DOCUMENTOS: MANUAL PARA DESARROLLADORES

DIANA OMBELLI
Y
FONS KNOPJES

OIM Organización Internacional para las Migraciones

Diana Ombelli
y Fons Knopjes

DOCUMENTOS: MANUAL PARA DESARROLLADORES

OIM Organización Internacional para las Migraciones

Las opiniones expresadas en el presente informe son las de los autores y no reflejan necesariamente las opiniones de la Organización Internacional para las Migraciones (OIM). Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican juicio alguno por parte de la OIM sobre la condición jurídica de ningún país, territorio, ciudad o zona citados, o de sus autoridades, ni respecto del trazado de sus fronteras o límites.

La OIM está consagrada al principio de que la migración en condiciones humanas y de forma ordenada beneficia a los migrantes y a la sociedad. Como organización intergubernamental, la OIM actúa con sus socios en la comunidad internacional, con el fin de ayudar a responder a los retos funcionales de la migración; contribuir a una mayor comprensión de los problemas ligados a la migración; promover el desarrollo social y económico mediante la migración y defender la dignidad humana y el bienestar de los migrantes.

Título:	Documentos: Manual para Desarrolladores
Redactores:	Diana Ombelli y Fons Knopjes
Editor:	Organización Internacional para las Migraciones 17, route des Morillons 1211 Ginebra 19 Suiza Tel: + 41 22 717 91 11 Fax: + 41 22 798 61 50 Correo electrónico: hq@iom.int Internet: http://www.iom.int
Diseño de la portada:	Jaap Drupsteen
Primera edición:	abril de 2008 (en inglés)

ISBN 978-92-9068-609-5

14_10

ÍNDICE

■ Ångström, Nils

Nils Ångström (1942) es licenciado en ciencias (BSc) y examinador forense de documentos. Trabaja con el Laboratorio Nacional Sueco de Ciencia Forense de Linköping (Suecia) desde 1972.
Datos de contacto: nils.ångström@skl.polisen.se

■ Baggeroer, Chuck

Chuck Baggeroer (1944), cuenta con más de 20 años de experiencia en el campo de la personalización de documentos financieros y de identidad. Antes de jubilarse trabajó como director de tecnologías de seguridad y como enlace con la industria en *Datacard Group*. Además, es miembro de distintos comités industriales, tales como el grupo de trabajo ISO/IEC JTC1/SC17/WG3, el grupo sobre documentos de viaje internacionales ISO/IEC JTC1/SC17/WG10, el comité sobre permisos internacionales de conducir y la *International Association of Financial Crimes Investigators*.
También es asesor del Grupo de Trabajo sobre nuevas tecnologías de la Organización de Aviación Civil Internacional (OACI). Ha impartido cursos de formación sobre examen documental a departamentos de investigación y forense de numerosos cuerpos policiales nacionales.
Chuck Baggeroer es licenciado en ciencias y posee una maestría en ingeniería mecánica por la Universidad de Purdue y una maestría en administración de empresas por la Universidad de Minnesota.
Datos de contacto: cbaggeroer@comcast.net

■ Baltazar, Isabel

Isabel Baltazar (1967) dirige la unidad de fraudes y el departamento de identificación de los servicios de inmigración portugueses en Lisboa (Portugal) desde 1993. Imparte cursos de formación sobre fraude documental y documentos de seguridad a los cuerpos de policía, el ejército, los servicios consulares y otras entidades similares en todo el mundo. Ha participado en el desarrollo de nuevos documentos de viaje, en particular el permiso de residencia para extranjeros y los pasaportes portugueses, y ha sido asesora sobre el uso de los equipos técnicos para la detección de documentos fraudulentos. Además de representar a Portugal en las reuniones de la UE sobre desarrollo de documentos de viaje y prevención de fraudes, también es miembro de la delegación de Portugal del Grupo consultivo técnico de la OACI. Estudió en el Instituto Superior de ciencias sociales y políticas de la Universidad Técnica de Lisboa, donde se licenció en relaciones internacionales en 1989.
Datos de contacto: isabelb@sef.pt

■ van Blankestein, Jan Heim

Jan Heim van Blankenstein (1963) posee una maestría en ciencias (M.Sc.) y es consultor principal en arquitectura de las tecnologías de la información y la comunicación, y seguridad de la información en *Montelbaan Internet* & ICT BV en los Países Bajos. Se graduó en biofísica en la Universidad de Utrecht en 1988, donde concentró su actividad en modelos informáticos y teoría de la información. Tras licenciarse fue becario de investigación en el centro de cardiología en la Universidad Erasmo de Rotterdam. En 1995 empezó a trabajar en el campo de las tecnologías de la información y la comunicación como consultor de tecnología de directorios y mensajería segura, y en 2000 puso en marcha Montelbaan Internet & ICT BV. En la actualidad concentra su actividad en aspectos técnicos y organizativos de la seguridad de la información, en general, y la biometría y la infraestructura de clave pública, en particular. Como director de proyectos de tecnologías de la información y la comunicación participó en el desarrollo e introducción del nuevo documento de viaje holandés en 2001.
Datos de contacto: jan.heim.van.blankenstein@montelbaan.nl

■ Broekhaar, Sjef

Sjef Broekhaar (1955), es en la actualidad oficial de capacitación y especialista técnico para la Organización Internacional para las Migraciones (OIM) (2008). Anteriormente ocupó el cargo de director de investigación y desarrollo de la oficina de documentos de viaje y bases de datos de antecedentes personales del Ministerio del Interior y Relaciones del Reino (2002). Es un experto en el campo de la investigación documental. Con anterioridad, fue director de programas en el programa de documentos y delitos de pago de la división de inteligencia criminal nacional de los cuerpos nacionales de policía (1998). Fue iniciador y codesarrollador de la base de datos electrónica para la solicitud de documentos de viaje internacionales: Edison TD (1991). También ha participado en cursos nacionales e internacionales sobre investigación documental como conferenciante invitado (1983). Es autor de varias publicaciones.
Datos de contacto: sbroekhaar@iom.int

■ Buursma, Cor

Antes de jubilarse, Cor Buursma (1940) ocupó una serie de cargos en Joh. *Enschede and Sdu Identification* (anteriormente, Enschede/Sdu). Tiene más de 40 años de experiencia en el desarrollo de documentos seguros, en particular en el campo de la producción y personalización. Fue director de varios departamentos, tales como la sección de preprensa e impresión, la sala de composición, el departamento de personalización de tarjetas de identidad y el departamento de desarrollo de proyectos y de producto.
Puso en marcha varios centros de producción, entre éstos una fábrica para la producción de tarjetas bancarias y un departamento de personalización de tarjetas bancarias y de identidad. En *Sdu Identification* fue responsable de la nueva generación de documentos de viaje holandeses, que incluyó el diseño y la producción de la nueva serie y la puesta en marcha de un nuevo proceso para la personalización de dichos documentos.
Datos de contacto: cor.buursma@wanadoo.nl

■ Cardell, Birgit

Birgit Cardell (1953) es examinadora forense de documentos en el Laboratorio Nacional Sueco de Ciencia Forense de Linköping (Suecia), al que se incorporó en 1986. En la actualidad es jefa del grupo de documentos.
Datos de contacto: birgit.cardell@skl.polisen.se

■ Chatwin, Charles

Charles Chatwin (1939) es consultor de impresión de seguridad e identificación. Posee dos licenciaturas en química por la Universidad de Oxford. Tras un breve periodo en la industria química, donde trabajó en el campo del PVC, dedicó 38 años de su actividad profesional a las artes gráficas, en actividades que van desde la prensa nacional a los carteles. Consagró 27 años de su carrera a los documentos seguros, primero con *McCorquodale*, después con Bradbury Wilkinson y por último en *De La Rue*, donde fue director técnico de la división de impresión de seguridad y posteriormente de la división de sistemas de tarjetas. Fue responsable del desarrollo de la tarjeta *Fortas de De La Rue*. Fue miembro fundador del Grupo de Trabajo 3 de la ISO (WG3, por sus siglas en inglés) y dirige su Equipo de Tareas 2; también es miembro del Grupo de Trabajo 10.
Datos de contacto: charles.chatwin@btinternet.com

■ Dell, Mike

Mike Dell (1969) posee una maestría en ciencias (MSc) y es consultor principal de seguridad de la información en *Montelbaan Internet & ICT BV* en los Países Bajos. Estudió en la facultad de matemáticas y computación en la Universidad de Utrecht, donde se graduó con una tesis sobre criptosistemas de depósito de claves (o key-escrow) en 1995. Empezó su carrera en las tecnologías de la información como especialista técnico en BSO/Origin. Posteriormente, BSO/Origin pasó a formar parte de Atos Origin, donde se incorporó al grupo de soluciones de infraestructura adaptativa como consultor de seguridad, convirtiéndose en presidente de desarrollo de servicios de seguridad. En noviembre de 2001 se incorporó a Montelbaan Internet & IT BV. Ha trabajado en varios proyectos en el campo de la infraestructura técnica, la integración de sistemas, los sistemas expertos, las telecomunicaciones, el comercio electrónico y, lo más importante, la seguridad de la información y la infraestructura de clave pública. Como consultor en tecnologías de la información, participó, en 2001, en el desarrollo y la introducción del nuevo y avanzado documento de viaje holandés.
Datos de contacto: mike.dell@montelbaan.nl

■ Felix, Idius

Idius Felix (1964) posee una maestría en ciencias (MSc) y es consultor de gestión de la división de consultoría y gestión de proyectos de *Atos Origin* en los Países bajos. Se graduó en administraciones públicas en la Universidad de Twente en Enschedé (Países Bajos), en la especialidad de problemas y cambios estructurales. Es un experto en resolver problemas estructurales y responder a los retos y las nuevas oportunidades derivados de los avances en las tecnologías de la información, y a sus efectos en las organizaciones. Ha participado en varios proyectos importantes en el campo de las tecnologías de la información emprendidos por el gobierno central de los Países Bajos,

tales como el desarrollo y la implantación de bases de datos municipales de antecedentes personales, la introducción y el manejo de la seguridad de la información en los organismos públicos, y el desarrollo e implantación del nuevo y avanzado documento de viaje holandés en 2001. Como consultor en temas de gestión, da apoyo a distintas organizaciones en procesos de estructuración y cambios orgánicos, y en materia de tecnologías de la información y seguridad de la información.
Datos de contacto: idius.felix@atosorigin.com

■ Graber, Daniele

Daniele Graber (1966) trabaja como asesor jurídico en la Asociación suiza de ingenieros y arquitectos (SIA) en Zurich. En la actualidad está preparando su tesis doctoral en la Universidad de Friburgo: "Contratación pública de servicios: derecho suizo, comunitario e internacional".
Tras un periodo de aprendizaje como delineante de maquinaria (1982-1986), estudió en *Hochschule für Technik NTB* en Buchs (Suiza), donde obtuvo el título de ingeniero técnico en micromecánica (1986-1989). Posteriormente, se especializó en óptica aplicada y estadística (1989-1991), y trabajó durante dos años en el Instituto IMAC del Instituto Federal suizo de tecnología en Lausana. Entre 1994 y 1999 estudió derecho en la Universidad de Friburgo, donde se graduó en 1999.
Datos de contacto: graber@sia.ch

■ Knopjes, Fons

Fons Knopjes (1953) es director de *IDManagement Centre*, una organización internacional independiente especializada en el campo de la cadena de la identidad y la capacitación en esa área. Fons fue director de investigación y desarrollo de documentos de viaje del Ministerio de Interior y Relaciones del Reino, y trabajó como jefe de proyecto en el desarrollo, producción e individualización de los documentos de viaje holandeses. También fue asesor en la creación de un gran número de documentos (electrónicos), de identidad y otros documentos de valor, introducidos en 2001. Obtuvo gran parte de su experiencia en la oficina de información nacional de la policía nacional holandesa, y durante más de 10 años fue representante de los Países Bajos en el Grupo de Trabajo sobre documentos falsos de la Unión Europea. Fue miembro del Grupo de trabajo de nuevas tecnologías (NTWG) y del Grupo de Trabajo sobre educación y promoción (EPWG) de la Organización de Aviación Civil Internacional (OACI). En la actualidad es miembro del Equipo de Tareas 3 (TF3, por sus siglas en inglés) del Grupo de Trabajo 3 de la ISO (ISO WG3/TF3) y del Grupo básico de expertos de las Naciones Unidas sobre delitos relacionados con la identidad. También es miembro del Consejo del Foro holandés sobre biometría y ha confeccionado e impartido varios cursos de formación nacionales e internacionales en materia de investigación documental. Cuenta con numerosas publicaciones en materia de documentos de identidad, falsificación, etc.
Datos de contacto: fons.knopjes@idmanagement-centre.com

■ Lakeman, Piet

Piet Lakeman (1958) es un alto directivo del departamento de gestión de fraudes de Visa Europa en Londres (Reino Unido). Anteriormente fue jefe de proyecto del Sistema de clasificación universal de tarjetas de pago falsificadas, una asociación público-privada entre la Secretaría General de la INTERPOL en Lyon (Francia) y el sector de las tarjetas de crédito. Anteriormente, trabajó en la oficina de información nacional de la policía holandesa. También fue consultor para el "grupo de proyecto sobre prevención de fraudes" de la Comisión Europea, así como para el grupo de proyecto sobre fraudes con tarjetas de pago del G8. Como consultor ha participado en la elaboración de documentos nacionales e internacionales. Es autor de numerosas publicaciones sobre fraudes con tarjetas.

