secundaria/universitarios) detalles sobre empleos anteriores o actuales, registros tributarios o detalles sobre la residencia actual o residencias anteriores, etc.

3.5.5 Uso de la biometría

Las tecnologías biométricas permiten confirmar los rasgos físicos de la identidad de la persona cuyas características biométricas se utilizan, para determinar la autenticidad de la identidad afirmada. Una vez asignadas, las características biométricas circunscriben al individuo a una identidad específica y restringen la posibilidad de viajar o de obtener otros documentos de viaje del Estado emisor utilizando múltiples identidades. Por lo tanto, es de particular importancia verificar la

identidad antes de que la información biométrica sea vinculada a la misma. Al desarrollar el proceso de inscripción de las características biométricas, resulta valioso contar con las salvaguardas adecuadas que garanticen que se haya establecido la identidad de la persona cuyos rasgos se están inscribiendo y que la misma esté ampliamente documentada antes de fijarla permanentemente a las características registradas.

3.5.5..1Reconocimiento facial

La tecnología de Reconocimiento Facial (RF) puede servir de herramienta a la autoridad emisora para eliminar la posibilidad de que una misma persona presente varias solicitudes con diferentes nombres. Esta tecnología también es sumamente efectiva cuando se utiliza antes de que se expida un documento comparando los datos contra una lista de observación o galería de "personas indeseables" o abusadores reconocidos de documentos de viaje de forma que, al compararse con respecto a la galería de imágenes, un impostor no logrará quedar con más de un documento. Como se indicó en el Capítulo 2, para que esta tecnología funcione de manera óptima, es importante que las imágenes utilizadas al momento de solicitar el documento cumplan con las especificaciones interfuncionales internacionales establecidas por la OACI.

3.5.5..2 Otros rasgos biométricos

Cabe la posibilidad de recolectar otras características biométricas como la huella digital y el iris como parte del proceso de emisión. Para las solicitudes de renovación de documentos de viaje, las características biométricas de la persona solicitante pueden compararse con las recolectadas anteriormente para verificar que la identidad sea la misma.

3.5.6 Revisión de la base de datos

El(la) solicitante debe pasar por una revisión en la base de datos de la AEDV (o archivo cuando no exista una base de datos electrónica), a fin de garantizar que no porte otros documentos de viaje con una identidad diferente. Es importante revisar la base de datos en busca de nombres similares, con ortografía similar y semejanzas en los datos biográficos.

El sistema debe estar diseñado para llevar a cabo dos tipos de búsquedas sobre los datos del solicitante: las coincidencias y coincidencias potenciales. Éstas últimas se presentan porque algo en la base de datos (nombres propios, por ejemplo) concuerdan de manera significativa con el elemento de entrada.

Los parámetros de los sistemas electrónicos de autorización de nombres deben definirse de forma que las correspondencias aparezcan cuando haya una correspondencia cercana en lugar de cuando haya una correspondencia exacta. Por ejemplo, con el uso de nombres el solicitante en ocasiones indicará un segundo nombre, una inicial en el medio o del todo no indicará un segundo nombre. Si la base de datos espera solamente uno de estos formatos, alguna de las otras dos posibilidades puede no dar ningún resultado en el sistema de autorizaciones. Algunos perpetradores de fraudes han aprendido a variar los nombres, fechas de nacimiento, número de identificación nacional u otros elementos críticos. También se recomienda descartar los nombres anteriores cuando hayan sido cambiados por orden judicial o matrimonio, entre otras razones.

La transliteración de otros idiomas y alfabetos es un punto de preocupación, de forma que es importante disponer de software de transliteración confiable y de alta calidad. El uso de algoritmos de verificación de nombres que permitan identificar las características de diferentes idiomas y alfabetos y que estén diseñados para revisar diversos tipos de nombres permitirá una mayor precisión a este respecto.

La resolución de una búsqueda (incluyendo la anulación de las búsquedas verificadas) debe formar parte del proceso para decidir/verificar la titularidad del solicitante. El sistema de emisión debe construirse de forma que registre el nombre o número de identificación del funcionario o funcionaria que invalide o anule una búsqueda, y un determinado porcentaje de esas anulaciones o invalidaciones deben ser revisadas al azar por el personal encargado de la supervisión. Todas las revisiones de la base de datos deben completarse y todas las búsquedas deben verificarse y despejarse antes de que el pasaporte sea expedido, razón por la cual las revisiones en la base de datos deben hacerse tan pronto como sea posible dentro del proceso, de forma de no retrasar la emisión.

3.6 Restricciones de viaje

El nombre, fecha y lugar de nacimiento del solicitante deben revisarse contra una base de datos electrónica que contenga los nombres de las personas que no puedan ser titulares de un documento de viaje por diversas razones, por ejemplo, personas con antecedentes de fraude de pasaportes; personas buscadas por la policía por actividades criminales; personas que no hayan pagado su pensión alimenticia, etc.) Los datos incorporados a esta base de datos deben provenir de los distintos socios de la AEDV y de los actores clave, como es el caso de autoridades de control fronterizo y migratorias, autoridades encargadas de la aplicación de leyes, servicios correccionales, autoridades del ministerio de Relaciones Exteriores, agencias de seguridad nacional, Interpol u otras fuentes internacionales, entre otros. Alternativamente, si esta información puede ser verificada contra las bases de datos de los socios de la AEDV no requerirá ser agregada a la base de datos de la propia autoridad emisora. El reconocimiento facial u otra comparación de características biométricas puede realizarse también contra las bases de datos de restricciones de viaje que contengan fotos o identificadores biométricos de individuos conocidos o señalados. Estas bases de datos deben actualizarse con regularidad.

3.7 Acciones cuando se detecten anomalías

Si la AEDV detecta anomalías en el proceso para establecer la identidad (por ej., credenciales o información que permanezca si verificar, o identificación de algún tipo de fraude), estas anomalías deben ser investigadas antes de continuar con el proceso de emisión. Tal investigación debe incluir los siguientes procedimientos:

- A menos que resulte claro que se trata de un fraude (en cuyo caso el asunto debe ser remitido directamente a personal dedicado a investigaciones) es importante pedir primero una explicación a el(la) solicitante. Si tal explicación no es satisfactoria, entonces la solicitud deberá ser investigada por personal dedicado.
- Si existe una discrepancia legítima que requiera modificar o sustituir los documentos madre o la documentación de apoyo, el(la) solicitante debe ser nuevamente referido a la autoridad que expidió estos documentos.
- Los documentos que se sospeche son fraudulentos deben ser confiscados hasta que la identidad del solicitante quede plenamente establecida.
- Si se comprueba que la identidad o las credenciales del solicitante son fraudulentas, los detalles del fraude deben registrarse en una o varias bases de datos en aplicaciones futuras para evitar otros fraudes en que se utilice la identidad o las credenciales en cuestión.

4 Tratamiento de materiales y libretas en blanco

4.1 Resumen

Entre los materiales y documentos de viaje en blanco se encuentran las libretas, etiquetas de identificación y observación, así como las láminas de seguridad. La protección y gestión segura de los documentos de viaje en blanco y las materias primas tiene una importancia crítica para la integridad del programa de producción y emisión, ya que si se pierden o son robados podrán utilizarse para crear documentos alterados sumamente convincentes.

La AEDV debe contar con políticas y procedimientos documentados sobre el tratamiento de materiales y libretas en blanco. La información que se presenta en este capítulo servirá para desarrollar dichas políticas y procedimientos. Es importante dar un seguimiento cercano a su cumplimiento.

4.2 Producción de las libretas

En muchos países, la producción de las libretas para pasaportes se encarga a una compañía privada o a un tercero que la realiza en instalaciones independientes. La AEDV debe garantizar que los materiales se produzcan y almacenen en instalaciones que sean seguras, siguiendo las buenas prácticas para zonas de seguridad y alta seguridad que se exponen en el Capítulo 7. Es necesario que las prácticas de seguridad para el transporte, almacenamiento, conteo y destrucción sean tan estrictas en lo que respecta a los materiales utilizados por la organización encargada de la manufactura, como en lo que respecta a las libretas en blanco utilizadas por la AEDV.

4.3 Numeración

Los documentos en blanco deben producirse mediante un sistema de numeración que permita que todo documento sea identificado en cualquier paso del proceso de emisión. Ello facilitará su inventario y rastreo mientras son producidos, transportados, almacenados y personalizados. Se considera altamente recomendable que este número se convierta en el número de documento de viaje, para facilitar su rastreo en caso de que se pierda o sea robado. En otros casos, los registros de inventario de los documentos de viaje (numeración) deben mantenerse, como mínimo, durante el período de validez del documento. El número de documento de la libreta/documento de viaje debe aparecer en cada página interna de la libreta –ya sea impreso, perforado con láser, etc.– y cada página debe estar numerada en secuencia (1-2-3-4…).

Los documentos también pueden contener números de versión para facilitar su verificación. Las técnicas para la seguridad física como la perforación con láser –para el número de libreta– y la tinta UV –para el número de página– deben utilizarse también para reducir el riesgo de que la libreta sea alterada o de que algún material sea usado para crear un documento nuevo. También pueden utilizarse otras características de seguridad.

4.4 Transporte y almacenamiento

Los materiales y libretas en blanco deben mantenerse en depósitos altamente seguros, por ejemplo bóvedas o cajas de seguridad, cuyo acceso esté limitado a personas de confianza con autoridad de supervisión. El acceso a materiales únicos y el almacenamiento de las libretas en blanco debe estar limitado al menor número posible de personas. El acceso a la bóveda o caja de seguridad debe controlarse mediante el uso de carnets de identificación, identificadores

biométricos, contraseñas, etc. y las instalaciones que contengan los materiales y libretas en blanco deben permanecer vigilados 24 horas al día los 7 días de la semana por guardas de seguridad y/o por televisión en circuito cerrado. Adicionalmente, el área segura debe incluir salvaguardas contra incendios u otras pérdidas catastróficas, y es además importante que haya instalaciones de almacenamiento de respaldo para garantizar la continuidad de las operaciones en caso de que todas las libretas y materiales en blanco fuesen destruidos (Capítulo 7).

El transporte de los materiales en blanco y materiales consumibles de los documentos de viaje desde las instalaciones de su manufactura hasta la AEDV debe realizarse en forma segura (en un vehículo blindado utilizado para transportar dinero en efectivo y con funcionarios/guardas de seguridad). El transporte debe ser vigilado de cerca y todas las libretas y materiales deben ser rastreados y contabilizados en todo momento. Tanto quien envíe como quien reciba todo el material debe firmar los lotes y documentos recibidos.

La asignación de las libretas en blanco al personal de producción debe encargarse al menos a dos empleados ("principio de los cuatro ojos", firma doble). Las libretas han de estar protegidas, incluso cuando sean asignadas al personal de producción, y almacenadas bajo llave de manera segura siempre que un empleado se ausente de su puesto, por ejemplo en recesos y durante el almuerzo. Las libretas en blanco no utilizadas deben devolverse al depósito seguro al final de cada jornada o de cada turno laboral.

4.5 Conteo

Es necesario que los números de control de inventario que se insertan en las libretas en blanco al producirlas sean rastreados desde el momento en que los documentos son transportados por el fabricante, hasta que todos y cada uno de ellos hayan sido contabilizados ya sea como documentos de viaje completados o como libretas estropeadas. Los registros de monitoreo deben mantenerse durante el período de validez del documento de viaje, lo cual requiere contabilizar y registrar las cantidades totales de documentos cada vez que cambien de manos, tarea que debe ser realizada por al menos dos funcionarios(as).

Dos personas deben contar las libretas en blanco en el depósito en que se encuentren bajo llave en la mañana, y los pasaportes no utilizados deben contabilizarse otra vez todas las noches o bien al final de los turnos laborales. El número de documentos de viaje en blanco debe conciliarse al final de cada día para asegurarse de que el conteo manual coincida con lo indicado por el registro automatizado de inventario. Dicha conciliación es también necesaria en caso de que el registro de inventario sea manual. Los registros deben mantenerse al menos durante el período de validez de los documentos de viaje y han de ser inspeccionados todos los días por un tercero, o una vez por turno laboral.

Los miembros del personal que tengan acceso a las libretas en blanco, ya sea para su almacenamiento o su producción, deben pasar por una revisión cada vez que salgan de las instalaciones de la AEDV, o bien con fines específicos o en forma aleatoria, para garantizar que ninguna libreta en blanco salga de allí.

4.6 Destrucción

La destrucción de libretas en blanco en exceso o que se encuentren estropeadas, defectuosas o parcialmente completadas debe encargarse y ser presenciada por dos funcionarios ("principio de los cuatro ojos"), tarea que debe realizarse a diario para evitar que se acumulen grandes cantidades de libretas. Además, se requiere que estas libretas sean contabilizadas para que las cifras coincidan con las del inventario maestro.

5 Personalización y entrega

5.1 Resumen

La personalización del documento de viaje se refiere a la incorporación de los datos variables a la libreta en blanco. En el caso del pasaporte esto incluye los datos personales de el(la) solicitante (incluyendo la foto del portador) que aparecerán impresos en la página de datos, así como la información que queda codificada en el chip.

Una vez personalizado, el documento de viaje puede entregarse por distintos medios, por ejemplo entrega personal (o a un tercero), correo seguro o servicios de entrega o de mensajería. Dependiendo de el(los) método(s) seleccionado(s), es posible recurrir a algunas técnicas para atenuar el riesgo de que un documento de viaje sea entregado a alguien que esté haciéndose pasar por el verdadero solicitante o que esté utilizando una identidad falsa.

5.2 Personalización

La función de personalización debe llevarse a cabo en un área altamente segura, por ejemplo una bóveda de seguridad a la que solamente tengan acceso individuos seleccionados. El control de acceso a la bóveda puede garantizarse mediante diversas tecnologías como el uso de carnets de identificación, identificadores biométricos, etc. En el Capítulo 7 se presentan más detalles sobre la seguridad física.

Debido a que el proceso de personalización requiere de la manipulación de materiales y libretas en blanco, todas las buenas prácticas que se incluyen en el Capítulo 4 deben seguirse, incluyendo la presencia de dos personas en todo momento durante el proceso de personalización. Es importante que la transmisión de los datos personales de el(la) solicitante a la imprenta/encargado de la codificación quede protegida mediante las buenas prácticas de seguridad informática que se detallan en el Capítulo 8.

5.2.1 Control de calidad

Una vez personalizado, el documento de viaje debe someterse a un proceso de aseguramiento de la calidad que garantice que no contenga errores ni desperfectos que puedan influir en la revisión a la que se sometería al titular en los cruces fronterizos cuando viaje.

En el caso de un DVLM regular, la zona de lectura mecánica debe ser leída por un lector equivalente a los utilizados en la frontera y la información contenida allí debe compararse con la de la página de datos, la información de la persona solicitante incluida en la base de datos de la AEDV, así como los formularios originales presentados por ésta. La página de datos también debe ser revisada para que quede debidamente terminada, cosida y laminada, además de verificarse unas cuantas características de seguridad (al azar).

Para un pasaporte-e, los datos del chip (incluyendo la foto) deben ser leídos también por un lector y compararse con los datos contenidos en el documento de viaje, la ZLM y la base de datos de la AEDV, así como los formularios de solicitud. Por último, es necesario verificar la validez/integridad de la firma digital empleada para proteger el chip.

5.3 Entrega o envío

5.3.1 Entrega personal

Se sugiere que sea el(la) solicitante quien recoja su documento de viaje recién emitido. Sin embargo, esto no resulta siempre práctico por razones geográficas, además de que podría derivar en un elevado número de solicitantes en las oficinas de la AEDV. Si se recurre a esta opción puede entregarse a el(la) solicitante un recibo al momento de registrar la solicitud.

Al entregar el documento de viaje, el empleado debe verificar y comparar la fotografía del documento (incluyendo la registrada en el chip) con la fotografía de la base de datos y con la persona propiamente. Para certificar que quien recoge el pasaporte sea el titular legítimo pueden utilizarse otras técnicas: puede pedirse a el(la) solicitante que muestre una identificación adicional que contenga una foto o datos personales como la dirección, segundo apellido, entre otros, y también cabe la posibilidad de verificar las características biométricas, esto es, recurrir a la tecnología de reconocimiento facial o la huella digital. Asimismo, es importante que el solicitante firme un recibo en señal de que ha recogido el documento especificando la fecha y hora, y actualizarse el estado de entrega del documento en la base de datos de la AEDV.

No es recomendable que el documento de viaje sea entregado a un tercero, por ejemplo un representante o pariente. Sin embargo, si es una opción permitida, éste debe presentar una autorización escrita y establecer su identidad mediante documentos de identificación que tengan su foto. En este caso, quien recoja el documento debe firmar también un recibo.

La AEDV podría utilizar un sistema de alerta para monitorear si el tiempo transcurrido una vez que el documento está listo para ser recogido se encuentra estandarizado. Si después de un tiempo los documentos no son reclamados la persona solicitante debe ser contactada. Es recomendable investigar en busca de fraudes los documentos que no sean reclamados.

5.3.2 Servicios de correo

Si los documentos de viaje personalizados son enviados por correo, es necesario que el servicio de correos sea confiable. Si el servicio público no es confiable, una alternativa es el correo controlado o un servicio privado de correo, por ejemplo uno de mensajería. En todos los casos ha de requerirse la firma de la persona solicitante o de alguien que viva en su misma dirección al momento de la entrega. La confirmación de entrega también ha de indicarse en la base de datos del AEDV. Si el servicio de correo utilizado no requiere la firma al momento de recibo, podría recurrirse a otros métodos como la devolución de una palabra código o de un recibo a la autoridad emisora. De nuevo, dicha autoridad podría aplicar un sistema de alerta para monitorear la confirmación de recibo del documento de viaje en períodos de tiempo estandarizados.

Entre las razones por las que los documentos de viaje enviados por correo no sean recibidos por el solicitante cabe mencionar:

- el documento fue enviado a una dirección equivocada por error de la AEDV;
- el documento se perdió en el correo por error del servicio de correos o de mensajería;
- el documento fue enviado a una dirección equivocada debido a un error del solicitante; o
- se trata de un indicador de fraude.

El hecho de que un pasaporte con la dirección correcta regrese a manos de la autoridad emisora por no concretarse su entrega puede ser un indicador de fraude, y es algo que debe verificarse contra la información incluida en el formulario de solicitud. Si la dirección es correcta y se ha verificado su existencia, la persona solicitante debe ser contactada para que recoja el documento

de viaje en las instalaciones de la autoridad emisora y de lo contrario el expediente debe remitirse para ser investigado como fraude.

Si el(la) solicitante reclama que no ha recibido un pasaporte que la AEDV ya envió, el caso debe ser manejado igual que si se tratara de un documento perdido o robado. El documento debe ser declarado de inmediato como inválido, incluirse e una base de datos de pasaportes perdidos/robados, e indicarse al solicitante que si el documento es posteriormente encontrado o recibido no podrá utilizarlo y deberá devolverlo a la AEDV para su destrucción segura.

6 Seguridad de los documentos de viaje

6.1 Resumen

En este capítulo se abordan las características físicas, técnicas y las características de los documentos de viaje, incluyendo el refuerzo de su seguridad y el incremento de su resistencia a los ataques y al uso indebido. Debido al acceso extendido a tecnologías de bajo costo que incluyen el escaneo de alta calidad, reproducción a color, procesamiento de imágenes e impresión de fotográfica de calidad, la capacidad de las personas para producir documentos de viaje convincentes pero alterados y alteraciones sumamente engañosas ha crecido de manera exponencial. Las siguientes son amenazas físicas que enfrentan los documentos de viaje:

- alteración de un pasaporte o documento de viaje completo;
- sustitución de la fotografía;
- borrado/alteración de la zona visual o de lectura mecánica de la página de datos en los DVLM; elaboración de documentos fraudulentos o partes de éstos, utilizando materiales de documentos legítimos;
- remoción y sustitución de páginas completas o visas;
- borrado de datos en las páginas de visas y en la página de observaciones;
- robo y personalización de documentos auténticos en blanco; y
- manipulación del chip (cuando exista) ya sea física o electrónicamente.

En esta Guía se expone una visión de conjunto de los principales avances en la tecnología de DVLM y en los conceptos de seguridad. El tema de la seguridad de los documentos de viaje se analiza en detalle en el **Anexo informativo del Documento 9303, Volumen 1, Sección III: Normas de seguridad para los documentos de viaje de lectura mecánica**.

6.2 Documentos de viaje de lectura mecánica (DVLM)

El DVLM es aquél que contiene, en un formato estandarizado, los detalles de identificación del titular, incluyendo una foto (o imagen digital), además de que los elementos de identidad obligatorios aparecen reflejados en una zona de lectura mecánica (ZLM) de dos líneas, impresos en un formato de reconocimiento óptico de caracteres. Las especificaciones de la OACI sobre los DVLM se encuentran detalladas en el **Documento 9303 de la OACI, Parte 1, Volumen 1.**

Este tipo de documento de viaje se desarrolló para lograr un mayor interfuncionamiento internacional y para incrementar la seguridad. Supone importantes beneficios para todos los actores clave incluyendo los gobiernos, aerolíneas y los viajeros, con costos de implementación relativamente bajos. Su formato uniforme amplía su capacidad de autenticación visual. Los datos estandarizados que pueden leerse hacen posible su vinculación a diversas bases de datos y permite compartir la información con varios actores clave para detectar mejor documentos falsos, robados o fraudulentos y por consiguiente mejora los procesos de control fronterizo. Asimismo, el DVLM simplifica el uso de sistemas Avanzados de Información de Pasajeros (AIP).

El DVLM permite el registro automatizado de datos: una mejora significativa con respecto al registro manual. Para ejemplificar los beneficios en cuanto a facilitación que ha traído consigo el DVLM cabe mencionar una mayor rapidez en el registro de datos con menos errores. Las ganancias en términos de facilitación, interfuncionamiento global y seguridad que ha traído consigo el uso de DVLM condujeron a la adopción de la **Norma 3.10 de la OACI** que requiere que todos los Estados Miembros de la OACI comiencen a emitir solamente pasaportes de lectura mecánica (PLM) a partir del 1 de abril del 2010 y que eliminen de manera gradual los pasaportes que no sean de lectura mecánica y que todavía se encuentren en circulación para el 24 de noviembre del 2015.

El Grupo de Trabajo sobre Implementación y Fortalecimiento de Capacidades (ICBWG) se conformó para apoyar a la Secretaría de la OACI en la realización de actividades de divulgación y desarrollo de capacidades para ayudar a los países a cumplir con el plazo de abril del 2010. Es recomendable que los países que necesiten ayuda para implementar su programa de pasaportes de lectura mecánica se comuniquen con el Programa correspondiente de la Secretaría de la OACI.

6.3 El pasaporte de lectura mecánica electrónico (PLM-e, pasaporte-e)

El trabajo realizado por la OACI desde 1998 redunda en el desarrollo de una nueva generación de documentos de viaje: el pasaporte de lectura mecánica electrónico o PLM-e. Este es un DVLM que contiene un circuito integrado sin contacto (IC) en su interior en el que se almacena la información de la página de datos del pasaporte y una medición de las características biométricas del titular. Los datos codificados en el chip se encuentran protegidos mediante tecnología de criptografía de Infraestructura de Clave Pública (ICP). Las especificaciones de la OACI sobre los PLM-e se encuentran en el **Documento 9303 de la OACI, Parte 1, Volumen 2.** Si bien la OACI identificó la imagen facial como el identificador biométrico de preferencia para alcanzar un interfuncionamiento global, la huella digital y el iris pueden utilizarse también como identificadores secundarios. El Control de Acceso Básico (CAB) y el Control de Acceso Extendido (CAE) se utilizan para proteger los datos del acceso no autorizado.

El pasaporte-e representa la mejora más significativa en la seguridad de los documentos de viaje desde que se introdujo el DVLM. Este mejora la integridad del documento al permitir establecer una correspondencia entre la información contenida en el chip, con los datos impresos en el documento y con las características físicas del titular; en otras palabras, permite una verificación en tres vías. El PLM-e también permite una verificación asistida por computador de la información biométrica y biográfica, estableciendo la correspondencia entre el documento y el viajero como su titular legítimo, a la vez que verifica contra las listas de observación o bases de datos adecuadas.

Si bien el PLM-e no es la respuesta a todos los tipos de fraude, ofrece una mayor protección contra el uso y manipulación fraudulenta, además de reducir el riesgo de fraude de identidad en los cruces fronterizos al mejorar la detección de impostores.

La **Práctica recomendada 3.9** del Anexo 9 del Convenio de Chicago tiene por objetivo que los Estados Contratantes de la OACI incorporen los datos biométricos a sus pasaportes de lectura mecánica, visas y otros documentos de viaje oficiales.

⇒ Para mayor información sobre el Pasaporte-e véase: APEC, a Guide to Biometric Technology in MRTDs (http://www.apec.org/apec/publications/free_downloads/2007.html)

Directorio de Claves Públicas de la OACI (DCP)
Una capa adicional de seguridad se agrega cuando la autenticidad de los datos del chip del PLM-e son validados en la frontera mediante los certificados de Infraestructura de Clave Pública (ICP). Tal validación se realiza para confirmar que:

- el documento que porta el viajero fue emitido por una autoridad de buena fe;
- la información biográfica y biométrica avalada en el documento al momento de expedirse no fue alterada posteriormente.

EL DCP fue establecido por la OACI para que funja como intermediario central en la gestión de intercambios entre certificados de infraestructura de claves públicas de pasaportes-e y las listas de revocación de certificados. Esta función resulta esencial para minimizar el volumen de intercambio

de certificados entre países, garantizar que la información se suba en forma oportuna y gestionar el apego a las normas técnicas que garantice que el interfuncionamiento se logre y se mantenga.

En abril del 2009 el Consejo de la OACI adoptó una Práctica recomendada relativa al DCP-OACI (Véase la Sección 6.4.2 sobre las Normas y Prácticas Recomendadas por la OACI).

⇒ Para mayor información sobre el DCP y cómo integrarse a éste: http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx

6.4 Normas, prácticas recomendadas y especificaciones de la OACI

6.4.1 Especificaciones contenidas en el Documento 9303

Para alcanzar el interfuncionamiento global y por lo tanto mejorar la seguridad, los documentos de viaje deben cumplir con las especificaciones de la parte correspondiente del Documento 9303:

Parte 1: Pasaportes de lectura mecánica

> **Volumen 1:** Pasaportes con datos de lectura mecánica almacenados en formato de reconocimiento óptico de caracteres.
>
> **Volumen 2:** Especificaciones para pasaportes habilitados electrónicamente con capacidad de identificación biométrica.