Datos de contacto: lakemanp@visa.com

■ Meuwly, Didier

Didier Meuwly (1968) se graduó en la Escuela de ciencias forenses (IPS) de la Universidad de Lausana en 1993 y obtuvo su doctorado en la misma institución en el año 2000.

Desde 2004 trabaja en el Instituto Forense de los Países Bajos, que forma parte del Ministerio de Justicia holandés. En la actualidad es científico principal, encargado del proyecto de investigación nacional sobre individualización forense basada en estadísticas de huellas dactilares y contribuye al programa de investigación y formación del Instituto Forense de los Países Bajos. Entre 2002 y 2004 fue científico forense principal de los servicios de ciencias forenses, órgano ejecutivo del Ministerio de Interior británico. Entre 1999 y 2002 fue responsable del grupo de investigación biométrica de la IPS.

También es miembro fundador de los grupos de trabajo de la Red Europea de Institutos de Ciencias Forenses (ENFSI, por sus siglas en inglés), el Grupo de trabajo de análisis forense auditivo y del habla (FSAAWG, por sus siglas en inglés) en 1997 y el Grupo de trabajo europeo sobre huellas dactilares (EFPWG) en 2000.

Datos de contacto: dmeuwly@mac.com

■ Nordberg, Tommi

Tommi Nordberg (1963) es vicepresidente ejecutivo de la línea de productos de identidad de Gemalto. También es Presidente Consejero Delegado de Setec Oy en Finlandia, una filial al cien por ciento de Gemplus. En 1998, se incorporó a Setec Oy, donde ha ocupado varios puestos directivos importantes, tales como responsable de la dirección de dos líneas de negocio, impresión de seguridad y organismos públicos y empresas. Posee una maestría en ciencias (MSc) por la Universidad de tecnología de Helsinki y se graduó en marketing internacional en la Escuela de económicas de Helsinki. Tras ocupar varios cargos como director de proyectos y desarrollo de marketing en *UPM-Kymmene plc*., se incorporó a Setec Oy.

Datos de contacto: tommi.nordberg@setec.fi

■ Ombelli, Diana

Diana Ombelli (1970) trabaja como jefa de proyectos en *Sdu Identification*, una imprenta de seguridad de Haarlem (Países Bajos). Anteriormente dirigió el laboratorio de esa misma imprenta. Durante tres años trabajó como científico forense en el laboratorio forense de la policía de Berna (Suiza), donde analizaba microrrastros y se especializó en el campo de pruebas de huellas dactilares. Más adelante fue contratada por la Oficina Federal Suiza de Extranjería, donde ayudó al jefe de proyectos de Expedición electrónica de visados (EEV) en la concesión del contrato público para el suministro de las etiquetas adhesivas de visados y equipos conexos.
Fue miembro del Grupo de Trabajo sobre nuevas tecnologías al que el Grupo consultivo técnico de la OACI pidió que realizara un estudio sobre nuevas tecnologías para la lectura mecánica de documentos de viaje y formulara recomendaciones al respecto. Estudió en el Instituto de la policía científica y criminología de la facultad de derecho de la Universidad de Lausana (Suiza), donde se graduó en ciencias forenses en 1993.
Datos de contacto: diana.ombelli@tiscali.nl

■ Ponsioen, Paul

Antes de jubilarse en 1993, Paul Ponsioen (1942) fue jefe de proyecto en *Sdu Identification* en Haarlem (Países Bajos). Tras recibir formación técnica, se especializó en técnicas de impresión. Ocupó varios cargos en el sector de las artes gráficas, tales como formador de un centro de formación de diseño en un país en desarrollo. Durante su carrera profesional en la imprenta estatal holandesa (*Staatsdrukkerij*), se especializó en garantía de calidad y desarrollo de documentos seguros, tales como cheques, boletos de lotería y pasaportes.
Datos de contacto: paul.ponsioen@planet.nl

■ Ruiter, Ineke

Ineke Ruiter (1951) es directora de *Management Centrum*, un centro de gestión de implantación estratégica para el sector público, fundado por el gobierno holandés en 1990. Ineke Ruiter se ha encargado de varios proyectos de gran envergadura para el Gobierno holandés. Fue subdirectora de proyecto en el proyecto para la creación de una base de datos municipal de registros personales y jefa de proyecto en el proyecto para la nueva generación de documentos de viaje, donde se ocupó del desarrollo y la implantación del nuevo documento de viaje en octubre de 2001. Como directora de programas es responsable, en la actualidad, del desarrollo e implantación de un nuevo sistema de números de identidad únicos para todos los ciudadanos de los Países Bajos.
Datos de contacto: ineke.ruiter@idmanagement-centrum.com

■ Wayman, Jim

Jim Wayman (1951) se doctoró en ingeniería por la Universidad de California, Santa Bárbara, en 1980 y se incorporó al departamento de matemáticas de la Escuela Naval de Posgrado de los Estados Unidos en 1981. Posee cuatro patentes por sus primeros trabajos en el campo del procesamiento del habla y reconocimiento del hablante. En 1986, el Departamento de Defensa de los Estados Unidos le concedió un contrato para el desarrollo y análisis de sistemas de seguridad técnicos y biométricos. En 1995, puso en marcha el centro de pruebas biométricas de la Escuela de Ingeniería de la Universidad del Estado de San José, que fue nombrado Centro Nacional de Pruebas Biométricas de los Estados Unidos por el Consorcio Biométrico en 1997 y funcionó como tal hasta el año 2000. Tiene más de dos docenas de publicaciones revisadas por homólogos en materia de biometría y pruebas de sistemas biométricos, es un experto principal del Reino Unido en el Comité ISO/IEC SC 37 sobre normas biométricas internacionales y es uno de los miembros principales del Grupo de Trabajo sobre biometría del Reino Unido; es miembro del Comité "Whither Biometrics" de la Academia Nacional de Ciencias/Consejo de Investigación Nacional (NAS/NRC por sus siglas en inglés); es miembro del comité NAS/NRC citado anteriormente sobre tecnologías de autenticación y sus consecuencias en la vida privada y miembro del IEE. Es coeditor de *Biometric Systems: Technology, Design and Performance Evaluation* (Springer, London, 2005) de J. Wayman, A. Jain, D. Maltoni y D. Maio. Vive en Monterrey, California, con su esposa Kristina y sus tres hijas.
Datos de contacto: biomet@email.sjsu.edu

PRÓLOGO

La gestión de la migración está convirtiéndose en un área cada vez más compleja del buen gobierno, unida inextricablemente a cuestiones de desarrollo económico y social, derechos humanos, seguridad, estabilidad y cooperación regional.

Abordar los problemas de la migración de forma integral y mediante la cooperación es, hoy en día, un requisito fundamental para una gobernanza nacional responsable, unas relaciones internacionales eficaces y una participación plena en las instituciones internacionales y regionales.

Los retos a que se enfrentan los gobiernos son complejos, por ejemplo, reducir la migración irregular, promover los derechos de los migrantes, proteger a los más vulnerables, reducir las presiones económicas que influyen en la emigración y canalizar la migración regular hacia objetivos nacionales estratégicos.

Uno de los mayores retos con que se encuentran los gobiernos en la actualidad es tratar de mejorar la fiabilidad y la calidad de los documentos de identidad y de viaje.

La Organización Internacional para las Migraciones (OIM) entiende que la gestión de los procesos migratorios se ve facilitada cuando los documentos de viaje son más seguros.

Como parte de una labor más amplia dirigida a ayudar a los gobiernos asociados a dotarse de mejores medios para canalizar la migración, la OIM también trabaja por mejorar la calidad de los documentos de viaje y los sistemas conexos de expedición e inspección.

Parte de esta labor consiste en ayudar a los países a evaluar de forma crítica sus sistemas y documentos en vigor, preparar nuevas especificaciones y procesos, apoyar la elaboración de pliegos de condiciones y gestionar la puesta en marcha de proyectos afines.

En ese contexto, la OIM ha advertido la necesidad de disponer de un mejor material de consulta que ayude a las partes a acometer el proceso de creación nuevos documentos de viaje o identidad.

El presente Manual para desarrolladores es un instrumento pedagógico que responde a esa necesidad, al aportar una visión de conjunto de los aspectos esenciales que deben tenerse en cuenta en el proceso de creación de cualquier documento seguro nuevo.

El manual pone de relieve la importancia de la "cadena de seguridad", en donde la seguridad de todo el documento se ve determinada por el eslabón más frágil, y aborda cuestiones que abarcan desde el concepto de seguridad hasta la infraestructura logística.

La información y las orientaciones contenidas en el presente manual pretenden ampliar los conocimientos en la materia y facilitar el trabajo de las personas y los organismos que intervienen en la confección de documentos de identidad y de viaje más seguros.

División de Cooperación Técnica sobre Migración

PREFACIO

Gestionar y utilizar documentos de identidad y de viaje seguros, incluidos los documentos que incorporan tecnología biométrica, es un problema cada vez más importante y complejo para los Estados. La gestión de documentos de identidad y de viaje tiene consecuencias en la movilidad, el acceso a los servicios, la seguridad y el buen gobierno. Gestionar la expedición y verificación de documentos seguros se ha convertido en una rutina cotidiana en todo el mundo. En particular, los procesos de verificación exigen que los documentos seguros sean muy fiables y fáciles de comprobar. Esos requisitos pueden influir en gran medida en la elección que se haga de las opciones disponibles para crear documentos seguros y en la selección de las entidades de expedición y producción de documentos de seguridad.

Generalmente, se considera que la elaboración de documentos es un proceso sumamente técnico. Ahora bien, existe un espectro de partes interesadas, tanto públicas como privadas, para quienes es importante comprender con claridad los conceptos y procesos básicos sobre los que se sustenta la expedición de un documento seguro. Así, muy a menudo se hace referencia a la función identitaria de un documento, sin saber realmente lo que es una identidad. Del mismo modo, con frecuencia se dan pasos para modernizar los documentos de viaje e identidad mediante la incorporación de elementos biométricos, sin llegar a comprender del todo cuáles son las ventajas y las limitaciones de la tecnología biométrica a la hora de contribuir a que la gestión de la identidad sea más segura.