Parte 2: Visas de lectura mecánica

Parte 3: Documentos de viaje oficiales de lectura mecánica

> **Volumen 1—** Documentos de viaje oficiales de lectura mecánica – DVLM con datos de lectura mecánica almacenados en formato de reconocimiento óptico de caracteres.
>
> **Volumen 2—** Documentos de viaje oficiales de lectura mecánica – Especificaciones para DVLM electrónicos con capacidad de identificación biométrica.

Para ordenar el *Documento 9303* diríjase a*:* http://icaodsu.openface.ca/mainpage.ch2 .

Históricamente, el Documento 9303 no contiene recomendaciones específicas con respecto a las características de seguridad que deben incluirse en los documentos de viaje. Cada Estado debe decidir, con base en sus evaluaciones de riesgos, cuál es la combinación de características de seguridad que se ajusta a sus necesidades.

Sin embargo, debido a la necesidad de una mayor seguridad en los documentos, la OACI publicó un documento de orientación sobre **Normas de seguridad para documentos de viaje de lectura mecánica** en la forma de un anexo informativo al Documento 9303, Volumen 1, Sección 3. Las recomendaciones incluidas en este documento abarcan la seguridad de los materiales empleados en la elaboración del documento, las técnicas de seguridad y protección en la impresión y reproducción que han de emplearse, así como los procesos utilizados en la producción de documentos en blanco. Es recomendable utilizar una combinación adecuada de estas características y técnicas, incorporadas al momento de la producción y/o al momento de personalizar los documentos, para abordar distintos tipos de ataques potenciales al documento. En última instancia la AEDV debe liderar y ser la autoridad encargada de aprobar el diseño del documento de viaje, sus características de seguridad y la elección de los materiales empleados en su elaboración.

6.4.2 Normas y prácticas recomendadas de la OACI

Algunos estándares y prácticas recomendadas que incluye el Capítulo 3 del Anexo 9 del Convenio de Chicago abordan de manera puntual la seguridad de los documentos de viaje. La AEDV debe cumplir con estas normas y seguir las prácticas recomendadas, en la medida de lo posible.

Seguridad de los documentos de viaje
Norma 3.8 – Los Estados Contratantes establecerán controles para la creación y emisión de documentos de viaje, a fin de crear salvaguardas contra el robo de sus inventarios y la apropiación indebida de los documentos de viaje recién expedidos.

Norma 3.7 — Los Estados Contratantes actualizarán de manera regular las características de seguridad en versiones nuevas de sus documentos de viaje, para protegerse contra su uso ilegal y facilitar la detección de casos en los que tales documentos hayan sido ilegalmente alterados, reproducidos o expedidos.

Debido a que las características de seguridad en un documento seguro pueden verse comprometidas en cualquier momento después de su implementación, es una buena práctica modificar su diseño aproximadamente cada cinco años. La introducción periódica de versiones rediseñadas y más seguras de los documentos de viaje impedirá actuar a los falsificadores. Tecnologías más avanzadas y seguras han de incorporarse en cada nueva versión del documento de viaje y deben ser comunicadas de forma segura y en confianza a todos los funcionarios que deban examinar el documento. Para facilitar esto, los documentos de viaje deben indicar la versión a la que corresponde su emisión.

Período de validez del pasaporte
Norma 3.4 — Los Estados Contratantes no ampliarán la validez de su documento de viaje de lectura mecánica.

Práctica recomendada 3.16 - …Los Estados Contratantes normalmente deberán prever que tales pasaportes tengan validez por un período de al menos cinco años… Nota 1 — En consideración a la durabilidad limitada de los documentos y la apariencia cambiante del titular con el paso del tiempo, se considera recomendable un período de validez no mayor a diez años.

Los estudios demuestran que las características de seguridad en un documento seguro comienzan a verse seriamente comprometidas a los pocos años de su implementación, por lo que se recomienda rediseñar y reemplazar el documento después de cinco años. Sin embargo, el servicio, el volumen y las implicaciones financieras son todas consideraciones importantes que han de tomarse en cuenta al determinar el período de validez del pasaporte.

Un pasaporte/una persona
Norma 3.15 – Los Estados Contratantes expedirán un pasaporte por aparte para cada persona, independientemente de la edad de la misma.

En el 2002, la OACI adoptó la norma de un pasaporte/una persona para maximizar los beneficios que traen consigo los pasaportes de lectura mecánica y combatir el secuestro y la trata internacional de niños y niñas.

Pasaportes de lectura mécanica
Norma 3.10 — Los Estados Contratantes comenzarán a expedir solamente Pasaportes de Lectura Mecánica de conformidad con las especificaciones del Doc 9303, Parte 1, a más tardar en abril del 2010.

Norma 3.10.1 – Para los pasaportes expedidos después del 24 de noviembre del 2005 y que no sean de lectura mécánica, los Estados Contratantes garantizarán que la fecha de vencimiento sea antes del 24 de noviembre del año 2015.

Documentos de viaje con identificadores biométricos
Práctica recomendada 3.9 – Los Estados Contratantes deberían incorporar los datos biométricos a sus pasaportes de lectura mecánica, visas y otros documentos oficiales de viaje, utilizando una o

más tecnologías de almacenamiento de datos para complementar la zona de lectura mecánica, como se especifica en el Doc 9303…

Directorio de claves públicas de la OACI
Práctica recomendada 3.9.1 – Es recomendable que los Estados Contratantes que (a) expidan o tengan la intención de expedir pasaportes-e y/o (b) que implementen en los puestos de control fronterizo revisiones automatizadas de los pasaportes-e se integren al Directorio de Claves Públicas de la OACI (DCP).

6.5 Tipos de documentos de viaje

Es altamente recomendable que las características mínimas de seguridad (mencionadas en la Sección 6.4.1 del Doc. 9303) se agreguen a todos los tipos de documentos de viaje, incluyendo pasaportes diplomáticos, oficiales, especiales, y en particular a los pasaportes temporales y de emergencia. Los pasaportes diplomáticos y los oficiales (especiales) deberían utilizar las mismas libretas en blanco y materiales que los pasaportes regulares, salvo por el color de la cubierta de la libreta.

Los pasaportes temporales y/o los de emergencia se expiden en el exterior por situaciones de urgencia comprobada o debido a requisitos relacionados con la residencia. La validez de un pasaporte de emergencia o temporal se limita a que el(la) solicitante cumpla con los requisitos de viaje. En muchos casos se trata de un único viaje para regresar al país de origen. Es recomendable que estos documentos, que en la actualidad se consideran altamente riesgosos para la seguridad, incluyan algunas características mínimas de seguridad para evitar que los datos sean borrados o alterados.

7 Seguridad de las instalaciones

7.1 Resumen

La seguridad de las instalaciones (o seguridad física) abarca los medios utilizados para prevenir el acceso no autorizado a las instalaciones y zonas de acceso restringido por parte de personas externas o del personal, así como para proteger los activos y la información. Hay múltiples estrategias y tecnologías para garantizar la seguridad de las instalaciones. Es recomendable que la AEDV emplee una gama variada de ellas según se considere adecuado, considerando las amenazas y vulnerabilidades así como los costos, la privacidad y los inconvenientes en términos de las operaciones.

7.2 Políticas de seguridad física

Es importante contar con una política integral de seguridad que abarque todas las instalaciones y espacios utilizados en el proceso de emisión, incluyendo espacios de oficina, áreas de producción, áreas de atención al cliente, salas de redes y de computadoras, entre otros. Esta política debe apegarse a las normas y lineamientos gubernamentales, así como a las normas internacionalmente aceptadas.

Si bien se trata ante todo de una norma ISO sobre tecnología de la información, el estándar ISO/IEC 27002:2005 para la seguridad de la información es una referencia ideal para mejorar la seguridad en la gestión de la información en las organizaciones. Esta norma aporta buenas prácticas relacionadas, entre otros, con la seguridad física y del entorno. Además, prevé salvaguardas y medidas para mitigar los riesgos de seguridad, además de asistencia adecuada para su implementación relacionada con el control de ingreso, seguridad de salones e instalaciones, trabajo en áreas seguras, acceso público y áreas de carga y entrega de productos, todas las cuales aplican a las instalaciones de la AEDV.

La norma ISO 27007 guarda una estrecha relación con la ISO/IEC 27001:2005, la cual establece los procedimientos y lineamientos para el desarrollo, implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Ambas normas se encuentran disponibles en la dirección http://www.iso.org/iso/store.htm.

Es recomendable que todas las instalaciones de la AEDV, o al menos las zonas dedicadas a las operaciones, seguridad y alta seguridad (véase la tabla a continuación), sean propiedad del gobierno a fin de garantizar un control completo y flexibilidad para la adopción de medidas para la seguridad física. Las instalaciones de socios tanto del sector público como del privado involucradas en el proceso de emisión también deben cumplir con las normas de seguridad definidas por la AEDV.

Todo el personal debe contar con la información y capacitación sobre las políticas y prácticas relativas a la seguridad física. Es importante que existan sanciones para el personal que no las cumpla, por ejemplo por no escoltar a los visitantes, no portar sus gafetes de identificación, permitir el acceso a personal no autorizado en zonas de acceso restringido, etc.

- Para un ejemplo de una política gubernamental de seguridad, véase “Operational Security Standard on Physical Security “, (Norma de seguridad operativa relativa a la seguridad física) del Gobierno de Canadá (2004): http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/osps-nosm-eng.asp.

7.3 Zonas de seguridad

Todas las instalaciones y áreas de trabajo de la AEDV deben estar definidas en función de las zonas de seguridad a las que deba adaptarse la seguridad física con base en las actividades que se lleven a cabo allí, el valor de los activos y los datos almacenados, como se indica a continuación:

Zonas	Actividades/funciones	Seguridad física
Área de acceso no restringido		
Zona de acceso público	• Alrededor de las instalaciones • Escaleras	• Ningún control de acceso • Pueden someterse a monitoreo para detectar actividades sospechosas
Zona de recepción	• Área de atención al cliente • Contacto inicial entre visitantes y la organización	• Acceso limitado a horas específicas del día • Detección de intrusos • Monitoreo en puntos de entrada (personal de seguridad) • Monitoreo para vigilar violencia relacionada con el trabajo • Puede haber otras medidas de protección física para proteger al personal
Áreas de acceso restringido		
Zona de operaciones	• Espacio de oficinas • Manejo de solicitudes/verificación de la titularidad	• Acceso controlado • Detección de intrusos • Monitoreo • Armario/mueble y caja de seguridad bajo llave (para datos/trabajo en proceso)
Zonas de seguridad y alta seguridad	• Personalización de documentos de viaje • Almacenamiento de libretas en blanco • Área de manejo de dinero en efectivo • Sala de redes • Almacenamiento de expedientes de solicitantes	• Acceso controlado y altamente restringido • Detección de intrusos • Monitoreo 24 hr. al día, 7 días x sem. • Especificaciones sobre seguridad física, por ej., bóveda/caja de seguridad.

7.3.1 Área de atención a clientes

La seguridad física es un elemento necesario para garantizar la salud y la seguridad de los empleados en el trabajo y para prevenir la violencia relacionada con el trabajo. Debido a la naturaleza de la producción y emisión de documentos de viaje, es posible que surjan situaciones en que el personal enfrente amenazas de violencia debido a sus obligaciones o debido a situaciones a las que se encuentre expuesto.

El área en donde el público solicita y recibe los documentos de viaje debe estar construida de forma tal que los clientes no tengan un acceso físico fácil al dinero pagado por concepto de cargos o al personal, para efectos de la seguridad de éste y de los materiales y las libretas en blanco. De ser necesario, la seguridad física puede incluir alarmas de coacción, vidrio a prueba de balas o magnetómetros u otras tecnologías para detectar armas que porten los solicitantes. También es recomendable que haya personal de seguridad presente en horas laborales para que dé una presencia tranquilizante en casos de agitación por parte de éstos, así como para escoltarles a su salida del área en caso de que ocasionen perturbaciones.

Es posible que haya una sala en donde el personal de policía entreviste a posibles perpetradores de fraude captados durante el proceso de solicitud o cuando regresen a recoger su documento de viaje. Sin embargo, quizás resulte preferible en determinadas circunstancias que el personal de policía saque a la persona de las instalaciones para su cuestionamiento.

7.3.2 Manejo de las solicitudes y verificación de la titularidad de los solicitantes (zona de operaciones)

Las áreas de operaciones, seguridad y alta seguridad deben designarse como zonas de acceso restringido, de forma que su acceso sea exclusivo para el personal autorizado. El acceso a las oficinas de manejo de solicitudes debe ser controlado y limitarse al personal que tenga autorización en razón de sus funciones y que haya pasado por un proceso de selección para pasar al nivel apropiado de seguridad. En ocasiones, es posible que personas visitantes o contratistas cumplan funciones en la zona de acceso restringido, aunque deben estar escoltadas en todo momento. El personal de limpieza y los guardas de seguridad deben contar también con permisos de seguridad. El acceso del personal a esta área ha de estar restringido a determinados períodos, esto es, solamente durante su turno de trabajo.

7.3.3 Área de personalización (zonas de seguridad y alta seguridad)

Esto incluye el área donde se encuentre la bóveda/caja de seguridad para el almacenamiento de las libretas en blanco y materiales y en donde se personalicen los documentos de viaje. El acceso a esta área debe ser altamente restringido y para ello existen varios métodos de control de acceso. Se recomienda el uso de una autenticación bifactorial, por ejemplo con tarjetas electrónicas, claves, códigos PIN e identificadores biométricos. El área donde se realice la personalización de los documentos de viaje debe quedar bajo llave al final de cada jornada laboral. Han de utilizarse sistemas de monitoreo y los aparatos de detección de intrusos para minimizar las posibilidades de robo. A fin de prevenir los robos internos, es recomendable instituir una política para prevenir que los empleados se encuentren solos en las áreas seguras. Así, debido a que un complot que involucre a más de una persona será inevitablemente más complejo y requerirá de una planificación avanzada, las oportunidades de actividades criminales espontáneas se verán reducidas (Capítulos 4 y 5).

7.4 Control de acceso y monitoreo

El control del acceso es un componente importante de cualquier abordaje de la seguridad física. Desde luego, el que se trate o no de un control eficaz para desalentar una amenaza depende de la índole de la amenaza. Controlar el acceso ofrecerá una protección mínima de quienes ya tengan acceso a las instalaciones, y por lo tanto será necesario que existan controles internos como los que se exponen en el Capítulo 9. Los equipos de monitoreo y detección de intrusos serán útiles para vigilar a distancia las áreas de ingreso en las que se pueda obtener el acceso a las instalaciones y algunas zonas que requieran de una mayor seguridad.

Existen diversos métodos de control del acceso, detección de intrusos y monitoreo, cada uno de los cuales ofrece diferentes niveles de protección y supone distintos costos. Es recomendable utilizar una combinación de estrategias y tecnologías. Vale la pena considerar el nivel de inconvenientes que cada opción ofrezca y el impacto en la privacidad del personal y del público. El control del acceso debe resultar tan conveniente para la normalidad de las operaciones como sea posible. A continuación se plantean algunas estrategias que podrían emplearse en todas las

instalaciones de la AEDV, con base en el nivel de seguridad requerido y las evaluaciones de riesgos y amenazas.

- **Personal de seguridad**: los guardas que tienen la tarea de velar por la seguridad en el sitio y monitorear todas las instalaciones las 24 horas del día, los siete días de la semana.

- **Gafetes de identificación para el acceso:** los empleados(as) han de llevarlos en todo momento mientras se encuentren en zonas de acceso restringido (zonas de operaciones, seguridad y alta seguridad). Estos gafetes deben llevar claramente la fotografía de su portador y mostrar códigos de colores u otros códigos que resulten obvios que indiquen visualmente los privilegios de acceso del portador. Los derechos de acceso para todo el personal deben someterse a auditorías de rutina. En caso de que se termine la relación de empleo la organización debe reclamar el gafete. Los visitantes y contratistas deben contar con gafetes temporales que les sean entregados a cambio de alguna identificación aceptable que incluya una fotografía, la cual ha de ser retenida por el personal de seguridad. Los miembros del personal deben firmar en un libro de registro de visitas, de forma que la identificación les sea devuelta cuando reintegren el gafete de acceso.

- **Acompañantes**: los visitantes deben estar acompañados en todo momento por un miembro del personal cuando se hallen en zonas de acceso restringido. Esto también se aplica al personal de la AEDV a que cuente con autorización de seguridad o que su cargo le restrinja el acceso a algunas zonas.

- **Barreras electrónicas o físicas en los puntos de entrada**: este es el caso de las puertas comunes, puertas giratorias y portones.

- **Cerraduras**: utilice llaves de distribución limitada, números de PIN, tarjetas electrónicas o llaves, o bien indicadores biométricos. Los números de PIN deben cambiarse con regularidad. Incluso en horas laborales, las puertas exteriores a las zonas de acceso restringido deben mantenerse bajo llave y solamente el personal gubernamental ha de tener acceso, las combinaciones o utilizar tarjetas electrónicas que permitan el acceso. Otras personas que requieran ingresar han de ser monitoreadas y permitírseles el acceso utilizando pantallas de reconocimiento visual en las puertas y mecanismos para abrir las puertas a distancia.

- **Detección de intrusos**: por ejemplo mediante alarmas y sensores de movimiento.

- **Monitoreo**: uso de monitores en las puertas, cámaras y circuitos cerrados de televisión (CCTV). Los registros de los videos de monitoreo deben mantenerse durante períodos apropiados o durante más de tres meses.

7.5 Otras medidas y prácticas relacionadas con la seguridad física

Algunas áreas o zonas requieren de medidas específicas de seguridad. Por ejemplo, las zonas de seguridad y alta seguridad requieren de medidas especiales de construcción, como es el caso de bóvedas o cajas de seguridad, mientras que el área de atención al cliente podría demandar el uso de equipos para la detección de armas y sistemas para la protección de los empleados, incluyendo vidrios a prueba de balas y alarmas de coacción.

El correo, incluyendo los materiales y solicitudes de documentos de viaje recibidas, debe seleccionarse en una sala o habitación especial debidamente ubicada, cuyo personal esté capacitado para detectar la presencia de materiales sospechosos mediante Rayos-X u otros métodos, además de aplicar un protocolo una vez identificado el material sospechoso.

Asimismo, es importante considerar la protección de las instalaciones, activos y datos contra incendios u otras pérdidas catastróficas. Es recomendable tomar medidas para el trabajo en sitios alternativos y contar con sitios de almacenamiento de respaldo, a fin de garantizar la continuidad de las operaciones en caso de que se imposibilite el acceso a las instalaciones utilizadas para la emisión, o bien en caso de destrucción de los materiales y los datos.

La información organizativa y los datos de quienes soliciten puestos de personal deben estar protegidos. Se requiere utilizar un armario bajo llave y salones protegidos para almacenar y proteger la información. Asimismo, han de utilizarse equipos para la destrucción o trituración de documentos, a fin de eliminar la información que ya no se requiera. Este aspecto se analiza en el Capítulo 2.

8 Seguridad informática

8.1 Resumen

La seguridad informática se define como las salvaguardas establecidas para preservar la confidencialidad, integridad, disponibilidad, uso deseado y valor de la información almacenada, procesada o transmitida en forma electrónica. En el pasado era posible proteger la información sencillamente controlando el acceso físico a la misma, pero en la era actual de interconexión mediante redes este tema plantea un desafío, ya que una inmensa cantidad de la información privada se encuentra almacenada en redes informáticas que suelen estar interconectadas.

Este es un aspecto de preocupación para la AEDV, cuya labor está cada vez más automatizada y se vale de la tecnología de la información para incrementar su eficiencia, seguridad y la eficacia en la prestación de sus servicios. Al mismo tiempo, el número y gravedad potencial de las amenazas, vulnerabilidades e incidentes aumentan de manera similar. Debido a que la AEDV requiere recolectar información personal detallada, en ocasiones incluyendo datos biométricos, la protección y seguridad de los sistemas informáticos y bases de datos resulta de importancia crucial.

8.2 Políticas y prácticas de seguridad informática

Es importante instituir una política de seguridad informática que se encuentre actualizada de acuerdo a las tecnologías y prácticas vigentes, que cubra todos los sistemas informáticos, bases de datos, flujos de información, etc. Esta política debe hacer referencia e incorporar normas internacionales vigentes tales como la ISO/IEC 27002:2005 para la seguridad de la información:http://www.iso.org/iso/store.htm. (Mencionada en el Capítulo 7).

Esta norma ISO ofrece los lineamientos para el desarrollo de normas de seguridad adecuadas y prácticas de gestión de la seguridad relacionadas con todos los tipos de información. Las políticas y prácticas de seguridad constituyen un elemento central de esta norma, que cubre la gama completa de aspectos de gestión de la seguridad. Se divide en once áreas de gestión que abarcan desde la gestión de las políticas de seguridad hasta la continuidad del negocio.

Un elemento importante de esta norma es las evaluaciones que contempla para identificar los riesgos y requerimientos de protección. Ello incluye evaluaciones de vulnerabilidad, de la privacidad de los datos informáticos, pérdida de información de bases de datos, acceso no autorizado a los datos, además de cualquier otra evaluación relacionada que deba llevarse a cabo regularmente para implementar medidas de protección, prevención y mitigación.

A continuación se mencionan una serie de aspectos que deben abordarse en las políticas y prácticas de seguridad:

- clasificaciones adecuadas de **confidencialidad** de las bases de datos e información relacionada, como es el caso de listas de observación, datos biométricos y otros activos de información. Es necesario contar con los medios y las tecnologías para prevenir el acceso, interceptación, reproducción u obtención electrónica por parte de personas equivocadas;
- **protección de la integridad de los datos** contenidos en las bases de datos e información relacionada, a fin de evitar que esta información sea modificada, añadida o borrada, salvo en los procesos debidamente definidos;
- **disponibilidad de los datos** contenidos en bases de datos y de la información relacionada, a fin de evitar que esta información sea bloqueada u ocultada a sus usuarios legítimos cuando estos la requieran;

- **permisos de acceso** a las bases de datos e información relacionada, de forma tal que esta información pueda ser accedida solamente por **sus usuarios autorizados legítimos.**

Todas estas políticas, prácticas, tecnologías y metodologías deben ser evaluadas por auditores informáticos profesionales, a fin de verificar su eficiencia y su desempeño.

Todos los productos tecnológicos como paquetes informáticos de bases de datos, servidores, instalaciones de comunicación, módulos de seguridad del hardware y otros productos comerciales que sean utilizados, deben ser certificados al Nivel de Aseguramiento de la Evaluación (NAE) de la seguridad que corresponda. Asimismo, es importante que los aparatos de criptografía utilizados estén certificados al nivel adecuado mediante estándares internacionales como el FIPS 140-2 o su equivalente.

8.3 Seguridad de los usuarios

8.3.1 Control de acceso

El acceso al sistema informático y a las bases de datos de la AEDV debe restringirse, mediante el uso de identificaciones biométricas o de nombres de usuario y contraseñas únicas para que las personas usuarias autorizadas ingresen al sistema. Tal acceso debe limitarse mediante el procesamiento de permisos y accesos a determinadas bases de datos, aplicaciones y tareas. Las contraseñas deben constar de combinaciones aleatorias de números y letras que no puedan ser adivinadas. Las fechas de cumpleaños, nombres de los padres, etc. deben evitarse, ya que pueden ser conocidas por muchos. El sistema debe obligar al cambio de nombres de usuario y contraseñas de manera regular. Todas las sesiones a las que se ingrese deben terminar automáticamente después de períodos cortos de inactividad, o requerir automáticamente que el usuario digite de nuevo su contraseña para reingresar. Los derechos de acceso de los empleados deben someterse con regularidad a una auditoría y las cuentas informáticas de quienes ya no trabajen para la AEDV deben cancelarse de inmediato. El sistema debe evitar el acceso fuera de horas normales de trabajo sin necesidad de la cancelación por parte del supervisor.

El equipo debe contar con un mecanismo de monitoreo y registro de auditoría que indique quién ha accedido al sistema y qué información se ha consultado. Es importante mantener los registros informáticos de ingreso y uso durante un tiempo razonable. Estos registros deben ser revisados por personal gerencial para identificar irregularidades en el acceso a las computadoras y cualquier acceso indebido debe estar sujeto a sanciones específicas. Esto resulta incluso más importante en el caso de los archivos clasificados como "VIP" o similar. La organización debe informar y recordar regularmente al personal sus responsabilidades en materia de informática y ofrecer capacitación. En caso de algún incidente de seguridad informática, es necesario llevar a cabo investigaciones e imponer sanciones si se determina que ha habido alguna conducta indebida o negligencia.

8.3.2 Uso de Internet y el correo electrónico

El acceso a Internet debe denegarse al personal y a los contratistas desde cualquier computadora o terminal utilizada en el proceso de emisión de documentos de viaje. Estos equipos deben estar física y tecnológicamente segregados: ya sea que se usen para el procesamiento de solicitudes de documentos de viaje, para envío y recepción de correos electrónicos internos, o para el acceso a Internet.

Se requiere contar con un programa para monitorear en forma aleatoria pero regular los mensajes de correo electrónico y el acceso a las aplicaciones de Internet por parte de todos los empleados y contratistas, a fin de detectar cosas o comunicaciones que puedan resultar de interés. Este proceso debe estar muy bien protegido mediante estrictas políticas y prácticas internas, de forma

tal que la información personal inocua obtenida a partir del monitoreo no sea revelada por ninguna razón. Toda la información resultante de este monitoreo que no sea de interés con fines de seguridad debe purgarse regularmente de los registros.

8.4 Personal de informática

El personal de informática debe tener derechos de acceso especial para ingresar a las instalaciones de informática como salas de cómputo, bases de datos y redes físicas, instalaciones de comunicación y sitios de respaldo. Estos privilegios de acceso deben involucrar identificaciones bifactoriales y requerir siempre dos o más individuos autorizados.