Existe muy poco material de consulta disponible públicamente sobre los procesos fundamentales que intervienen en la elaboración de

un documento seguro. Esa falta de material de consulta animó a dos especialistas en documentos, Diana Ombelli y Fons Knopjes, a compilar y preparar un manual sobre cómo elaborar documentos seguros, para lo que colaboraron estrechamente con una serie de especialistas de prestigio internacional, a fin de documentar y dejar constancia de sus conocimientos y experiencia. El presente manual pretende proporcionar una visión de conjunto exhaustiva de todos los aspectos relacionados con la elaboración e implantación de un documento de seguridad nuevo, y servir de inspiración a la hora de poner en marcha un proyecto para la elaboración de documentos.

El presente manual no es una guía práctica en que se indique paso a paso el método que hay que seguir, sino que constituye una fuente de consulta, donde las entidades encargadas de gestionar y elaborar documentos seguros pueden encontrar instrumentos e ideas para poner a punto su proyecto y su producto. Dada la variedad de tipos y formas de documentos seguros que existen, los editores se han centrado en los documentos de viaje e identidad. El manual tiene por objeto presentar una visión de conjunto de los elementos esenciales que han de tenerse en cuenta en todo proceso de elaboración de un nuevo documento seguro. Engloba cuestiones que comprenden desde el concepto de seguridad hasta la infraestructura logística. El manual también pone de relieve la importancia de la "cadena de seguridad", donde el eslabón más frágil determina el grado global de seguridad del documento.

En resumen, el presente manual ha sido concebido para proporcionar a todos los interesados asesoramiento actualizado en materia técnica y de gestión respecto de los procesos de elaboración de los nuevos documentos de viaje e identidad (incluidos los pasaportes). El manual para desarrolladores existe en inglés, francés, español, ruso y árabe.

Nota de agradecimiento de los editores

Conscientes de que las entidades encargadas del diseño y elaboración de documentos han de abordar una gran cantidad de factores en el proceso de creación de un documento seguro nuevo, hemos contado con la participación de distintos especialistas. La combinación de

sus conocimientos prácticos y teóricos, y de la experiencia adquirida en el campo de los documentos seguros, hacen que este libro sea excepcional. Los editores, Fons Knopjes y Diana Ombelli, desean expresar su especial agradecimiento a Birgit Cardell, Charles Chatwin, Chuck Baggeroer, Cor Buursma, Daniele Graber, Didier Meuwly, Idius Felix, Ineke Ruiter, Isabel Baltazar, Jan Heim van Blankenstein, Jim Wayman, Sjef Broekhaar, Mike Dell, Nils Ångström, Paul Ponsioen, Piet Lakeman y Tommy Nordberg por su valiosa contribución. En la sección “Aportaciones. Currículum vitae” se presenta a cada uno de ellos por separado.

Los editores también están profundamente agradecidos a Jaap Drupsteen por el diseño de la portada del manual, a John Mercer y Ana Bela Nobre por su trabajo de revisión y las observaciones realizadas, y a Fred Zwarts por su apoyo en la etapa inicial del libro (2001).

Por ultimo, los editores desean expresar su agradecimiento a la Organización Internacional para las Migraciones por su apoyo en la traducción del presente manual al francés, español, ruso y árabe, y su publicación.

CAPÍTULO 1

INTRODUCCIÓN GENERAL

1.1 Definición de documento seguro

Por documento seguro se entiende cualquier tipo de documento que tiene un valor especial para el titular del mismo, contiene datos e información específicos, y tiene la propiedad de que en cualquier momento puede confirmarse su veracidad, validez y autenticidad, con el fin de verificar que es un documento auténtico expedido por las autoridades u organismos competentes para un fin determinado.

El hecho de que la autenticidad de un documento seguro pueda ser corroborada en cualquier momento hace que ese documento tenga un valor legal o comercial para su usuario o titular oficial. Como tal, es, además, un documento jurídico, pues confiere al titular autorizado ciertos derechos, como el de acceso o el de valor monetario. Cuando se utiliza para viajar o identificarse, dichos documentos constituyen la prueba inmediata de la condición jurídica del titular, en particular, con respecto a su identidad y nacionalidad.

Hay dos características fundamentales en la creación de un documento seguro: su función y su valor. Éstas serán descritas en las secciones que siguen a continuación.

1.2 Función

La función específica de un documento ha de ser determinada antes de su producción. Por ejemplo, ¿va a servir como medio de identificación, de pago, o ambas cosas? Definir su función también es importante porque ello determinará las normas que la parte contratante deberá especificar en su pliego de condiciones (véase el Capítulo 2 “Puesta en marcha”).

En el pasado, los documentos seguros solían tener una única función, al igual que un billete de banco. Sin embargo, hoy en día, los documentos son cada vez más multifuncionales. Tomemos el pasaporte como ejemplo. Tradicionalmente, ha sido un documento de viaje, pero ahora también funciona como medio de identificación. En América del Norte, el permiso de conducir sirve como documento de identificación, además de ser prueba de que se sabe conducir. Atribuir varias funciones a un documento aumenta su valor, pero al mismo tiempo, cuantas más funciones tenga, más vulnerable será a un posible uso indebido.

Empezar a utilizar documentos multifuntionales ha sido posible gracias a los avances de la tecnología, en particular de las artes gráficas. Una imprenta moderna está mucho más avanzada hoy de lo que lo estaba hace 50 años. Las planchas de Offset han reemplazado a los tipos de plomo, los polímeros han sustituido al papel y los departamentos de maquetación utilizan técnicas de "*offset digital*" (CTP). Esos avances tecnológicos son realmente fascinantes y han aumentado el nivel de seguridad de los documentos. Ahora bien, también han hecho que los procesos de elaboración sean más complejos y requieran la intervención de un mayor número de disciplinas.

Si bien es posible definir un método general para elaborar los distintos tipos de documentos seguros, las características funcionales de cada tipo exigen enfoques más específicos. El método que se aplique también estará relacionado con el valor intrínseco del documento.

■ 1.3 Valor

Los documentos seguros pueden clasificarse en función de su valor, ya sea monetario o jurídico (van Assem et al, 1994). Ese valor, del que el usuario del documento no suele ser consciente, exige un nivel de seguridad adecuado. El riesgo y las consecuencias del peligro de fraude de un documento determinarán el nivel de seguridad que se asigne.

En la Figura 1-1 aparecen los distintos tipos de documentos conocidos clasificados por categorías. Los documentos de la categoría 1 se fabrican en un entorno seguro con materiales adaptados a los requisitos de su uso y su expedición queda registrada. Los documentos de la categoría 2 pueden incorporar algunos elementos básicos de seguridad.

Los documentos de la categoría 3 tienen un valor (privado) para el propietario y raramente están protegidos por elementos que permitan confirmar su veracidad.

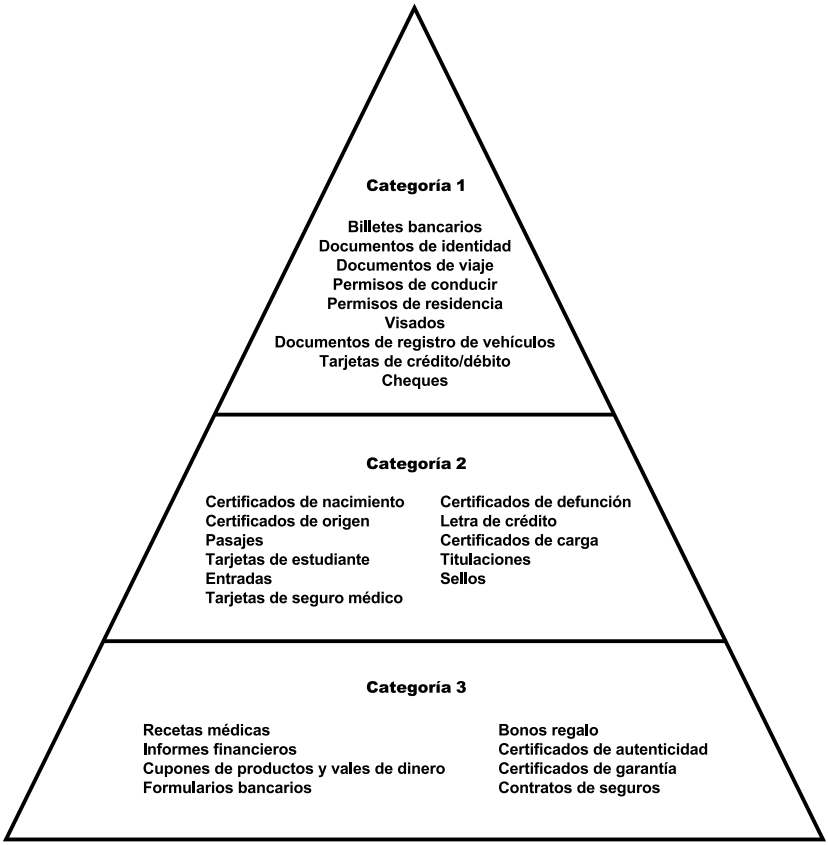


Figura 1-1: Categorías de documentos

■ 1.4 Medios para proteger un documento

No existe un método único y exclusivo para proteger un documento contra el fraude. La protección contra el fraude es un proceso que ha de actualizarse constantemente, y sólo puede lograrse combinando distintos elementos de seguridad, probablemente, con un efecto puramente temporal.

Elegir los elementos de seguridad que han de utilizarse y cómo combinarlos depende del nivel de seguridad que se atribuya al documento. Aparte del riesgo de fraude, el nivel de seguridad del

documento también está íntimamente ligado al proceso de autenticación. Las personas que intervienen en ese proceso y su nivel de conocimientos en materia de verificación a menudo determinan la combinación de elementos de seguridad que se utilizarán (véase también el Capítulo 2, Grupo destinatario). Así por ejemplo, un billete de banco necesita puntos de control para:

- los ciudadanos
- los dependientes de comercios
- el personal bancario y postal (incluido el tratamiento en los bancos centrales)
- los investigadores forenses
- la entidad productora

Del mismo modo, un documento de viaje puede ser examinado por:

- compañías aéreas y agencias de viaje
- empleados de hoteles y comercios
- la policía
- las autoridades de control fronterizo
- los laboratorios forenses
- la entidad productora

En cada uno de esos casos, las personas que verifican el documento deben conocer suficientemente los rasgos de seguridad. Cualquier persona que inspeccione un documento, independientemente de su nivel, ha de saber qué aspecto tiene el documento auténtico y qué es lo que hay que buscar al examinarlo.

Ahora bien, por lo general, el grado de conocimiento de la persona que examina el documento se corresponde con el nivel de seguridad pertinente.

Existen, al menos, tres niveles de seguridad a que suelen referirse los especialistas en documentos:

- El nivel 1 de seguridad atañe al ciudadano común y corriente. El documento puede ser examinado a simple vista. Algunos de los rasgos de seguridad más evidentes son las filigranas, los hilos de seguridad, los elementos difractivos ópticamente variables y las características del papel utilizado (el tacto y el sonido).

Figura 1-2
Marca de agua en un billete bancario de 100 coronas suecas

Figura 1-3
Hilo de seguridad en el mismo billete bancario que aparece en la Figura 1-2

- El nivel 2 de seguridad requiere la utilización de un equipo básico, como una lupa o una lámpara de rayos ultravioleta (luz negra). Algunos de los elementos de seguridad comprendidos en este nivel son la impresión microscópica (microimpresión) y la utilización de tintas o partículas (por ejemplo, fibras) que reaccionan a la luz ultravioleta.