Es recomendable no asignar a una sola persona todas las responsabilidades relacionadas con un sistema informático, ya que ello dejaría al sistema vulnerable a abusos no detectados. Así, las responsabilidades deben estar segregadas y claramente definidas. La infraestructura informática debe estar instalada de forma tal que ningún individuo, independientemente de su nivel de antigüedad o rango en la organización, tenga jamás derecho de invalidar o anular las políticas y prácticas de seguridad, tomar decisiones arbitrarias, tomar respaldos de las bases de datos y otros archivos de información en forma arbitraria, o de ninguna forma comprometer el sistema de emisión y su información confidencial.

Las políticas de seguridad deben recordarse con frecuencia al personal de informática. Las revisiones y auditorías deben llevarse a cabo de manera regular y se requerirá imponer sanciones si se determina que algún funcionario(a) ha incurrido en conductas indebidas o negligencia.

9 Protección y promoción de la integridad del personal y de la autoridad emisora

9.1 Resumen

Para prestar sus servicios a la población, la AEDV depende y se encuentra vulnerable ante las acciones, la precisión en el trabajo y las decisiones de su personal. Por lo tanto, contar con personal confiable, capaz y seguro desde el punto de vista operativo es algo que resulta de vital importancia. La autenticidad de los documentos de viaje depende de la integridad de quienes los expidan, por lo que es necesario contar con un programa efectivo de seguridad del personal para garantizar que el proceso de emisión se lleve a cabo con total integridad.

La moral del personal, la organización del trabajo y los controles internos inciden de forma muy significativa en la prevención y detección de fraudes internos. Si existen sospechas o si se detecta algún fraude, es necesario que existan los mecanismos para proceder con las investigaciones internas y la imposición posible de posibles sanciones.

Una referencia útil en este sentido es el documento de la Comisión para la Corrupción y el Crimen de Australia Occidental titulado "Misconduct Resistance Integration Guide" (Guía de integración de la resistencia a la conducta indebida", disponible en la dirección: http://www.ccc.wa.gov.au/pdfs/CCC-MR-GUIDE.pdf.

9.2 Permisos de seguridad y sesiones informativas sobre seguridad

9.2.1 Investigaciones de antecedentes y de confiabilidad

La AEDV debe garantizar la confiabilidad de quienes tengan acceso a las instalaciones de emisión de pasaportes. Esto comienza incluso antes de que el personal sea contratado por la organización, cuando se verifica que la persona que esté siendo considerada para el puesto sea confiable y no fácilmente corruptible. Antes de ofrecerle un puesto, resulta importante realizar verificaciones de antecedentes y de confiabilidad, verificaciones a las que también ha de someterse a los contratistas.

La profundidad de la investigación debe estar relacionada con el cargo, responsabilidades, acceso y nivel de toma de decisiones que el funcionario(a) vaya a tener. A todos los cargos deberán asignárseles clasificaciones de seguridad que reconozcan lo delicado del cargo y el empleado que ocupe esa posición debe haber obtenido con éxito una autorización de seguridad para acceder a ese nivel.

Las verificaciones deben hacerse en colaboración con los organismos encargados de la aplicación de leyes, autoridades policiales o de seguridad nacional. Para los cargos que se encuentren dentro de las clasificaciones superiores de seguridad, por ejemplo los que desempeñen funciones gerenciales y los que involucren la toma de decisiones sobre la titularidad de un solicitante a un documento de viaje, las investigaciones han de ser más minuciosas y podrían incluir a los familiares y amistades, además de entrevistas a empleadores anteriores, así como una revisión del historial financiero, a fin de minimizar el riesgo de vulnerabilidades financieras. Es recomendable que las funcionarias y funcionarios a cargo de verificar la titularidad de los solicitantes sean ciudadanos del propio país.

La cultura y las tradiciones del individuo deben tenerse siempre en cuenta para asegurarse de que éstas no invaliden o limiten la probidad con la que se realizan las investigaciones de antecedentes y de confiabilidad, ni la contratación de ningún individuo.

9.2.2 Controles regulares de seguridad y vigilancia constante

Es posible que los empleados que incurran en deudas inmanejables sean vulnerables al soborno o la corrupción. La avaricia es sencillamente un elemento de motivación para cometer fraudes, de forma que las señales evidentes de que una persona viva más allá de sus posibilidades económicas deben tomarse en serio. Quienes se desempeñen en puestos gerenciales deben permanecer vigilantes una vez que se otorgue una autorización de seguridad y actuar a partir de cualquier información nueva que pueda poner en duda la confiabilidad o lealtad de un individuo. Los controles de seguridad deben practicarse a los empleados de manera regular de acuerdo a un cronograma recomendado durante el período de contratación. Si bien no existe un mecanismo definido para evaluar las probabilidades de que un empleado incurra en la ilegalidad, las revisiones periódicas de antecedentes pueden poner en evidencia algunos riesgos de seguridad.

9.2.3 Riesgos de oportunidad

Otra amenaza que amerita consideración es que los empleados sin antecedentes penales conocidos ni otros motivos para suscitar sospechas puedan obtener fácilmente autorizaciones de seguridad, aunque esto no garantiza que continúen siendo confiables. Un empleado puede verse sujeto a diversas presiones externas que lo lleven a incurrir en el fraude y por lo tanto debe tenerse especial atención de limitar los riesgos de oportunidad y garantizar la confiabilidad y lealtad continuas del personal. Se requiere delimitar las áreas seguras e imponer controles internos para limitar la autoridad de los empleados, tanto física como electrónicamente, a fin de desalentar y develar los actos ilegales. Esto también se aplica a cualquier organización asociada en la producción y emisión de documentos de viaje y de identidad. Vale la pena anotar que en sí misma una autorización de seguridad no confiere acceso a información o áreas seguras. Ni siquiera quienes cuenten con la autorización respectiva deben tener acceso a un área o a los datos a menos que sus obligaciones así lo requieran. Restringir la cantidad de personal que tenga acceso autorizado a las áreas seguras reducirá los riesgos de oportunidad.

9.2.4 Personal temporal

Muchas AEDV contratan personal temporal durante los períodos de máxima demanda, algo que puede representar una amenaza significativa a la seguridad si estas personas no pasan por la investigación de antecedentes respectiva debido a las limitaciones de tiempo. Por lo tanto, resulta crucial que el personal temporal pase por las mismas verificaciones de antecedentes que el permanente. Es recomendable mantener un grupo de personas que ya hayan pasado por esta verificación para hacer frente a situaciones de exceso de trabajo o escasez de personal (Véase el Capítulo 1).

9.2.5 Conciencia de la seguridad y códigos de conducta

Una vez que un empleado(a) o contratista nuevo se presenta a trabajar para la autoridad emisora debe recibir instrucción verbal sobre seguridad y lineamientos escritos sobre los controles internos y políticas de seguridad de la autoridad emisora. Debe ser informado sobre los privilegios y prohibiciones en cuanto acceso que conlleva su nivel de autorización de seguridad. Desde su primer día de trabajo y mientras dure la relación laboral, la persona debe ser informada regularmente y recibir capacitación sobre seguridad para mantener actualizados sus conocimientos sobre el tema (Capítulo 1).

Al inicio de su relación laboral, es necesario introducir al personal a las normas organizativas de conducta, valores y lineamientos éticos, lineamientos que comunican las acciones y componentes que la organización considera aceptables o inaceptables. Además, tales lineamientos han de incluir cláusulas específicas sobre conflictos de intereses, prohibiendo la aceptación por parte del personal de dádivas o propinas a manos de vendedores y proveedores que hagan negocios o busquen hacer negocios con la autoridad emisora, así como la aceptación de regalos y propinas a manos de quienes soliciten un documento de viaje por el cumplimiento normal de sus funciones o en espera de favores especiales. Debe preverse el tiempo para que el funcionario(a) pueda leer estos lineamientos y plantear sus preguntas al respecto. La gerencia debe asegurarse de que estas directrices sean entendidas y solicitar un acuso de recibo y conocimiento.

9.3 Organización del trabajo

9.3.1 Segregación de las funciones

Las funciones laborales recomendadas deben establecerse de forma tal que un solo empleado o empleada no pueda llevar a cabo todas las funciones de verificación de la titularidad de los solicitantes y emisión. De esta forma, será necesario que varios empleados expidan un documento de viaje a favor de alguien que intente comprar u obtener un documento recurriendo a la subversión. Debido a que es más difícil organizar un complot para incurrir en un acto ilegal a que una persona lo haga sola, es mucho más probable que la AEDV develen conspiraciones que involucren a varios empleados a que descubra a quienes actúen en solitario.

9.3.2 Delegación aleatoria del trabajo

A fin de reducir las posibilidades de incurrir en actos ilegales al interior de la organización, es recomendable que los procedimientos de flujo de trabajo eviten que el público seleccione al funcionario o funcionaria con quien desean tratar. Por ejemplo, en los casos en que más de un empleado acepta las solicitudes de documentos de viaje del público, el flujo de solicitantes debe preverse de forma tal que todas las ventanillas reciban público de una sola fila dependiendo de quién esté libre para atender la siguiente solicitud (en lugar de que los y las solicitantes seleccionen a un empleado en particular haciendo una fila específica).

El mismo principio aplica a la verificación de titularidad de las solicitudes [desk entitlement]. Debe requerirse al personal que tome el siguiente lote de trabajo en forma secuencial, lo cual reduce las posibilidades de que éste tenga acceso o asuma solicitudes específicas. Por la misma razón, debe requerirse al personal que rote para desempeñarse en diversas funciones, por ejemplo atención al público, verificación de titularidad de solicitudes enviadas por correo [desk entitlement of mailed applications], digitación de datos, verificación de documentos madre, entre otros.

El personal y la gerencia no deben tramitar ni aprobar las solicitudes de familiares, amistades ni personas conocidas. Solamente para circunstancias excepcionales es importante que exista un método para acelerar el trámite de las solicitudes, por ejemplo en el caso de altas personalidades (“VIP” o similar). Este servicio excepcional debe documentarse con minuciosidad y realizarse bajo la supervisión de un alto funcionario(a) designado para ello, quien no podrá actuar solo al expedir tales documentos.

9.3.3 Transparencia del proceso

La transparencia es crucial en todos los pasos del proceso de emisión. Resulta esencial registrar todas las decisiones vitales tomadas durante el proceso de emisión, lo cual es aun más importante cuando hay atrasos significativos en la carga de trabajo. Debe tomarse nota adecuada en los expedientes de las solicitudes y bases de datos con respecto a la evidencia vista y/o las acciones emprendidas para justificar todas las decisiones adoptadas por el personal a cargo de verificar la titularidad de los solicitantes. Esto permitirá contar con las justificaciones escritas necesarias, de forma que las acciones tomadas puedan ser revisadas posteriormente durante las auditorías realizadas en forma aleatoria, o en caso de que haya alguna pregunta específica sobre por qué se tomó una decisión con respecto a una solicitud determinada. Contar con procedimientos claramente establecidos con respecto a estas anotaciones debe ser un componente de un programa de capacitación.

9.4 Ánimo del personal [Satisfacción con el trabajo]

Es recomendable prestar atención a los temas relacionados con la moral del personal. Un personal con la moral elevada se siente valorado por sus aportes, es más productivo y eficaz en su trabajo y tiene un sentido de lealtad hacia la organización. Por el contrario, un empleado(a) descontento puede tornarse vulnerable y estar en mayor riesgo de responder de forma positiva en caso de ser abordado para participar en algún acto ilegal.

El instrumento más eficaz para combatir la ilegalidad es desarrollar la autoestima y el orgullo entre los empleados y empleadas por los logros de la organización, ya que la satisfacción laboral es un factor fundamental para garantizar su lealtad. A continuación se mencionan algunos elementos que influyen en el ánimo y la satisfacción laboral:

- un contrato escrito;
- un salario regular (o garantizado);
- un salario justo;
- condiciones de trabajo razonables;
- un ambiente libre de conflictos;
- adecuada supervisión, gerencia y comunicaciones;
- participación en la toma de decisiones;
- oportunidades de capacitación y experiencia para calificar para puestos más altos;
- buenos permisos y otros beneficios;
- posibilidad de plantear formalmente quejas y que estas sean escuchadas y abordadas de manera justa.

Las anteriores son buenas prácticas gerenciales que serán de utilidad en cualquier organización, pero son aún más importantes en organizaciones cuyo mandato y trabajo pueda tener un impacto en la seguridad nacional e internacional. No está demás insistir en que el tiempo y los recursos económicos que involucra la capacitación del personal en los puestos de supervisión y gerenciales para desarrollar competencias de liderazgo y buenas prácticas gerenciales serán una inversión valiosa. Una gerencia hábil y experta estará en capacidad de mejorar la productividad y a la vez disuadir al personal de involucrarse en fraudes internos.

El clima organizativo debe reflejar que al empleador realmente le importa el personal y su trabajo. Los sistemas de reconocimiento a los empleados y empleadas desempeñan un papel importante en este sentido. Desde el simple hecho de garantizar que se le agradezca al personal por sus esfuerzos, el aprecio de la organización y del público, la entrega de reconocimientos, o el hecho de remunerar las horas libres, todo son recursos para retribuir y reconocer el rendimiento del personal.

Una buena práctica que permitirá a la alta gerencia medir el ánimo del personal y revelar áreas problemáticas consiste en realizar encuestas periódicas de satisfacción y analizar sus resultados.