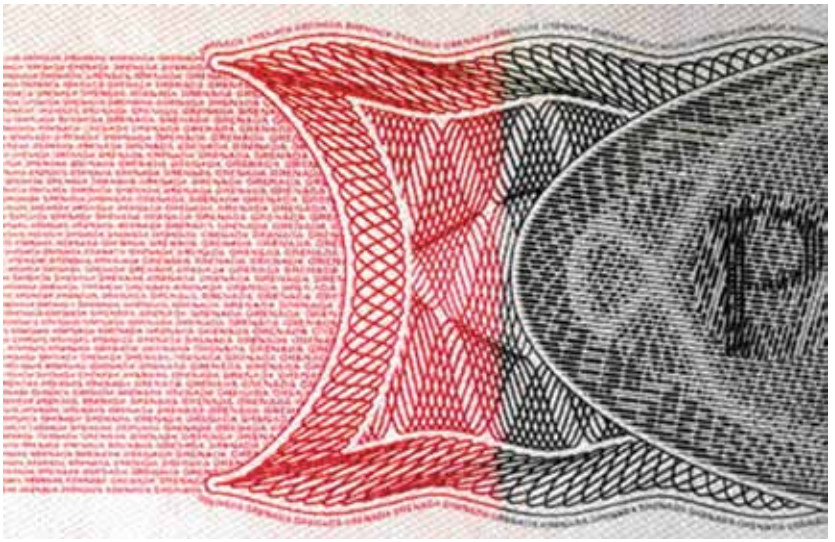


Figura 1-4
Microimpresión

Figura 1-5
Impresión fluorescente a los rayos UV de un permiso de residencia europeo

- Los elementos utilizados en el nivel 3 de seguridad son confidenciales y su verificación requiere el acceso a equipos más complejos, tales como microscopios, equipos sensibles a la luz infrarroja o laboratorios. En este nivel, el fabricante puede añadir elementos que permitan confirmar si un producto concreto ha sido fabricado en sus instalaciones

Figura 1-6
Empleo de microscopios y equipos infrarrojos
(Cortesía del Laboratorio Nacional Sueco de Ciencia Forense de Linköping)

Figura 1-7
Control de producto en prensa (Cortesía de Setec Oy de Finlandia)

Los elementos del primer nivel de seguridad son sumamente importantes, pues permiten que la población pueda examinarlos rápidamente sin necesidad de ningún instrumento. Ahora bien, en este momento se están desarrollando demasiados elementos de nivel 2 de seguridad que requieren el uso de instrumentos para determinar su autenticidad. Y si bien existe una amplia gama de instrumentos en el mercado, tales como lentes, lámparas y filtros, los inspectores de documentos han de tener acceso a ellos para examinar con eficacia un documento. Además, aun cuando se tenga acceso a las herramientas adecuadas, cualquier documento que contenga un sinfín de complejos elementos de seguridad será difícil de autenticar. Por lo general, el verificador no dispone de mucho tiempo para examinar un documento, y podría limitarse a comprobar los rasgos de seguridad que son más fáciles de verificar. Así pues, es conveniente que las entidades productoras tengan en cuenta esas restricciones antes de agregar demasiados elementos de seguridad.

Este es un buen argumento para crear un número limitado, si bien de gran calidad, de elementos de autenticación. Ahora bien, la información sobre dichos rasgos debe estar protegida y su divulgación ha de ser equilibrada. Mantener en secreto esas características no tiene que alertar a las personas interesadas, pero su divulgación tampoco debe facilitar la falsificación. Por otro lado, los conocimientos de los usuarios profesionales (por ejemplo, las instituciones financieras) pueden mejorarse a través de cursos de formación en el propio servicio, que también podrían abordar la verificación de los elementos de nivel 2 de seguridad.

■ 1.5 La cadena del documento seguro: descripción general

La elaboración y el uso de un documento protegido forman parte integrante de una cadena más amplia. Dado que la resistencia de una cadena depende de su eslabón más débil, todo documento protegido pasa por las etapas siguientes:

- solicitud
- producción

- expedición
- uso
- retirada

1.5.1 Solicitud

Hay distintas formas de solicitar un documento seguro. Puede solicitarse en persona, en un mostrador o por correo. En el caso de los documentos relacionados con la identidad es esencial que la identidad del solicitante sea comprobada, utilizando un documento original o copias de éste (véase el Capítulo 4 para más detalles).

Como muestra la fotografía *infra*, no siempre es una cuestión de tecnología. La presencia de la autoridad competente y la verificación en persona de la identidad por parte de dicha autoridad son fundamentales para garantizar la integridad de un documento.

Administración de cédulas de identidad (2006)
(Cortesía de *ID Management Centre*, Países Bajos)

1.5.2 Producción

Los documentos con un alto grado de seguridad deben elaborarse y producirse en entornos seguros, utilizando materiales concebidos específicamente para su fabricación. También hay que verificar la calidad y las cantidades a lo largo de todo el proceso de producción.

1.5.3 Expedición

Algunos documentos protegidos se personalizan tras su producción. Ello significa que es preciso añadir información variable al documento genérico como, por ejemplo, datos personales, fecha y lugar de expedición, organismo expedidor, etc. Muy a menudo los documentos se expiden en un lugar diferente al de su producción.

Además, es preciso analizar otras cuestiones. En algunos casos, el receptor del documento también es su usuario (por ejemplo, un pasaporte). Asimismo, hay que tener en cuenta a las autoridades expedidoras: quiénes son y cómo se desarrolla el proceso de solicitud y expedición; si se expide el documento inmediatamente una vez personalizado o si hay etapas intermedias.

1.5.4 Uso

En esta etapa, el documento está en manos de los usuarios, quienes pueden expresar sus quejas a las entidades expedidoras y productoras. Esa información debe ser recabada y analizada antes de diseñar la siguiente generación de documentos. Por otro lado, no hay que olvidar que el desarrollador de un documento a menudo pierde contacto con el producto final tras su elaboración, salvo que tenga que utilizarlo personalmente.

1.5.5 Retirada

Los documentos seguros pueden retirarse de la circulación por distintas razones, tales como el desgaste (por ejemplo, los billetes de banco). También pueden reemplazarse por una nueva edición.

■ 1.6 Definición del proceso

Con el fin de evitar ambigüedades, por “proceso de gestación” se entiende el proceso de creación e implantación de un nuevo documento seguro. Por “proceso de desarrollo” se entiende únicamente una parte

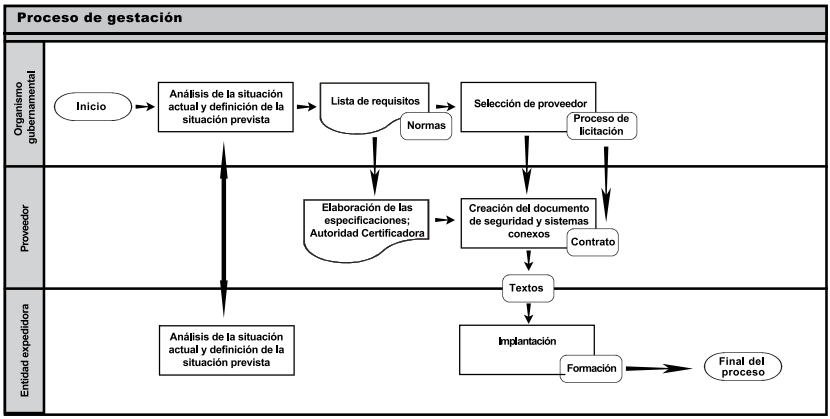


Figura 1-9
Proceso de gestación

del proceso de gestación. En la Figura 1-9 se ilustra una situación característica en que tres actores diferentes participan en el proceso de gestación de un documento expedido por el Estado: la entidad pública (normalmente uno o más ministerios), el proveedor (la entidad productora o el integrador de sistemas del sector) y el organismo expedidor (organismo ejecutivo del Estado, por ejemplo, la policía o la oficina de pasaportes).

■ 1.7 Asegurar la calidad

1.7.1 Calificación de la calidad de las empresas

Existen dos indicadores principales de la gestión de la calidad en contextos empresariales: la norma ISO 9001 y los programas de certificación.

A. ISO 9001

La norma ISO 9001 forma parte de un programa de normas universales de certificación de la calidad de servicios remunerados. Siguiendo un modelo de umbrales, los programas de excelencia tienen por objeto la obtención de mejoras para alcanzar esos umbrales o niveles objetivo. Se basan en mediciones periódicas (autoevaluaciones) y atañen a todas las partes interesadas (clientes, empleados, gerentes, proveedores, etc.).

La finalidad de la norma ISO 9001 es ayudar a las organizaciones a aplicar y administrar sus sistemas internos de gestión de calidad. La gerencia de las empresas que tienen la certificación ISO 9001 han de garantizar la aplicación y conformidad de determinadas normas en todas las etapas del proceso de producción. Esas etapas incluyen la concepción, el desarrollo, la producción, la instalación y los servicios posventa, que deben estar descritos y documentados en el manual de calidad, es decir, en el manual de gestión de la calidad de la empresa. Las políticas, las metas y los sistemas de calidad, que incluyen organigramas y procedimientos,[1] tales como procedimientos operativos e instrucciones o procedimientos de trabajo (Maniak et al, 1997), también deben estar descritos en ese manual. Los sistemas de calidad de las empresas que hayan obtenido la certificación ISO estarán sujetos, con regularidad, a inspecciones por auditores externos.

B. Programas de certificación

La Confederación internacional de industrias gráficas e industrias afines (*International Confederation for Printing and Allied Industries* (INTERGRAF)), con sede en Bruselas, ha preparado dos programas de certificación para las imprentas y proveedores de documentos de seguridad.

La certificación CWA 14641:2003 (*CEN Workshop Agreement*) para imprentas de seguridad proporciona una serie de criterios bien establecidos a efectos de ejecutar sistemas de gestión seguros y eficaces, así como procesos de auditoría precisos que certifiquen su cumplimiento.

Por otro lado, la certificación CWA de sistemas de gestión de seguridad para impresión segura se concede a las imprentas, basándose en una serie de especificaciones acordadas por las distintas partes interesadas del sector: imprentas, clientes, proveedores y organismos públicos (véase CWA 14641:2003). Las palabras seguridad, fiabilidad y calidad parecen estar unidas, y, de hecho, están íntimamente ligadas en la

[1] Un procedimiento puede definirse como una forma específica de llevar a cabo una actividad (ISO 8402).

cadena del documento. En particular, en el contexto de las inspecciones realizadas por los organismos del Estado, la seguridad y la fiabilidad de un documento seguro se basan en la calidad del producto: la mala calidad puede suscitar la sospecha de fraude.

1.7.2 ¿Qué se entiende por calidad?

La calidad puede definirse recurriendo a las claves del sector y la industria. En un entorno industrial, el concepto de calidad se utiliza para caracterizar un producto y fabricarlo de forma sistemática. Desde el punto de vista del consumidor, la calidad es, a menudo, un rasgo subjetivo. Muchos especialistas en calidad han tratado de racionalizar esa subjetividad. Así por ejemplo, el profesor David Garvin, de *Harvard Business School*, distingue ocho dimensiones de la calidad: desempeño, rasgos, fiabilidad, conformidad, durabilidad, capacidad para prestar el servicio, estética y calidad percibida. Los clientes raramente hablan de todas esas dimensiones y normalmente se fijan en una o dos que les llaman la atención (Flower, 1990).

De éstas, las dimensiones aplicables a los documentos de seguridad son las siguientes: conformidad, rasgos, fiabilidad, durabilidad, calidad percibida y estética.

Por *conformidad* se entiende el grado en que el documento de seguridad se ajusta a las reglas establecidas por las normas internacionales.

Por *rasgos* se entienden los elementos de seguridad que protegen el documento contra el fraude.

Por *fiabilidad* se entiende el grado en que la población lo acepta para el uso para el que ha sido concebido.

Por *durabilidad* se entiende la capacidad del documento para resistir las condiciones normales de uso durante un período de tiempo acordado.

En un documento de seguridad, la *calidad* puede venir determinada por varios elementos, tales como la nitidez de los detalles impresos o la

filigrana, la firmeza del papel o la pulcritud de la encuadernación de un pasaporte.

Por ultimo, está la *estética*, pues como advierte el dicho, "sobre gustos no hay nada escrito".

Distintos especialistas, entre éstos Garvin, han refutado el mito de que la calidad cuesta dinero. Si se analizan los procesos y se eliminan las etapas superfluas o se hacen más eficaces, se reducirán los costos. Por consiguiente, una mayor calidad puede redundar en menores costos (Flower, 1990).

Una vez definida la calidad, es esencial saber cómo medirla. Para ello puede utilizarse una combinación de instrumentos de gestión de procesos y de control del producto. Entre los instrumentos para la gestión de procesos figuran los exámenes, el procedimiento de supervisión paso a paso y el ciclo "planificar-hacer-verificar-actuar" (PDCA, por sus siglas en inglés). Originalmente elaborado por Walter A Shewhart y popularizado por W. Edwards Deming en el decenio de 1950, el ciclo PDCA es una herramienta que ayuda a determinar distintas fuentes variables que pueden hacer que un producto se aleje de lo que el cliente desea y espera. Recomienda ubicar los procesos empresariales en un bucle de retroalimentación continuo, de manera que los gerentes puedan determinar y modificar las partes del proceso que deben mejorar. En el Capítulo 5 se expondrán con detalle los procedimientos de control del producto (véanse las secciones 5.3 Materiales y 5.4 Técnicas de personalización).

■ 1.8 Aspectos generales de los Capítulos siguientes

En los Capítulos que siguen a continuación se explican minuciosamente las etapas y los aspectos importantes del proceso de elaboración de un documento seguro. El Capítulo 2 describe las actividades preparatorias, tales como el análisis (de fraude), la confección de listas de requisitos y la organización de proyectos. También se mencionan las normas sobre documentos seguros. El Capítulo 3 está dedicado a la elección del

proveedor: desde el procedimiento de licitación hasta el contrato. El Capítulo 4 describe los elementos que integran la cadena del documento.

En el Capítulo 5 se describen todos los aspectos físicos relacionados con la elaboración de los documentos seguros: material y diseño, proceso y técnicas de personalización, pruebas y producción. El Capítulo 6 ofrece información más exhaustiva sobre la identificación. El Capítulo 7 proporciona una visión de conjunto sobre el vínculo entre el documento y el individuo mediante el uso de la biometría. El Capítulo 8 explica el proceso de la identificación digital. Por último, el Capítulo 9 incluye un amplio espectro de fuentes de información y describe distintos programas de cooperación y elementos de capacitación.

Referencias

2006 Fundación Europea para la Gestión de la Calidad, http://www.efqm.org , Bruselas.

Flower, J.,
1990 "*Managing Quality*", *Healthcare Forum Journal*, Vol. 33 (5); 64-68, sept-oct.

Maniak, R. et al.,
1997 *Marketing industriel*, Nathan, París.

van Assem, B., Brongers, D. *et al.*,
1994 *Sterke papieren, Praktische gids in de wereld van beveiligd drukwerk*, *Sdu Publishing, Koninginnegracht*, La Haya.

CAPÍTULO 2

■ PUESTA EN MARCHA

■ 2.1 Evaluación general

Los puntos fuertes, los puntos débiles y los posibles riesgos pueden detectarse de forma estructurada mediante la realización de evaluaciones. Un análisis detallado durante la etapa de desarrollo del documento permitirá reconocer oportunamente esos riesgos durante el proceso de elaboración y proporcionará información sobre el tipo de riesgos. Ese planteamiento analítico metódico también hace posible detectar y prever posibles obstáculos y amenazas.

Las fuentes de información que han de utilizarse dependen del tipo y funcionalidad del producto que vaya a elaborarse. Pueden estar próximas al lugar de origen, como el lugar de trabajo del productor, el organismo público pertinente o la entidad expedidora. "Las fuentes cerradas" son igualmente importantes, dado que proporcionan información que a menudo es confidencial e inaccesible para el público en general. Entre las "fuentes cerradas" figuran la policía, las oficinas de aduanas y los servicios de inmigración.

Las fuentes de información también pueden proporcionar detalles específicos sobre productos derivados. Así, por ejemplo, el registro de imágenes holográficas protege a los productores de dispositivos ópticos variables, que integran la Asociación Internacional de Fabricantes de Hologramas (IHMA, por sus siglas en inglés), frente la falsificación y concede derechos de autor a sus dispositivos ópticos variables (véanse el Capítulo 9).

En términos generales, cualquier evaluación debe permitir comprender los aspectos siguientes:

- Función
- ¿Cómo y con qué frecuencia se utilizará el documento?
- ¿Dónde y cómo se guardará o portará?
- ¿En qué medio físico se utilizará el documento?
- ¿Cuáles son las condiciones climatológicas? Frío y seco, o cálido y húmedo
- Vida útil deseada
- Ampliación de la validez y sustitución
- Grupo destinatario
- Métodos de autenticación
- Procedimiento de solicitud
- Expedición
- Circunstancias de las inspecciones

2.1.1 Función

El modo en que se elabora un documento depende de su función. Ello suscita una serie de preguntas. Por ejemplo, ¿servirá el documento como medio de identificación?, ¿como medio de pago? o ¿para entrar a un evento, como un concierto de pop? Si el documento va a servir como medio de pago, tendrá que cumplir las normas bancarias. Si el documento va a servir únicamente como prueba a la vista, como en el caso de la entrada para el concierto de pop, es fundamental que se reconozca. Por otro lado, hay que distinguir entre lo reconocible que puede ser un documento y la legibilidad de los datos del titular del mismo.

Los documentos pueden tener diferentes funciones:

- revestir un valor monetario
- servir para determinar la identidad
- conceder autoridad
- probar la propiedad
- conceder acceso

Entre los documentos con valor monetario figuran los billetes bancarios, los cheques, las tarjetas de débito, los sellos, los cheques-regalo, los avales bancarios y las tarjetas de crédito. Por otra parte, los documentos que determinan la identidad se utilizan para verificar la identidad del titular. Entre éstos figuran los documentos nacionales de identidad, los pasaportes, los permisos de residencia para extranjeros y, en algunos casos, los permisos de conducir.

Si se trata de un documento que otorga autoridad, éste puede servir como prueba de que su titular posee competencias que le capacitan para realizar determinadas tareas. Esos documentos incluyen diplomas, permisos, permisos de conducir, licencias de piloto, licencias de taxi, etc. Algunos documentos también pueden servir para probar la titularidad de la propiedad, lo que les hace aún más valiosos. Entre estos documentos figuran los documentos registrales, las escrituras de propiedad, los documentos del registro de vehículos y las escrituras notariales.

La última de las categorías expuestas anteriormente, de concesión de acceso, suele ser importante en el sector privado. Ese tipo de documentos pueden conceder acceso a distintas instalaciones, a archivos informáticos o a los servicios sociales.

Función de un documento

Pasaporte
El pasaporte es un documento de viaje internacionalmente reconocido que garantiza la identidad de su titular. Permite que el titular pueda solicitar un visado para entrar a los países que exigen ese requisito. También permite a las autoridades hacer anotaciones en el pasaporte y registrar la fecha de entrada y salida del país. En algunos casos, el pasaporte sirve a terceros como medio de identificar a su titular, ya sea dentro o fuera del territorio de éstos.

Billete bancario
Los billetes bancarios son un medio de pago legal que emite el banco central de forma oficial y sirve como medio de cambio en la transferencia de bienes o la adquisición de servicios. Para que pueda utilizarse es esencial que la población confíe en su integridad como medio. Esa confianza se basa en una política de emisión bien concebida por el banco central y en la autenticidad de los billetes en circulación.

2.1.2 ¿Cómo y con qué frecuencia se utilizará el documento?

Todo documento tiende a desgastarse cada vez que se utiliza. Por ejemplo, cada vez que un documento se introduce en un sistema de lectura, puede deteriorase y doblarse. Cuanta más información proporcione la entidad expedidora a los posibles proveedores sobre el uso probable del documento, mejor podrán responder éstos con soluciones eficaces con relación al costo.

2.1.3 ¿Dónde y cómo se guardará o portará el documento?

El hecho de que los documentos se vean sometidos a un constante deterioro y flexionado es uno de los factores que más atención requiere en su elaboración. Los documentos de formato pequeño (por ejemplo, el ID-1, véase la sección 2.6 Normas), sujetos a un uso frecuente podrían necesitar una funda protectora.

Esa cuestión adquiere una mayor pertinencia a medida que aumenta el número de documentos que utilizan tecnologías de lectura mecánica.

Figura 2-1
Funda para proteger una tarjeta bancaria
(Cortesía de Fons Knopjes, Países Bajos)

2.1.4 ¿En qué entorno se utilizará el documento?

Los entornos pueden distinguirse del modo siguiente:

- entornos cerrados: el documento se utiliza en una única organización
- entornos híbridos: el documento de una organización puede utilizarse en otras organizaciones
- entorno nacional: el documento se utiliza a nivel nacional
- entorno internacional: el documento se utiliza en todo el mundo

¿Dónde se utiliza el documento?

Pasaporte

En los puntos de control fronterizo, el pasaporte es manipulado por un grupo de inspectores de documentos con amplios conocimientos de los documentos de viaje vigentes. Si un inspector tiene dudas acerca de la autenticidad de un documento en concreto o sobre la identidad del titular, ha de tener a su disposición servicios auxiliares con instrumentos y personal especializados. En otras situaciones, el pasaporte puede ser utilizado por terceros para

determinar la identidad de una persona. Ése es un grupo de usuarios que supuestamente tiene menos experiencia para evaluar la autenticidad de un documento y los datos que contiene. El documento debe poder ser utilizado con eficacia por cualquiera de los dos grupos.

Billetes bancarios

Los billetes bancarios son documentos que prestan un servicio al conjunto de la población. Se trata, pues, de un grupo de usuarios amplio, variado y con escaso conocimiento de los documentos. Es más, a menudo no hay mucho tiempo para examinar detenidamente los billetes, y únicamente se cuenta con instrumentos sencillos para disipar cualquier duda sobre su autenticidad. Los billetes bancarios son impersonales y las condiciones en que se guardan varían, ya que cambian a menudo de manos. Los elementos de primer nivel deben ser de máxima calidad pues han de ser durables y comprensibles. Así pues, las autoridades expedidoras deben hacer un esfuerzo especial para informar al conjunto de la población de tales características.

2.1.5 ¿Cuál es el medio físico: frío y seco o cálido y húmedo?

Los documentos actuales deben ser capaces de resistir todo tipo de condiciones meteorológicas extremas. El calor y la humedad extremos atacan a la estructura de las tarjetas de un modo diferente al que lo hacen las bajas temperaturas. Es importante que se definan, analicen e incluyan en la lista de requisitos los diferentes medios a que pueda estar sometido el documento.

Por ejemplo, un documento que en un momento dado se lleve a Alaska, donde son frecuentes temperaturas de 40 grados centígrados bajo cero, también ha de poder llevarse a la selva tropical, donde las temperaturas

pueden alcanzar los 40 grados centígrados y donde la humedad es elevada. Definir de forma exhaustiva los diferentes medios físicos en que debe utilizarse un documento, permitirá al cliente tomar decisiones con una base más sólida respecto del material, el diseño y los elementos de seguridad del documento.

2.1.6 ¿Cuál es la vida útil deseada?

Los distintos materiales y técnicas de elaboración ofrecen distintos niveles de durabilidad, lo que también puede repercutir en los costos. Por lo general, una tarjeta con una vida útil larga es más cara que una con una vida útil más corta. Es, pues, importante determinar si el documento ha de tener una vida útil corta o larga. Un documento de identificación que tenga que ser válido durante un día o una semana puede que necesite ser seguro, pero no necesariamente durable. Por otro lado, invertir en materiales más resistentes podría contrarrestar el costo ligado a la sustitución de documentos dañados o desgastados.