Esto le da al personal la posibilidad de expresar de manera confidencial su grado de satisfacción con el trabajo y con las prácticas gerenciales de la organización.

9.5 Investigaciones internas y sanciones

9.5.1 Reporte de incidentes de seguridad

Es necesario recordar regularmente al personal sobre la importancia de mantenerse alerta y atento ante actos ilegales y fraudes internos a manos de sus colegas, por ejemplo el robo de documentos, artículos de consumo y dinero en efectivo y pedírsele que denuncien cualquier incidente o amenaza. También debe alentársele para que avise a la gerencia en caso de ser abordados por personas que deseen inducirlos al fraude.

La AEDV debe contar con una política documentada sobre la denuncia de incidentes de seguridad que requiera que todo incidente sea reportado, en especial si involucra conductas indebidas y negligencia. Esta política también debe esbozar las responsabilidades del personal y de la gerencia en cuanto al manejo de los informes. Los procedimientos relacionados con la denuncia de incidentes deben reflejar el requisito de que todo incidente quede documentado. Además, deben comprender instrucciones claras sobre cómo se manejarán tales reportes, incluyendo orientación sobre la agencia de investigación o unidad de la AEDV correspondiente, independiente de la de operaciones, a la cual han de ser remitidos. Dependiendo de la índole y gravedad del incidente, las investigaciones pueden ser de carácter administrativo o penal. Las denuncias deben ser confidenciales y el denunciante debe estar protegido de comentarios negativos independientemente de la índole de la violación o de la persona involucrada.

A través de la denuncia e investigación eficaz de incidentes de seguridad pueden determinarse las vulnerabilidades y reducirse el riesgo de que se concreten en el futuro.

9.5.2 Investigaciones

Debe quedar claro, mediante una legislación sólida al respecto, cuál es la entidad gubernamental responsable de investigar los fraudes en documentos de viaje. A menudo ocurre que tal responsabilidad está dividida, de forma que una entidad tiene a su cargo los fraudes externos y otra diferente maneja los casos internos. Independientemente de esto, es importante que el director o directora de la AEDV se reúna con frecuencia con la dirigencia de la entidad responsable de las investigaciones de fraude, tanto para mantenerse al tanto sobre los casos que se encuentren en proceso como para asegurarse de que la autoridad emisora ofrezca su plena cooperación.

Los hallazgos de las investigaciones de fraudes internos deben ser comunicados plenamente a la autoridad emisora, incluyendo la índole del fraude, cómo se cometió y las mejoras que podrían introducirse para evitar que casos así se repitan en el futuro. Esto es importante porque la AEDV debe extraer aprendizajes de todo caso de fraude interno y tomar rápidamente acciones correctivas para prevenir que se repita.

9.5.3 Sanciones

La autoridad emisora debe asegurarse de que existan leyes adecuadas para presentar cargos y llevar a juicio a los empleados sospechosos de fraude interno, y que las leyes prevean la imposición de penas significativas. Tales sanciones también deben imponerse en casos de incidentes de seguridad que involucren una conducta indebida o negligencia.

Lo normal es que las personas que como resultado de las investigaciones resulten responsables de cometer fraude interno sean despedidas sin derecho a beneficios. Esto aplica a incidentes menores y mayores. Al cometer un acto de fraude, no importa cuán insignificante sea, un funcionario o funcionaria muestra su voluntad de quebrantar las reglas. Si lo amerita el caso, debe ser llevado a juicio y aplicársele todo el peso de la ley, incluyendo su enjuiciamiento penal.

La autoridad emisora debe presionar por la imposición de penas significativas no solo por la pena que involucre el caso sino también –y aun más importante– como elemento disuasivo, como prueba ante otros empleados de que no se tolerará su participación en situaciones de fraude y que las penas son reales. Los resultados de cada caso (condena, despido o renuncia) deben darse a conocer de forma que quienas puedan haberse sentido traicionados por su antiguo colega sepan que esa persona fue debidamente sancionada.

10 Documentos de viaje perdidos o robados

10.1 Resumen

El uso indebido de documentos de viaje auténticos obtenidos en circunstancias ilícitas acarrea serios riesgos para la seguridad nacional que se requiere abordar. Ya sea que hayan sido alterados o dejados intactos y utilizados por un impostor, si no se detectan, estos documentos podrían permitirle a terroristas, criminales y migrantes irregulares viajar casi sin ser identificados.

Pese a sus mejores esfuerzos de seguridad, en todos los países se experimentan pérdidas y robo de documentos de viaje, ya sea individualmente o en cifras múltiples. Estos documentos de viaje pueden ser libretas en blanco o documentos completamente personalizados. El efecto neto es que existe potencialmente un número elevado de documentos de viaje perdidos, robados o cancelados que en la actualidad se encuentran en circulación que son utilizados por personas distintas a su titular auténtico. En algunos casos los documentos de viaje son reportados como robados o perdidos, pero continúan siendo utilizados por el titular legítimo tras encontrar el documento.

La adopción de medidas preventivas puede reducir el número de documentos robados y perdidos y, una vez que han sido reportados como tales, las medidas de mitigación posiblemente reduzca el riesgo de seguridad que éstos conlleven.

10.2 Medidas preventivas

Las medidas preventivas para limitar los casos de pérdida o robo de documentos incluyen: sensibilización del público para alentar a los titulares a que cuiden adecuadamente sus documentos de viaje; denunciar de inmediato la pérdida de un documento de viaje; y hacer una selección más rigurosa de los solicitantes con un historial de pérdida o robo de documentos.

10.2.1 Sensibilización del público

10.2.1..1 Resguardo del documento de viaje

La AEDV debe desarrollar y establecer una estrategia de comunicación para reducir la frecuencia de casos de robo, alentando a los titulares a que mantengan su pasaporte guardado en un lugar seguro en todo momento. Las campañas de sensibilización del público permiten educar a los titulares sobre cuestiones como cuán difícil y caro resulta obtener un pasaporte de reemplazo. La autoridad emisora debe asegurarse de que el público esté plenamente informado sobre sus responsabilidades con respecto al documento que porta y las posibles consecuencias de que éste sea robado o se pierda.

10.2.1..2 Denuncia de pasaportes robados o perdidos

Se debe recurrir a las estrategias de sensibilización de la ciudadanía para informar y alentar al público a que actúe en caso de que su documento sea robado o se pierda. El público debe reportar ante la AEDV o ante las autoridades encargadas de la aplicación de leyes de que su documento fue robado o se ha perdido tan pronto ello se descubra.

Es importante que el público cuente con medios sencillos para reportar los documentos robados o perdidos, por ejemplo líneas gratuitas, números de fax, páginas en Internet o personalmente, todos los cuales deben ser de fácil acceso. Asimismo, debe haber orientación fácilmente accesible para los ciudadanos(as) que pierdan su pasaporte en el exterior. Tal orientación también debe destacar que una vez que un documento es reportado como robado o perdido será cancelado, de forma que no podrá ser utilizado más para viajar, en cuyo caso se necesitará una nueva solicitud para reemplazar el documento. De ser posteriormente recuperado, el documento no podrá ser

revalidado, y debe ser presentado ante la autoridad emisora para su cancelación o destrucción física.

Cuando un pasaporte es reportado como perdido o robado, quien reporta la pérdida o robo debe llenar un informe completo y la autoridad emisora debe asegurarse de que se hagan suficientes preguntas personales para determinar si se trata del titular auténtico.

En algunos países es delito no reportar la pérdida o robo de un pasaporte tan pronto como la persona se dé cuenta de ello. También puede ser un delito el uso de un pasaporte que haya sido cancelado para viajar, incluso cuando se trate de su titular auténtico.

Ejemplos de herramientas para sensibilizar al público sobre la necesidad de reportar el robo o pérdida de los documentos de viaje

- EE.UU.: http://travel.state.gov/passport/lost/us/us_848.html
- Canadá: http://www.ppt.gc.ca/planification/203.aspx?lang=eng
- Australia: https://www.passports.gov.au/Web/LostStolenInfo.aspx
- Nueva Zelanda: http://www.passports.govt.nz/diawebsite.nsf/wpg_URL/Services-Passports-Lost-or-Stolen-Passports

10.2.2 Políticas más estrictas de renovación de pasaportes

La aplicación de políticas más estrictas para los solicitantes con un historial de pérdida o robo de documentos de viaje servirá de incentivo para que los titulares cuiden más sus documentos.
A continuación se mencionan algunas medidas para desalentar el robo y la pérdida de documentos de viaje:

- que la persona solicitante sea tratada como si solicitase su documento de viaje por primera vez (cuando el país cuente con un proceso simplificado de renovación);
- el requisito de presentarse en persona para hacer la solicitud de reemplazo;
- una entrevista personal;
- el cobro de un cargo más elevado por concepto del reemplazo;
- el endoso obligatorio identificando el documento como uno de reemplazo, lo cual tenderá a llamar la atención de los funcionarios de los puestos fronterizos y de migración;
- un tiempo obligatorio entre la solicitud y la emisión para que se realice una investigación;
- limitación de la validez de los documentos de viaje de reemplazo; y
- (si aplica por ley) la negativa a expedir otro documentos de viaje después, por ejemplo, de que se haya expedido un segundo documento o si existen evidencias de que un documento reportado como robado en realidad fue prestado o vendido.

Las solicitudes en reemplazo de pasaportes u otros documentos de viaje robados o perdidos representan una potencial vulnerabilidad y deben ser investigadas por fraude por parte del personal encargado de decidir/verificar la titularidad de los solicitantes. En el caso de pérdidas múltiples podría requerirse una entrevista personal con el solicitante y una investigación policial. Varios elementos pueden llevar a una persona a declarar falsamente un documento como robado o perdido para obtener uno de reemplazo:

- que se hayan impuesto al documento existente restricciones aduaneras o de cruce de fronteras;
- el(la) solicitante busca mantener su residencia temporal en contra de las regulaciones de un país obteniendo un pasaporte nuevo que no tenga sellos anteriores de ingreso;
- el(la) solicitante intenta burlar la ley de inmigración de otro país u otras leyes; o
- el documento de viaje contiene páginas de visas sospechosas.

10.3 Medidas de mitigación

Entre las medidas de mitigación para reducir los riesgos de seguridad que supongan los documentos robados o perdidos cabe mencionar la cancelación inmediata de documentos reportados como tales, su registro en una base de datos nacional, así como el intercambio de esta información con socios nacionales e internacionales.

10.3.1 Cancelación de documentos de viaje perdidos o robados

Una vez que un pasaporte u otro documento de viaje se reporta como perdido o robado, debe ser de inmediato cancelado o invalidado para viajar. Esto aplica tanto a las libretas en blanco como a los documentos personalizados (pasaportes regulares, diplomáticos, oficiales, especiales, temporales/de emergencia) y el titular deberá presentar una nueva solicitud para reemplazarlo.

En muchos casos, un titular legítimo reporta un documento como perdido o robado y posteriormente lo encuentra, en cuyo caso el documento debe continuar siendo inválido, no volver a circular, y ser presentado ante la AEDV para su cancelación o destrucción física. El uso de documentos de viaje reportados como perdidos o robados por el titular auténtico puede ocasionar al viajero considerables inconvenientes y gastos adicionales. Cabe la posibilidad de que no se le permita abordar un avión, que se le niegue el ingreso o que sea detenido al llegar a su destino.

10.3.2 Reporte de documentos robados o perdidos para inclusión en la base de datos del país

Un documento de viaje robado o perdido debe ser reportado de inmediato como inválido e incluirse en una base de datos de documentos de viaje robados o perdidos, al menos durante su período de validez. Es recomendable que cada gobierno mantenga una base de datos que pueda ser accedida como parte del proceso de cruce de fronteras. Los datos sobre documentos robados o perdidos deben actualizarse con regularidad, de preferencia todos los días. Debe prestarse especial atención a la precisión e integridad de los datos para evitar inconvenientes a los viajeros que hayan cumplido con su obligación de reportar un documento robado o perdido. Si se confirma que se ha cometido un error, la autoridad emisora ha de tomar todas las medidas necesarias para eliminar los datos correspondientes a ese documento de la base de datos.

El uso de números de serie para cada documento en blanco y personalizado facilita su cancelación al denunciarse su pérdida o robo. La reutilización del número de documento o de libreta a lo largo de la vida de un individuo hace más difícil su rastreo en caso de pérdida o robo e incrementa las probabilidades de que el titular tenga problemas en la frontera.

El intercambio de información sobre documentos de viaje perdidos o robados es una estrategia clave para mitigar los riesgos en lo que respecta a los controles fronterizos, la inmigración y el robo de identidad. Como tal, resulta importante que el personal de migración y de los cruces fronterizos en todos los puertos de ingreso que verifique todos los pasaportes nacionales (y otros documentos de viaje) corrobore en la base de datos si no han sido reportados como robados o perdidos. Es importante que esta información se encuentre disponible en tiempo real. La base de datos debe estar igualmente disponible para las autoridades encargadas de la aplicación de leyes a fin de detectar casos de robo de identidad, así como para las autoridades encargadas de la emisión de visas, con miras a prevenir que se expidan documentos robados o perdidos.

Las bases de datos nacionales de documentos robados o perdidos ofrecen información que puede ser analizada y utilizada para evaluar las amenazas relacionadas con los documentos de viaje nacionales y el proceso de emisión. Para utilizar la base de datos con este propósito, esta debe

incluir información detallada sobre la pérdida de documentos de viaje tanto a nivel individual como colectivo.

10.3.3 Intercambio de información a escala internacional

A través de su base de datos nacional, los países hoy en día tienen por lo general la posibilidad de identificar el uso de sus propios documentos de viaje robados y perdidos cuando estos son presentados en sus fronteras nacionales. Sin embargo, para determinar si un documento extranjero presentado en la frontera fue declarado como robado o perdido los países deben compartir esta información con sus socios internacionales. Además del intercambio de datos en el ámbito bilateral o regional, hay alianzas internacionales que facilitan el intercambio de datos sobre documentos de viaje robados y perdidos. Ejemplos de ello son la Base de Datos de Documentos de Viaje Robados y Perdidos de Interpol (SLTD), y el Sistema de Alerta de Movimientos Regionales de la Región APEC (RMAS por sus siglas en inglés).

El intercambio global de información sobre pasaportes robados y perdidos ofrece una mayor integridad y ayuda a identificar los robos ya sea en la frontera o en otras situaciones en las que los documentos de viaje son presentados como modo de identificación.

10.3.3..1 Base de datos de documentos de viaje robados y perdidos de Interpol

Interpol maneja la llamada Base de Datos de Documentos de Viaje Robados y Perdidos (SLTD, por sus siglas en inglés), la cual contiene información detallada sobre pasaportes, cédulas de identidad o similares, visas, etc. que hayan sido reportados como robados o perdidos, con información de todos los países alrededor del mundo. Ésta permite que el personal de primera línea de los puestos fronterizos y de migración revise en forma instantánea si un documento presentado por un viajero fue reportado como perdido o robado.

Todas las AEDV deben reportar los detalles relativos a los documentos de viaje robados o perdidos ante Interpol a la mayor brevedad posible, de preferencia dentro de las 24 horas siguientes a la recepción de los datos. Esto incluye las libretas de pasaportes en blanco y los documentos personalizados. Las bases de datos nacionales pueden apoyar con la transferencia de la información a la SLTD.

Una oficina central u autoridad claramente designada para ello de cada país debe tener a su cargo el reporte de estos datos ante Interpol, para garantizar que las autoridades encargadas de la aplicación de leyes sepan dónde reportar los datos sobre documentos robados o perdidos y garantizar que los datos sean regularmente transmitidos a Interpol. Los países deben asegurarse de que su Oficina Central Nacional (OCN) esté al tanto de los procedimientos de reporte, actualización y verificación de su información sobre documentos de viaje robados o perdidos ante Interpol.

La información a enviar a la SLTD debe incluir, entre otros, los siguientes aspectos:

a) número de documento registrado en la ZLM (o número de serie en las libretas en blanco)
b) tipo de documento, esto es, pasaporte u otro
c) código de la OACI de país emisor
d) si se trata de un documento ya expedido o de una libreta en blanco
e) si se trata de un documento robado o perdido
f) fecha y lugar de emisión
g) fecha y lugar del robo o pérdida.

Se debe tener cuidado de garantizar la calidad y precisión de los datos y que éstos se encuentren completos, particularmente el número de documento. Cualquier error a la hora de registrarlos puede tener consecuencias para los viajeros auténticos y puede generarle costos a la autoridad emisora, por ejemplo si el viajero procurase obtener una compensación y la autoridad emisora hubiese cometido un error. Si se confirma que existe un error, la autoridad emisora debe adoptar todos los procedimientos necesarios para eliminar el documento en cuestión de la base de datos.

Todos los países deben esforzarse por poner la SLTD a disposición del personal de primera línea de los puestos fronterizos y de inmigración para que éste verifique en tiempo real los documentos de toda persona que llegue a los puertos de entrada al país. La base de datos debe estar a disposición de las autoridades encargadas de la emisión de visas a fin de prevenir que éstas sean expedidas en documentos robados o perdidos, y también de las autoridades encargadas de la aplicación de leyes, de forma que éstas puedan detectar los casos de robo de identidad. Es recomendable que la autoridad emisora se mantenga en contacto con INTERPOL 24 horas al día los 7 días de la semana para confirmar el estado de los documentos reportados y resolver las búsquedas en la base de datos de Interpol en forma oportuna.

Para ayudar a los países a conectarse con facilidad, Interpol desarrolló dos soluciones integradas utilizando dos bases de datos de redes integradas, una fija y una móvil, conocidas como FIND y MIND respectivamente. Ambas soluciones pueden integrarse al sistema de verificación asistida por computadora de un país. Además, la base de datos MIND también puede ser utilizada en un país que no cuente con un sistema. El acceso a los datos internacionales y la integración a los sistemas existentes son dos de los principales beneficios de estas dos bases de datos.

⇒ Sitio web de Interpol sobre MIND y FIND: www.interpol.int/Public/FindAndMind/Default.asp

La iniciativa de Interpol SLTD cuenta con el aval de varios foros internacionales, entre ellos la OACI, el G8, la UE y la OSCE (Decisión Nº. 4/04 sobre la necesidad de informar sobre pasaportes robados o perdidos al servicio de búsqueda automatizada/base de datos de documentos de viaje robados o perdidos de Interpol) y la ONU (Resolución del Consejo de Seguridad 1617).

⇒ Documentos de orientación desarrollados por el Subgrupo de expertos en materia de inmigración G8 Roma-Lyon:
  - Procesamiento de viajeros que presenten documentos de viaje robados o perdidos
  - Buenas prácticas dictadas por el G8 en materia de control de calidad en el reporte de datos sobre documentos de viaje robados y perdidos

⇒ Decisión Nº 4/04 de la OSCE: www.osce.org/documents/mcs/2004/12/3907_en.pdf

⇒ Resolución 1617 del Consejo de Seguridad: http://daccessdds.un.org/doc/UNDOC/GEN/N05/446/60/PDF/N0544660.pdf?OpenElement

El Sistema de Alerta sobre Movimientos Regionales (RMAS, por sus siglas en inglés) es una iniciativa de la APEC que permite la validación positiva de los pasaportes. Dicho sistema permite a las economías participantes verificar el estado de los pasaportes en tiempo real en la fuente, y alerta a los organismos relevantes en caso de que se requieran acciones. Además de verificar si se trata de pasaportes perdidos, robados o inválidos, el RMAS está en posibilidad de determinar si un pasaporte es reconocido por la autoridad que lo expidió como válidamente emitido.

⇒ APEC RMAS: http://www.businessmobility.org/RMAL/RMAL.html

11 Emisión de documentos en el exterior

11.1 Resumen

Los documentos de viaje expedidos en el exterior suelen emitirse en cantidades mucho menores que los emitidos en el propio país, y a menudo se encuentran bajo la jurisdicción de una instancia gubernamental distinta que los expedidos en el propio país. A pesar de esto, es importante que la seguridad en el proceso de emisión sea equivalente en ambos casos, incluyendo las buenas prácticas que se han expuesto en los diversos capítulos de esta Guía. Las oficinas centrales deben supervisar el trabajo procesado en la misión respectiva para garantizar que estas buenas prácticas de seguridad se cumplan en todo momento.

Para garantizar la uniformidad y la seguridad en el proceso de verificación de la titularidad y de personalización de los documentos de viaje, algunos países repatrían una o ambas funciones a sus oficinas centrales. Desde luego, esto prolonga el tiempo requerido para expedir y enviar los documentos de viaje y puede influir en el número de documentos temporales y de emergencia que se expidan. En este capítulo se discuten los casos en los que las funciones de verificación de la titularidad y personalización se llevan a cabo en las misiones en el exterior.

11.2 Supervisión del trabajo

El personal localmente contratado algunas veces desempeña funciones de emisión en las representaciones diplomáticas, por lo que es importante que pase por una revisión exhaustiva de seguridad al mismo nivel que el personal de pasaportes en el país de origen. Sus actividades en el proceso de emisión deben ser monitoreadas al mismo nivel que las de los empleados nacionales. El personal destacado en el exterior debe recibir la misma capacitación que el personal en el país de origen, incluyendo información, capacitación y sensibilización sobre el tema de la seguridad. Las políticas, criterios de verificación de la titularidad, evidencia documental de ciudadanía e identidad, requisitos de solicitud, entre otros, deben ser prácticamente idénticos a los del país de origen.

Es importante que exista una comunicación constante entre las oficinas centrales y las misiones en el exterior, para garantizar que el personal de éstas últimas conozca y entienda las políticas y prácticas sobre la emisión de los documentos de viaje. Deben realizarse con regularidad auditorías, evaluaciones, inspecciones in situ y evaluaciones de control de calidad para garantizar que todas las misiones en el extranjero apliquen las políticas y prácticas. La buena comunicación entre el país y las representaciones diplomáticas, así como el contar con condiciones de trabajo adecuadas, contribuyen a crear un sentido de apropiación entre el personal localmente contratado, lo cual fomenta la lealtad hacia el país.

11.3 Verificación de la titularidad

Cuando el personal localmente contratado está a cargo de verificar la titularidad de los solicitantes, es necesario que un supervisor(a) que sea ciudadano(a) del país apruebe siempre el trabajo hecho con respecto a la solicitud, incluyendo la revisión documental, investigación de la huella social, verificación de los garantes y verificación de referencias. El personal consular debe dar la autorización final sobre cualquier decisión para corroborar la titularidad de quienes soliciten documentos de viaje.

Siempre que las posibilidades lo permitan, las representaciones diplomáticas que emiten documentos de viaje deben tener acceso en línea a las mismas bases de datos, autorizaciones, listas de observación y datos sobre restricciones de viajes que las oficinas nacionales. Cuando

exista duda sobre la integridad de la información y/o de los documentos proporcionados por la persona solicitante o sobre cómo interpretar las políticas de verificación de la titularidad, el caso debe ser remitido a las oficinas centrales. Los documentos de viaje expedidos por las representaciones diplomáticas deben incluirse en alguna base de datos nacional.

11.4 Personalización

En las libretas personalizadas en el exterior debe utilizarse la misma tecnología de impresión e inventario, incluyendo sus características de seguridad, que las libretas producidas en el país de origen.

Es necesario que el control sobre las libretas en blanco sea incluso más estricto en el exterior que en las instalaciones en territorio nacional. Las mismas buenas prácticas descritas en los capítulos 4 y 5 deben aplicarse a la emisión de documentos de viaje en el exterior. Las libretas en blanco deben mantenerse en un área segura dentro de la misión a la que tengan acceso solamente los funcionarios responsables de expedir los documentos. Si la personalización está a cargo de personal localmente contratado, un alto funcionario o funcionaria consular que sea ciudadano o ciudadana del país ha de supervisar siempre el trabajo y realizar un control de calidad. Al igual que en las oficinas centrales, el conteo de las libretas en blanco debe ser realizado por al menos dos funcionarios(as), incluyendo uno que sea ciudadano(a) del país, al inicio y al fin de cada día.

12 Actores clave nacionales e internacionales

12.1 Resumen

Los documentos expedidos por la AEDV son utilizados y verificados por varios actores clave en el ámbito nacional e internacional. Recíprocamente, para garantizar la seguridad de sus documentos y del proceso de emisión, la AEDV debe consultar y estar en contacto con varios actores en la esfera nacional, internacional y en el sector privado. En esta sección se identifican los socios y actores clave más importantes con los que la autoridad emisora debe mantener contacto y el tipo de información y datos que debe ser comunicado en forma bilateral.

12.2 Actores clave en el ámbito nacional

La autoridad emisora debe entablar alianzas activas con las autoridades nacionales que funjan como actores clave en la emisión y uso de documentos de viaje. A continuación se mencionan algunas, aunque la siguiente no es una lista exhaustiva:

- controles fronterizos
- inmigración
- aplicación de leyes o policía
- laboratorio forense de documentos
- otros organismos involucrados en la elaboración y mantenimiento de listas de observación y restricciones de viajes para efectos de verificación de la titularidad de quienes soliciten documentos de viaje
- estadísticas vitales, esto es, de entidades emisoras de documentos madre y documentación de apoyo
- cualquier otro socio involucrado en el proceso de emisión de documentos de viaje, por ejemplo su emisión en el exterior; emisión de pasaportes diplomáticos, especiales u oficiales; organizaciones que reciban las solicitudes.

Todos estos organismos pueden contribuir al desarrollo de las características físicas del documento de viaje; influir en las decisiones sobre la titularidad de las personas solicitantes; incidir en la seguridad del proceso de emisión; o bien pueden verse afectados por los cambios o decisiones que tome la autoridad emisora relacionadas con el documento de viaje y su proceso de emisión.

12.2.1 Control fronterizo e inmigración

Las autoridades de control fronterizo e inmigración son los socios más cercanos de la AEDV. Estas determinan quién puede ingresar al territorio nacional y quién no, con base en gran parte en el análisis del documento de viaje que porte el viajero. El personal de migración y de control fronterizo sabe cuáles características de seguridad son las más efectivas y más fácilmente verificables en las inspecciones primarias y secundarias.