El requisito mínimo que debe cumplir todo documento seguro es que ha de durar tanto como el uso para el que está previsto. Los documentos que están concebidos para identificar a su titular suelen tener una vida útil más larga. Es bastante frecuente que una tarjeta de identidad tenga una vida útil de cinco años. Algunos países conceden el documento de identidad durante más de cinco años, incluso para toda la vida. Una vida útil larga puede dificultar el control eficaz de los datos personales del titular del documento a la hora de determinar si la persona que figura en éste es idéntica a su usuario. La apariencia del titular de un documento puede variar considerablemente a lo largo de cinco años, y aún más a lo largo de diez. Por consiguiente, la entidad promotora debe sopesar la elección de los materiales y técnicas elegidos frente a los riesgos ligados a los documentos con una vida útil larga y el gasto derivado de su reemisión a intervalos más cortos.

El uso de rasgos biométricos constituye un caso especial. Hay rasgos biométricos codificados, como los rasgos faciales, que pueden cambiar. Ahora bien, si están contenidos en sistemas de almacenamiento estáticos, el documento únicamente será válido en tanto que los rasgos

biométricos sigan siendo aplicables. Si deben actualizarse los rasgos biométricos, entonces habrá que expedir un nuevo documento.

Hay otros factores que afectan a la vida útil de un documento, tales como su diseño técnico, las técnicas aplicadas y el trato que reciba. Desde un punto de vista económico, la autoridad responsable posiblemente considere más ventajoso los periodos de vigencia más largos, mientras que los productores podrían preferir limitarlos.

En resumen, aparte del costo, hay distintos factores que cabe considerar. Por esa razón puede ser difícil decidir cuál será la vida útil de un documento.

2.1.7 Ampliación de la validez o sustitución

Una cuestión importante es la posibilidad de que la validez de un documento pueda ampliarse después de haber sido expedido. Otra cuestión es si un documento debe ser reemplazado después de un periodo determinado. La respuesta depende del objeto del documento y de la validez deseada. Tras varios años, un documento suele quedar técnicamente obsoleto. Por otro lado, la frecuencia de uso de un documento también es un factor importante. En algunos casos, es menos caro tanto para la entidad expedidora como para el usuario ampliar su validez en lugar de sustituirlo. Sin embargo, eso no ocurre en los casos de documentos de viaje de lectura mecánica, dado que la validez de la información (fecha de caducidad) está incluida en la Zona de lectura mecánica (ZLM) y no puede actualizarse en el documento con fiabilidad.

2.1.8 Grupo destinatario

Los destinatarios de los documentos seguros varían. En principio, cualquier ciudadano de un Estado puede ser titular de un documento expedido por el gobierno, mientras que hay grupos específicos que pueden obtener determinados documentos emitidos por el sector privado. Determinar cuál es el grupo destinatario es importante, pues

únicamente entonces podrá una organización evaluar la cantidad, el grado de seguridad, la evolución y los riesgos ligados al documento. Así por ejemplo, ciertos documentos pueden provocar actitudes diferentes en distintos usuarios. Hay quienes pueden considerar que son un fastidio, mientras que para otros pueden ser fuente de orgullo. Así, los usuarios de un pase de policía suelen estar orgullosos de su documento de identidad y por consiguiente lo cuidan.

Grupo destinatario

Pasaporte

Un pasaporte se expide a nombre de su titular. Si bien el titular disfruta de las ventajas del documento de viaje, éste no es el único usuario. Las principales partes interesadas son los funcionarios de fronteras internos y externos. Ahora bien, un documento de viaje también puede utilizarlo un tercero para determinar la identidad del titular. Por ejemplo, el pasaporte puede servir para determinar la identidad de un cliente con quien un tercero va a realizar una importante transacción financiera o celebrar un acto jurídico.

Billetes bancarios

El usuario de un billete de banco suele ser su propietario hasta el momento en que cambia de manos. Del mismo modo, el receptor de un billete bancario también es un usuario. Esos documentos suelen utilizarse como medio de cambio, lo que exige un elevado grado de fiabilidad. Son emitidos por un banco central, que garantiza su fiabilidad y adecuada circulación, de forma tal que su uso por la sociedad queda garantizado en lo que atañe a la calidad y la cantidad. El banco central también posee la titularidad de los derechos de autor de los billetes bancarios.

2.1.9 Métodos de autenticación

Los elementos de seguridad que se incorporan a un documento deben reflejar el contexto de la autenticación. ¿Es posible la autenticación en línea? En caso afirmativo, la autenticación de los datos puede reducir la necesidad de algunos rasgos de seguridad físicos.

2.1.10 Proceso de solicitud

Existen muchas formas de solicitar un documento. Cada método tiene sus restricciones dependiendo del tipo de documento. Algunas solicitudes pueden ser presentadas por personas físicas o jurídicas. Pueden presentarse en persona, pero también en nombre de otro, y por escrito o a través de Internet o por teléfono (véase la sección 4.3 del Capítulo 4).

2.1.11 Expedición

El procedimiento de expedición, que puede ser local, regional o centralizado, puede afectar a la elección que haga el solicitante de determinado documento de seguridad (en el Capítulo 4 se examinan los procedimientos de solicitud y expedición con más detalle). Esos procesos determinan en gran medida los requisitos del producto, que, a su vez, influyen en la elección de una entidad productora en concreto.

2.1.12 Circunstancias de las inspecciones

Es necesario tener una visión de conjunto de las circunstancias en que puede producirse una inspección. Hay una gran diferencia entre verificar una tarjeta de identidad en una oficina de correos, donde hay mejores condiciones (en cuanto a luz, medios de consulta y apoyo tanto en ventanilla como por los servicios auxiliares), que en un bar, donde por lo general la iluminación es deficiente y el personal suele estar distraído. Las condiciones de los controles influyen en las decisiones que se adopten a la hora de determinar las características de un documento.

■ 2.2 Análisis del riesgo de fraude

2.2.1 El enemigo

La disponibilidad de las computadoras, impresoras, escáneres y otros equipos complejos ha facilitado los intentos ilegales de imitar, alterar, cumplimentar o transformar documentos para que parezcan auténticos. La credibilidad de un documento falso depende en gran medida de lo mucho o poco que se parezca al original. Las pinturas célebres y sus copias son un ejemplo concreto de ello. En lo que respecta a los documentos, el parecido se basa en la forma, el color, los materiales utilizados y las circunstancias en que se efectúe el control. Es como cuando se compara dos monedas de euro de dos países diferentes, que son idénticas por una cara e individualizadas para cada país por la otra. El falsificador que elabora un documento falso tipo suele imitar las características más evidentes y evitar las más complejas.

Con el fin de contener el uso indebido o la violación de documentos, es importante analizar el factor delictivo, en especial en lo que atañe a los documentos que son delicados desde un punto de vista político o que pueden dañar gravemente la reputación de una empresa. El análisis de esas amenazas permitirá a las entidades productoras adoptar las medidas pertinentes para reducir el riesgo. A fin de aislarlas, los documentos han de considerarse en un contexto mucho más amplio. Por ejemplo, los delincuentes pueden explotar las amenazas vinculadas al transporte, la expedición o la venta de documentos. En tales casos, no sólo hay que tomar medidas para evitar la alteración del documento en sí mismo, sino que hay que tomar precauciones durante el transporte y la etapa previa a su expedición. Los procedimientos también pueden hacerse más rigurosos.

El uso indebido de documentos también puede verse influido por los acontecimientos políticos. La liberalización del mercado de trabajo entre los Estados miembros de la Unión Europea ilustra este hecho. Según la legislación de la Unión Europea, todo ciudadano tiene derecho a trabajar en cualquiera de sus Estados miembros. Ahora bien, antes de que un ciudadano pueda ser admitido en el mercado laboral, el posible empleador tiene que establecer, en primer lugar, si el ciudadano en

cuestión es en efecto europeo. Eso exige un pasaporte o una tarjeta de identidad que especifique la identidad y la nacionalidad. De más está decir que la liberalización del mercado laboral ha hecho que aumente el valor de los pasaportes europeos y ha dado lugar a que los delincuentes trafiquen con esos documentos.

La aplicación o función de un documento en la vida cotidiana también afecta al modo en que éste puede ser utilizado indebidamente. Hay documentos que se utilizan indebidamente con mayor frecuencia, mayor rapidez y mayor facilidad que otros. El análisis de documentos falsificados permite comprender los distintos tipos de uso indebido. También vale la pena investigar las condiciones bajo las cuales se falsifican los documentos.

2.2.2 Análisis de la cadena

La realización de un análisis del riesgo de fraude antes de empezar a elaborar un documento permite detectar posibles amenazas de antemano. Las autoridades responsables del documento y las partes contratantes deben conocer qué riesgos corre concretamente un documento y si es vulnerable a determinadas formas de fraude.

Por consiguiente, habrá que hacer un análisis de los distintos eslabones de la cadena del documento. Así por ejemplo:

¿Dónde se guardan los documentos?

¿Se comprueban los documentos guardados con regularidad?

¿Existe una división de tareas entre los empleados que manipulan los documentos?

Si hay que pagar tasas para la presentación de solicitudes, ¿quién se encarga de su supervisión?

¿Exige la ley que se cumpla el procedimiento previsto, o se trata de meras directrices administrativas?

¿Son todas las normas en vigor, pertinentes y aplicables, al nuevo documento que vaya a elaborarse?

Los distintos aspectos del proceso de producción y los materiales utilizados también determinan los riesgos. Teóricamente, el proceso de producción debe estar dividido en diferentes etapas. Las salas de producción han de estar separadas y protegidas, y las etapas de verificación deben estar integradas en el proceso de producción. A través de la compartimentación, los productores pueden reducir el riesgo de uso indebido de la maquinaria de producción. En un entorno de producción de documentos mal protegido y con controles ineficaces el riesgo de robo de material y productos acabados aumenta de forma inmediata.

El personal de producción también debe tener una actitud adecuada y ser consciente del valor de los documentos producidos. En algunos casos, las autoridades responsables del documento pueden exigir requisitos especiales al personal, como por ejemplo, que se comprueben sus referencias antes de asignarlos a esta tarea.

Si la producción se lleva a cabo en más de un lugar, y hay que transportar materiales y componentes, el nivel de riesgo aumenta. De por sí, el transporte implica riesgo y el control en el lugar de expedición entraña aún más. Eso ocurre en particular con documentos que tienen valor monetario (por ejemplo, los billetes de lotería) o con los que se utilizan como documentos de identidad. En la medida en que esos documentos estén en blanco y no contengan datos personales, resultarán muy atractivos para los delincuentes. Por esa razón, es necesario guardarlos y supervisarlos de acuerdo con el principio de los “cuatro ojos”, también conocido como “regla de las dos personas”.

Personas que utilizan documentos fraudulentos
El uso de documentos fraudulentos no es un medio de por sí. Por lo general, se trata de un medio para perpetrar delitos más graves. Se utilizan, en primer lugar, para alcanzar una meta final que va más allá del mero acceso a una zona o región determinadas, y, en segundo lugar, para burlar los sistemas de seguridad implantados por los gobiernos como parte de su misión de proteger la soberanía nacional.

Esos documentos son manipulados para ocultar cierta identidad a fin de obtener un documento auténtico o para adaptar determinados datos de un documento para que concuerden con la historia que sustenta la nueva identidad. Esa transformación puede hacerse directamente mediante borrado mecánico, baño químico, programas informáticos digitales o procesos de reproducción no oficiales. También puede hacerse de forma indirecta, recurriendo a sobornos, manipulando los puntos flacos de cada sistema y explotando las similitudes étnicas y fisonómicas entre individuos. En resumen, la amenaza reside en la vulnerabilidad del documento a ser manipulado para gozar de un derecho que normalmente sería denegado.

2.2.3 Formas de falsear o falsificar un documento

Un documento puede ser copiado o manipulado de formas muy diferentes, y, por tanto, todo documento ha de protegerse contra cualquier tipo de usos indebidos.