En su calidad de usuarios de primera línea, las autoridades de migración y de control fronterizo también son testigo y recopilan datos sobre incidencias y tendencias en materia de fraude de documentos. Las AEDV deben mantener una comunicación regular con estas autoridades y desarrollar alianzas para intercambiar información sobre fraudes, así como informar sobre el desarrollo, diseño e incorporación de las características de seguridad a los documentos de viaje. La autoridad emisora debe tomar todas las medidas necesarias para garantizar que cualquier

característica técnica o física que incorpore a los documentos de viaje sea desarrollada en consulta y teniendo en cuenta los requisitos de las autoridades migratorias y de control fronterizo.

Cuando se incorporan nuevas características de seguridad o especificaciones al pasaporte o se adoptan nuevas versiones, los funcionarios de migración y de los puestos fronterizos tanto en el ámbito nacional como en el internacional deben ser informados dentro de un plazo razonable. La cooperación y la comunicación con estas autoridades es también esencial para garantizar que la introducción de versiones nuevas o actualizadas de los documentos de viaje, por ejemplo la introducción del pasaporte-e, sea interfuncional con la infraestructura y sistemas vigentes y futuros, como es el caso de los lectores, el control fronterizo automatizado y el software.

Las autoridades de control fronterizo y de migración pueden contribuir a las listas de observación utilizadas en el proceso de verificación de la titularidad de las solicitudes de documentos de viaje. La AEDV comparte de manera recíproca datos sobre pasaportes reportados como perdidos, robados o cancelados con estas autoridades. También es importante que existan mecanismos de comunicación bilateral para confirmar la validez de los datos proporcionados por ambos organismos.

12.2.2 Autoridades encargadas de la aplicación de leyes, autoridades policiales y laboratorios de documentos forenses

Los organismos encargados de la aplicación de leyes, las autoridades policiales y los laboratorios de documentos forenses son muy concientes de las amenazas a la seguridad de los documentos de viaje y las tendencias en materia de fraudes. Investigan casos de fraude con documentos de viaje y técnicas de alteración. Esta información tiene un valor incalculable para la AEDV para el desarrollo, diseño e incorporación de características de seguridad a los documentos de viaje, así como para la incorporación de mecanismos de seguridad y controles internos al proceso de emisión.

Las autoridades encargadas de la aplicación de leyes y las policiales también aportan datos a las listas de observación y de restricciones que se utilizan durante el proceso para corroborar la titularidad de los solicitantes de documentos de viaje.

12.2.3 Estadísticas vitales

La decisión sobre la titularidad del solicitante requiere corroborar su identidad y ciudadanía mediante los documentos madre y la documentación de apoyo, a menudo expedida por distintos organismos gubernamentales. Es importante que exista una comunicación constante con estos organismos para obtener información sobre las diferentes versiones del documento que estén siendo expedidas, sus características de seguridad, además de información relacionada con los fraudes. Asimismo, es recomendable que exista un mecanismo para verificar regularmente la integridad de los documentos presentados por la persona solicitante. Como se indicó en el Capítulo 4, es recomendable que exista un acceso electrónico directo a los registros adecuados.

12.2.4 Otros

Autoridades que aportan datos a las listas de observación y de restricciones de viaje

Los datos que incluyen las diversas listas de observación y de restricciones de viaje utilizadas para las decisiones sobre la titularidad de las personas solicitantes varían en cada Estado. Las autoridades de control fronterizo, inmigración y aplicación de leyes deben aportar datos a estas listas, además de las autoridades judiciales, servicios correccionales, relaciones exteriores y la administración tributaria, entre otras.

Socios involucrados en el proceso de emisión

Es recomendable que todas las organizaciones involucradas en el proceso de emisión –incluyendo las encargadas de la emisión de documentos de viaje en el exterior– además de los organismos que aceptan solicitudes en representación de la AEDV, estén involucradas y tengan conocimiento sobre cualquier cambio en las políticas y procesos que introduzca la AEDV y que pueda tener algún impacto en la seguridad del proceso de emisión.

12.3 Socios internacionales

La autoridad emisora debe entablar asociaciones o alianzas activas con otras naciones, y participar en foros y grupos de trabajo internacionales, además de compartir información sobre normas, especificaciones, tendencias y fraudes en materia de documentos de viaje; compartir información relevante sobre documentos de viaje; y procurar asistencia para el desarrollo de capacidades de ser necesario. Entre otros, cabe mencionar los siguientes organismos:

- Organización de Aviación Civil Internacional (OACI)
- Interpol
- Foro de Cooperación Económica Asia-Pacífico (APEC)
- Organización Internacional para las Migraciones (OIM)
- Organización para la Seguridad y la Cooperación en Europa (OSCE)
- Organización de los Estados Americanos (OEA)
- Cualquier otro foro regional y/o internacional cuya labor se centre en los documentos de viaje, la seguridad fronteriza, las migraciones, etc.

12.3.1 Organización de Aviación Civil Internacional (OACI)

La OACI establece las normas o estándares y prácticas recomendadas con respecto a los pasaportes y otros documentos de viaje (Sección 3 del Anexo 9 del Convenio de Chicago). El Grupo Técnico Asesor sobre Documentos de Viaje de Lectura Mecánica (TAG/MRTD) elabora y adopta las especificaciones sobre documentos de viaje contempladas en le Documento 9303, además de publicar materiales de orientación e informes técnicos y documentos informativos para apoyar a los Estados en la implementación de sus especificaciones. Dos grupos de trabajo se conformaron bajo la rectoría del TAG/MRTD:

El Grupo de trabajo sobre nuevas tecnologías (NTWG)
En asocio con la Organización Internacional de Estandarización (ISO), este grupo de trabajo desarrolla estrategias, políticas y material de orientación relacionado con la manufactura, seguridad, prueba, emisión, implementación y uso interfuncional global de los DVLM y los pasaportes-e, tanto en formato impreso como electrónico.

Grupo de trabajo sobre Implementación y Fortalecimiento de Capacidades (ICBWG)
Este grupo de trabajo apoya a la Secretaría de la OACI en la realización de actividades de divulgación y fortalecimiento de capacidades para ayudar a los Estados Miembros de la OACI en la emisión y mejoramiento de la seguridad en sus procesos de emisión.

En caso de requerir fondos o conocimientos expertos relacionados con la emisión de documentos de identidad y de viaje, diríjase al Programa sobre DVLM de la Secretaría de la OACI

⇒ Programa sobre DVLM: http://www2.icao.int/en/MRTD/Pages/default.aspx

⇒ Para solicitar el Documento 9303:
http://www2.icao.int/en/MRTD/Pages/OrderICAOPublication.aspx

12.3.2 Intercambio internacional de datos e información

Como se mencionó en el Capítulo 10, es recomendable que la información sobre documentos de viaje reportados como perdidos o robados sea compartida con los socios internacionales, al permitir que los países identifiquen el uso o nivel de abuso de sus propios pasaportes perdidos y robados, además del uso y abuso de los documentos expedidos por otros países. La Base de Datos sobre Documentos Robados y Perdidos de Interpol (SLTD) permite que los funcionarios de primera línea verifiquen en forma instantánea si un documento de viaje es robado o perdido. Además de corroborar si se trata de documentos robados, perdidos o inválidos, el Sistema de Alerta de Movimientos Regionales (RMAS) del Foro de Cooperación Asia-Pacífico está en capacidad de determinar si un pasaporte es reconocido por su autoridad emisora como válidamente emitido.

Se han establecido varias alianzas bilaterales, regionales e internacionales en todo el mundo para facilitar y mejorar la cooperación y el intercambio de datos entre aliados, a fin de agilizar el cruce de fronteras entre Estados vecinos. A manera de ejemplo cabe mencionar el Área Shengen, MERCOSUR, ECOWAS y CARICOM.

12.3.3 Cooperación internacional y desarrollo de capacidades

Además de la OACI; hay varias entidades internacionales y regionales con programas de desarrollo de capacidades, conocimientos expertos, financiamiento y/o recursos disponibles para colaborar con los países que requieran ayuda en el campo de la emisión de documentos de viaje. La OIM, OEA y OSCE son ejemplos de organizaciones activas en este campo.

Organización Internacional para las Migraciones (OIM): cooperación técnica en materia de gestión migratoria y desarrollo de capacidades
La OIM es un organismo intergubernamental que agrupa a 122 miembros. Las actividades de su División de Cooperación Técnica sobre Migraciones (TCM) ayudan a los gobiernos a dotarse de las políticas, legislaciones, estructuras administrativas, sistemas operativos y la base de recursos humanos necesaria para abordar diversos problemas relacionados con la migración. La OIM ofrece servicios de asesoría, asistencia técnica y capacitación.

⇒ OIM-TCM: http://www.iom.int/jahia/Jahia/pid/749

⇒

Organización de los Estados Americanos (OEA) — Comité Interamericano contra el Terrorismo (CICTE)
El principal propósito del Comité Interamericano contra el Terrorismo (CICTE) consiste en promover y desarrollar la cooperación entre los Estados Miembros para prevenir, combatir y erradicar el terrorismo. El programa de Seguridad de Documentos y Prevención de Fraude tiene por objetivo mejorar la capacidad del personal encargado de la aplicación de leyes, aduanas y migración de los países objetivo, con miras a mejorar sus controles y la emisión de documentos de viaje y de identidad y su capacidad para detectar documentos fraudulentos, así como para prevenir su alteración y uso fraudulento.

⇒ OEA-CICTE: http://www.cicte.oas.org/Rev/En/

Organización para la Seguridad y la Cooperación en Europa (OSCE) — Unidad de Acción contra el Terrorismo (UAT)

Conformada en el año 2002, la Unidad de Acción contra el Terrorismo es el punto focal de la OSCE para coordinar y facilitar las iniciativas y los programas de desarrollo de capacidades de la Organización en la lucha contra el terrorismo. El programa de seguridad para documentos de viaje presta asistencia técnica y orientación en la implementación de compromisos antiterrorismo. La OSCE ha liderado numerosas actividades de desarrollo de capacidades durante los últimos años, incluyendo talleres sobre seguridad de documentos de viaje y manejo y emisión de documentos de viaje, además de capacitaciones sobre documentos alterados.

⇒ OSCE-UAT: http://www.osce.org/atu/

12.4 Socios del sector privado

Además de los socios nacionales e internacionales, tanto las AEDV como las compañías privadas obtienen beneficios de mantenerse en contacto e intercambiar información.

12.4.1 Aerolíneas

Debido a que los gobiernos demandan cada vez más de las aerolíneas, desde la verificación de la integridad de los documentos de viaje hasta el almacenamiento y comunicación de información sobre pasajeros, es una buena idea que la AEDV se mantenga en contacto con aerolíneas y asociaciones, por ejemplo la IATA, para compartir información sobre las características y elementos de seguridad de los documentos de viaje.

12.4.2 Compañías privadas

La Organización Internacional de Estandarización (ISO) y las empresas privadas que se encuentran evolucionando en el campo de los documentos de viaje, lectores, chips, identificadores biométricos, impresoras, entre otros, son fuentes excelentes de información sobre nuevas tecnologías disponibles, sistemas y procesos. Realizar solicitudes de información (SDI) es una buena práctica para mantenerse al tanto de las más recientes investigaciones e innovaciones.

Documentación de referencia

1. *Security Standards for Machine Readable Travel Documents* — Informative Annex of Document 9303
2. *Minimum Security Standards for the handling of MRTDs and other passports* — Informative Annex to Section III of Document 9303
3. *ICAO-New Technologies Working Group (IEC JTC1 SC17 WG3/TF1), "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation"*, Draft 1.4, 7 March 2007, TAG-MRTD/17-WP/16
4. *Recommended Standards for Secure Proof of Status and Nationality Documents to Facilitate Cross-Border Travel, Security and Prosperity Partnership Deliverable* 1.1.3
5. *A Guide to Biometric Technology in Machine Readable Travel Documents*, APEC Business Mobility Group
6. *G8 Best practice for the processing of travellers who present lost of stolen travel documents*
7. *G8 Best practices on quality control of reporting on lost and stolen travel document data*

Abreviaturas

ABC	Automated Border Control system
AEDV	Autoridad Emisora de Documentos de Viaje
APEC	Foro de Cooperación Económica Asia-Pacífico
CAB	Control de acceso básico
DCP	Directorio de claves públicas
DVLM	Documento de Viaje de Lectura Mecánica
DS	Document Signer
CAE	Control de acceso extendido
FIND	Base de Datos de Red Fija de Interpol (Fixed Interpol Network Database)
ICBWG	Grupo de Trabajo sobre Implementación y Fortalecimiento de Capacidades
ICP	Infraestructura de clave pública
ISO	Organización Internacional de Estandarización
MIND	Base de Datos de Red Móvil de Interpol (Mobile Interpol Network Database)
NTWG	Grupo de trabajo en nuevas tecnologías
OACI	Organización de Aviación Civil Internacional
OCN	Oficina Central Nacional de Interpol
OEA	Organización de los Estados Americanos
OIM	Organización Internacional para las Migraciones
OSCE	Organización para la Seguridad y la Cooperación en Europa
PLM	Pasaporte de lectura mecánica
PLM-e (o Pasaporte-e)	Pasaporte de lectura mecánica electrónico
RMAS	Sistema de Alerta de Movimientos Regionales de la Región APEC
SDI	Solicitud de información
SLTD	Base de Datos de Documentos de Viaje Robados y Perdidos
TAG	Grupo Técnico Asesor
UE	Unión Europea
ZLM	Zona de lectura mecánica