A continuación figuran los principales tipos de fraude:

- *Falsificación:* reproducción de un documento relativamente nuevo con un material similar o completamente diferente que trata de simular los rasgos de seguridad auténticos.
- *Falseamiento*: modificaciones del contenido de un documento auténtico, tales como sustituir la fotografía, modificar los datos personales o de valor, o manipular las páginas, por ejemplo, cambiándolas.

- *Procedimientos de expedición no autorizados*: personalización no autorizada de un documento auténtico en blanco no expedido.
- *Engañar al expedidor*: obtener un documento auténtico de manera fraudulenta.
- *Impostura:* asumir el nombre o la identidad de un individuo (vivo, muerto o ficticio), con el fin de obtener de forma fraudulenta un documento legítimo de identidad o de viaje.
- *Documentos alternativos:* documentos elaborados, expedidos y entregados por organizaciones no existentes o no reconocibles, o por países que ya no existen.

Los documentos falsificados pueden ser de diferente tipo, desde una sencilla fotocopia sin pretensiones de simular los rasgos de seguridad a falsificaciones excelentes que imitan con gran eficacia el papel, los elementos impresos y los rasgos de seguridad. Es ahí donde se pone de manifiesto la importancia de que los documentos auténticos sean de buena calidad. Si el documento auténtico tiene mala calidad, resultará difícil distinguirlo de uno falso.

El falseamiento ha ido evolucionando en los últimos años y ahora las manipulaciones de documentos son más sofisticadas. La sencilla sustitución de fotografías fácilmente detectable es ahora infrecuente y ha sido reemplazada por técnicas más diestras y avanzadas. Hay distintos modos de alterar la información de un documento, como por ejemplo, utilizando técnicas mecánicas de borrado que eliminan la información original, usando productos químicos o una combinación de ambas técnicas. Una alternativa elegante es incorporar partes de otro documento auténtico al documento (por ejemplo, una página o un laminado), lo que dificulta detectar la manipulación.

Por otro lado, es muy difícil detectar el uso indebido de un documento, pues el material es auténtico. Así pues, se recomienda añadir un atributo adicional durante el proceso de expedición o utilizar una técnica de personalización que aporte singularidad.

Si alguien obtiene un documento seguro de forma fraudulenta presentando un documento de identidad falso, puede resultar difícil localizarlo con posterioridad. Por consiguiente, todos los países han

de tratar que sus documentos de identidad sean tan seguros como sus pasaportes. Entre los documentos de identidad figuran los certificados de nacimiento, las tarjetas o cédulas de identidad y otros documentos de identificación personal.

La impostura documental se produce cuando un documento auténtico y sin manipulaciones es presentado por la persona que no es: por un impostor. La única forma de descubrirlo es realizando los exámenes pertinentes y haciendo comprobaciones biométricas.

Probablemente, la estrategia de la impostura haya ganado popularidad en los últimos años, debido a que los documentos de identidad y de viaje son más difíciles de alterar o falsificar. No obstante, es difícil determinar la gravedad del problema. Podemos suponer que la cifra real es mucho más elevada de lo que se cree, dada la dificultad de detectar las imposturas, si no se dispone de equipos digitales biométricos en los puestos de control fronterizo.

Los documentos alternativos pueden ser ficticios o documentos cuya finalidad es camuflar. Esos documentos se parecen a un documento seguro, en particular los pasaportes, pero provienen de organizaciones no competentes o no reconocibles. Aunque no son una prueba aceptable de la nacionalidad o la identidad, aparecen con suficiente frecuencia como para que se consideren una amenaza. La única manera de detectar y combatir con eficacia este tipo de fraude es mediante la actualización de la información y la capacitación.

2.2.4 Contramedidas

Como parte del esfuerzo permanente por mejorar la respuesta de los documentos frente a los continuos avances tecnológicos en este campo, se ha introducido una serie variable y equilibrada de elementos de seguridad con el fin de combatir el elevado número de falseamientos y falsificaciones. Paralelamente, las estrategias de cambio de rutinas destinadas a burlar a los falsificadores han resultado ser muy eficaces. Algunos ejemplos son la introducción y puesta en circulación sucesivas de distintas generaciones de documentos. Aunque se trata de una espada de doble filo, pues si bien los nuevos documentos son mejores,

el cambio constante de éstos puede provocar confusión y cansancio en los inspectores.

Otras medidas son los controles previos al embarque, que permiten examinar los documentos y a los individuos con antelación, o el despliegue de oficiales de enlace en los puntos de embarque donde existe riesgo. La divulgación de información concisa, precisa y oportuna por la entidad competente también es un arma eficaz en la lucha contra el fraude documental.

Si bien el riesgo de alteraciones y falsificaciones está disminuyendo debido a que los métodos de producción son más fáciles de analizar, y, por consiguiente, más eficaces, el uso indebido de documentos auténticos ha aumentado. Esa táctica fraudulenta entraña bien el uso de documentos de otra persona o la adquisición de documentos auténticos utilizando documentos justificativos falsos o por medios corruptos. Un ejemplo de esto es el empleo del certificado de nacimiento de un bebé fallecido, o el delito moderno de usurpación de identidad, por ejemplo, mediante el robo de los datos personales electrónicos de otro individuo. Esos impostores utilizan documentos falsos de menor valor para obtener documentos legítimos de gran valor.

El problema de la falsificación no puede resolverse simplemente introduciendo medidas de seguridad adicionales. El exceso de información en un documento dificulta el reconocimiento del rasgo esencial de seguridad y puede, por tanto, dar lugar a una autenticación falsa. Así, por ejemplo, si durante una comprobación rápida todo apunta hacia la existencia de una marca de seguridad determinada – marcas de agua, intaglio, etc. – se tenderá a validar el documento en función de esa marca, sin llevar a cabo una comprobación minuciosa del documento o de los datos que contiene.

La validación de un documento como objeto físico no es garantía suficiente de propiedad, pues cualquiera puede ser titular de un documento, pero sólo hay una persona que tiene un vínculo real e indisoluble con éste. Por consiguiente, es preciso analizar el perfil del titular del documento. Es muy importante que se observe e interprete la conducta y el carácter del individuo, y se evite, así, un análisis

meramente basado en la observación del documento. El documento existe en un contexto y ese contexto debe tenerse en cuenta a la hora de determinar la autenticidad del documento.

Todos los casos expuestos son difíciles de detectar e investigar, ya que al recabar las pruebas entran en juego otros factores, a saber:

- la vulnerabilidad de los procesos de expedición de los documentos de identidad
- la existencia de normas ineficaces respecto del almacenamiento de los documentos seguros
- la utilización de medios descentralizados de entrega de documentos a las personas que los han solicitado (envío por correo)
- las normas actuales relativas a los procedimientos aeroportuarios, que exigen controles más rápidos para responder al creciente movimiento y desplazamiento de personas por el planeta

Una consecuencia de la globalización de la economía mundial es el aumento del número de personas que cruzan las fronteras; ello exige un control más rápido, pero más eficaz, de los elementos de seguridad de un documento y de su validación respecto de las bases de datos pertinentes, en especial las que contienen sistemas de alerta para hacer cumplir la ley. Ese proceso afecta necesariamente al individuo y a los documentos.

Así, la biometría adquiere especial importancia en el caso de las imposturas. Implica el uso de mecanismos capaces de almacenar parámetros bio-fisonómicos, que permanezcan inalterados durante el periodo de vigencia del documento y establezcan una relación constante, actualizada y rigurosa entre su legítimo titular y el documento seguro (véase el Capítulo 7). En consecuencia, ese inextricable vínculo de información entre la identidad contenida en el documento y su legítimo titular, no sólo facilita la inspección del documento, sino que además tiene una eficacia comprobada, que, junto con las técnicas de reconocimiento de impostores, constituye una garantía para las personas bienintencionadas y facilita la detección de fraudes y delitos.

Ahora bien, el uso de documentos de lectura mecánica y su vínculo con parámetros biométricos también plantea algunos problemas, en particular con relación a su legibilidad y la formación requerida por los inspectores de documentos. Por tanto, es importante señalar los factores que influyen en la legibilidad de los documentos de lectura mecánica. El desgaste de un documento debido a un uso constante, una manipulación descuidada, a accidentes o a las condiciones atmosféricas y ambientales puede provocar alteraciones imprevistas que podrían invalidar la aceptación de un documento por una máquina. Cuando eso ocurre, es importante que los inspectores sepan a qué otros mecanismos de control han de recurrir.

Es importante recordar que la lectura mecánica de un documento no autentifica de forma automática la totalidad del documento. Cuando una máquina lee un documento, únicamente puede captar y validar una parte de los datos variables. Así, por ejemplo, en el caso de un pasaporte, la fotografía del titular, los visados, los sellos de entrada y salida, la numeración de las páginas y la paginación también deben comprobarse cuidadosamente de forma manual.

Esa es una advertencia importante, ya que los delincuentes explotan de inmediato cualquier punto flaco del sistema. Pensemos en el robo de documentos en blanco. Ése es un tipo de delito que a menudo se organiza a escala transnacional. Es, pues, necesario aplicar de forma coordinada contramedidas eficaces nacionales e internacionales. Además de regular el almacenamiento de documentos en blanco y establecer procedimientos estrictos para su transporte, en especial en el caso de sistemas no centralizados de expedición, se pueden aplicar otras medidas de seguridad, entre éstas:

- Definir medios seguros de autenticación de documentos (sellos electrónicos, por ejemplo, firmas digitales o imágenes insertadas, repujado en seco, sellos húmedos, etc.) y de distribución de la información pertinente entre las entidades interesadas.
- Establecer la posibilidad de acceder a los formularios de solicitud originales en los puertos de entrada, en especial a las fotografías y los documentos justificativos.
- Utilizar normas biométricas.
- Cooperar a nivel internacional para establecer canales rápidos y adecuados de intercambio de información, en concreto, mediante

el acceso a bases de datos en línea que contengan información sobre documentos en blanco robados, viajeros sospechosos y documentación fraudulenta.

Si el documento físico es auténtico, es mucho más difícil detectar el fraude. En el caso de los documentos físicos auténticos, lo único que hay que comprobar es la forma en que se han introducido los datos personales y los elementos de autenticación, sobre lo que apenas existe ninguna información de referencia. Independientemente de los rasgos de seguridad, es crucial que las entidades asociadas intercambien información sobre técnicas de personalización y autenticación.

También hay que subrayar que el método más eficaz de combatir la expedición ilegal de documentos en blanco robados es centralizar la producción y la personalización, hecho que ha sido apuntado en varias publicaciones examinadas en todo el mundo. En ese contexto, también hay que prestar especial atención a: 1) la seguridad física de todas las instalaciones, desde las de producción y almacenamiento hasta las de despacho; 2) el registro de todo el material: utilizado, no utilizado, defectuoso o malogrado; y 3) los números de seguimiento y control de todos los componentes documentales importantes (laminados, sistemas ópticos variables, etc.).

Además, no hay que olvidar los documentos en blanco robados y falsificados en forma de pegatinas o etiquetas adhesivas. Mediante la manipulación del número de serie o montaje – ocultando o añadiendo caracteres – los defraudadores tratan de reducir el riesgo de detección al consultar las bases de datos sobre documentos en blanco robados. En esos casos, la mejor manera de afrontar el problema es difundir rápidamente la información entre las entidades pertinentes.

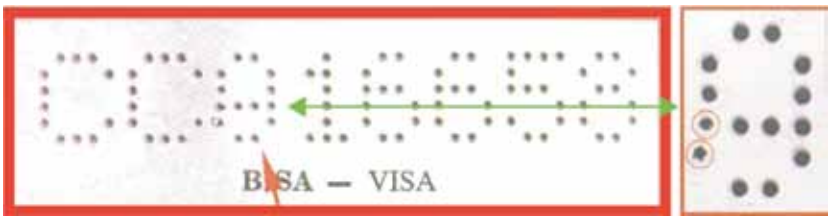


Figura 2-2
Manipulación de una cifra. Añadiendo dos pequeñas perforaciones, el 9 se ha transformado en un 8. (Cortesía del *Serviço de Estrangeiros e Fronteiras* de Lisboa, Portugal)

■ 2.3 Lista de requisitos

Para confeccionar una lista de requisitos es preciso abordar todos los aspectos mencionados anteriormente. Cuanto más exhaustiva sea la información, más útil será la lista. La falta de información puede generar malentendidos y puntos débiles, es decir, riesgos. La idea de elaborar una lista de requisitos fue propuesta por van Renesse (Renesse Rudolf L. 2006). Las conclusiones que se extraigan en la etapa de inventario, junto con otros requisitos que debe cumplir el documento propuesto, han de quedar plasmadas en un documento con las especificaciones del producto, que debe formar parte de la lista de requisitos elaborada por o para la entidad promotora.

Tal lista de requisitos puede ser exhaustiva, lo que significa que no podrá hacerse ningún cambio ni modificación adicionales durante el proceso de elaboración. Ahora bien, la complejidad de la cadena podría llamar la atención hacia aspectos nuevos durante el proceso de elaboración que exijan cambios o adiciones. Una lista de requisitos sirve para especificar cuándo debe cumplir el producto un requisito concreto y el modo en que ello ha de ser evaluado.

Confeccionar esa lista exige un esfuerzo considerable por parte de la entidad contratante, pero su importancia es crucial, pues la obliga a adoptar un enfoque estructural, que exige un examen de la utilidad y necesidad de cada requisito, de forma tal que la información obtenida en la etapa de inventario quede integrada en el proyecto final. También garantiza que cada uno de los requisitos sea formulado de forma inequívoca. Además, la lista ofrece un sólido punto de partida para que la parte contratante compare las soluciones que ofrecen los distintos productores.

Es evidente que confeccionar una lista completa de requisitos lleva tiempo. A menudo, hacer un inventario o elaborar una lista de requisitos lleva tanto tiempo como cumplir los requisitos en sí mismos, pues hay que revisar todo el proceso de desarrollo del producto definitivo, incluida la fabricación de materiales específicos, componentes y elementos adicionales de seguridad.

En la última etapa de la elaboración de la lista de requisitos, la entidad contratante podría decidir que desea que se haga un boceto para complementar dicha lista. Esto podría facilitar el proceso de toma de decisiones interno y la valoración de ofertas. El diseñador se elige en función de la lista de requisitos. Pero el boceto no sólo funciona como un indicador: ofrece cierto margen para posteriores adiciones y detalles, que en parte dependen de las posibilidades técnicas y de los resultados del desarrollo de producto del proveedor seleccionado.

2.3.1 Alcance y formato de la lista

La lista de requisitos sirve para varios fines. Así, por ejemplo, la parte promotora podría utilizarla para llamar a licitación, mientras el productor puede consultar la lista para decidir si le interesa el contrato y extraer la información necesaria a fin de hacer una propuesta. También le permite efectuar cálculos precisos y presentar una oferta competitiva en función de los mismos. Además, la parte promotora también puede utilizarla junto con la descripción de los requisitos para comprobar si un producto se ajusta a la descripción.

La lista de requisitos se asemeja a un libro exhaustivo, donde se especifica claramente el tipo de producto que hay que realizar y los requisitos específicos que deben cumplirse. Permite a la parte promotora elaborar una descripción muy estructurada y detallada del producto y los servicios deseados. Así, se distinguirán y especificarán los requisitos primarios y los secundarios. Una marca de agua multitono o determinado tipo de hilo de seguridad, podrían ser algunos de los elementos que un documento de seguridad "debe tener", mientras que las fibrillas de seguridad o papel testigo podrían figurar entre los elementos que "debería tener". Si bien algunos de los requisitos son optativos, podría ocurrir que la entidad expedidora prefiera tenerlos. El productor deberá decidir si desea encontrar un modo creativo de satisfacer esos deseos. No obstante, si no lo hiciera, ello no sería razón suficiente para rechazar un encargo.

La lista de requisitos indica cuáles son las normas internacionales que se aplican al documento que vaya a elaborarse. Por lo general, un

nuevo documento de viaje debe cumplir las normas de la Organización Internacional de Normalización (ISO) y la Organización de Aviación Civil Internacional (OACI) en cuanto a dimensiones, lectura mecánica, etc. La lista también debe indicar cuáles son los métodos de prueba que se utilizarán durante el proceso de elaboración y qué métodos de prueba se aplicarán con relación a los requisitos que no estén incluidos en las normas anteriormente citadas. En particular, la evaluación de la resistencia al fraude (falsificación y alteración) y las cualidades de uso del documento no deberán estar por debajo de las especificaciones para documentos internacionales y de las normas del sector. La parte contratante podrá indicar cuáles son los organismos públicos pertinentes a quienes hay que dirigirse para efectuar esa evaluación, cuál va ser el método de evaluación, y en qué momento se considerará que el documento es aceptable.

Junto con las especificaciones físicas y las limitaciones de uso del documento, la lista de requisitos también debe proporcionar indicaciones en materia de cantidad, plazos de elaboración y producción, materiales, componentes, equipos de producción y procesos logísticos pertinentes. También hay que abordar aspectos relativos a las garantías deseadas por la parte contratante en materia de seguros y continuidad del proceso de producción durante la vigencia del contrato. En función de la naturaleza del encargo, el cliente puede pedir que se mantengan existencias reguladoras de materiales y componentes, duplicación, almacenamiento custodiado de los registros electrónicos y las películas utilizadas en la producción de los documentos y, en los casos de centralización e individualización, podría pedir que haya provisiones de reserva o que se produzca en varias ubicaciones, con o sin capacidad de reserva.

2.3.2 Definición del producto

Antes de dar la orden de producción, es necesario realizar una descripción exhaustiva de lo que se espera del producto. Las especificaciones de los requisitos deben formularse de forma tal que haya margen para alternativas, para que el producto pueda beneficiarse de los últimos avances en materia de técnicas de producción y materiales. Si las especificaciones son demasiado rígidas, existe el riesgo de que el

producto final no pueda adaptarse con posterioridad para responder ante nuevas amenazas de los falsificadores.

Una vez que se haya decidido qué tipo de documento va a elaborarse, es esencial que todos los requisitos técnicos que debe cumplir dicho documento se incorporen a la lista. Eso no sólo afecta a la composición material del documento físico, sino también a su personalización.

También debe reflexionarse detenidamente sobre las posibilidades de desarrollo del documento en una etapa posterior. En algunos casos, el organismo expedidor podría tener previsto efectuar cambios en su producto con posterioridad. Por consiguiente, es fundamental llegar a un acuerdo sólido con el productor antes de iniciar el proceso de producción. Si el potencial de desarrollo de un documento se especifica insuficientemente antes de poner en marcha la producción, podrían surgir problemas graves más adelante (por ejemplo, problemas legales con relación a lo dispuesto en la licitación). Podría ocurrir que el productor entregara el producto inicial, pero que no fuese capaz de llevar a cabo un desarrollo posterior según lo previsto por la parte promotora. Ello equivaldría a encargar el producto erróneo. A veces los productos se piden asumiendo que se utilizará determinado equipo en el proceso de inspección. Si no se compra ese equipo para la etapa de inspección, nuevamente el producto será defectuoso.

Otra cosa que hay que considerar es el tipo de proceso de expedición que vaya a seguirse. Los sistemas de personalización centralizada ofrecen muchas ventajas, pues todos los recursos pueden concentrarse en un único lugar o en un número limitado de lugares. Los procesos de expedición centralizados disponen de equipos más sofisticados y costosos que los procesos de expedición descentralizados; si la producción es homogénea y está muy estandarizada, el riesgo de robo de documentos en blanco se reduce al mínimo.

Si se elige un sistema de expedición centralizado, por ejemplo, para un pasaporte nacional, es fundamental que se decida cuáles van a ser los requisitos de seguridad de un pasaporte provisional. De lo contrario el problema de la falsificación se trasladará a otro documento.

2.3.3 Apoyo en la elaboración de la lista de requisitos

La parte promotora sólo desarrolla un nuevo producto de forma periódica. Eso significa que no puede esperarse que cuente con los conocimientos técnicos necesarios para realizar un encargo por sí sola, y, por tanto, es posible que solicite la ayuda de asesores. Ahora bien, es esencial que la parte promotora tenga la seguridad absoluta de que el asesor es un experto con experiencia. Si el laboratorio nacional forense u otro organismo análogo, revisa y supervisa cada propuesta, y propone la mejor opción desde el punto de vista forense, también deberá consultarse a las partes que intervienen en materia de la inspección.

■ 2.4 Gestión del proyecto

La ejecución de grandes encargos también entraña riesgos para el productor. Normalmente, antes de que el productor reciba la orden de iniciar la producción de un documento, la parte promotora y el productor han examinado el proyecto reiteradamente y en profundidad. Han de tenerse en cuenta los aspectos siguientes:

- cooperación y coordinación
- producto y costo
- planificación y modificaciones

Todos ésos son riesgos que deben considerarse antes de que se dé la orden de iniciar la producción. Una vez que ésta esté en marcha, el documento se someterá al proceso de desarrollo especificado en el pliego de condiciones de la licitación y la lista de requisitos. Interferir en el proceso en una etapa posterior entraña riesgos y debe evitarse en la medida de lo posible.

2.4.1 Equipo de desarrollo del documento

Una vez que la parte promotora elige un proveedor y un diseñador artístico, se plantea la cuestión de cómo integrar lo mejor posible la lista de requisitos, por un lado, y el concepto de producto y el diseño artístico, por otro. El objetivo fundamental es elaborar un documento

de un modo eficaz y estructurado. Para ello hay que crear un pequeño equipo profesional de desarrollo de documento, que, en teoría, debe estar integrado por un representante de la parte promotora, el diseñador artístico y el desarrollador de producto del proveedor. Para ser eficaz, el equipo de desarrollo debe tener una actitud respetuosa y abierta hacia las cualidades de los distintos miembros que lo integran y compartir el objetivo de lograr el mejor resultado posible para la parte promotora. Los miembros del equipo también deben tener creatividad y ser capaces de trabajar juntos para resolver los problemas que se vayan presentando.

La parte promotora actúa como presidente y ha de estar capacitada para adoptar decisiones con el fin de que el desarrollo sea rápido y eficaz. Para hacer esto con responsabilidad, el representante de la parte promotora debe contar con conocimientos especializados en materia de uso y producción de documentos. Del mismo modo, el diseñador artístico debe ser capaz de transformar el concepto de producto elegido en el diseño deseado, integrando adecuadamente los requisitos que afectan a la seguridad del documento y a un uso ergonómico del mismo. Por otro lado, el desarrollador del producto debe contar con los conocimientos técnicos y estructurales necesarios para llegar al producto final, además de conocer en detalle el concepto del producto y la lista de requisitos.

El equipo de proyecto planifica, gestiona y supervisa el proceso de elaboración. Este equipo está guiado por el plan de proyecto del proveedor, donde se especifican los plazos de que se dispone para las distintas etapas del desarrollo del documento. El equipo de proyecto planifica junto con el productor la frecuencia de las reuniones, el modo en que se notifican los progresos realizados y las medidas adoptadas para que se efectúen los contactos bilaterales necesarios entre el diseñador y el especialista técnico.

En esa etapa, es primordial que haya una gran apertura y se intercambie información para que todos los miembros del equipo puedan avanzar partiendo del mismo nivel de conocimientos. La parte promotora proporciona la información necesaria, explica la lista de requisitos y subraya los aspectos que considera importantes. El diseñador artístico presenta su visión del documento y su uso, y aclara el concepto en que

se basa su diseño. Lo ideal es que el proyecto de diseño sirva para guiar el desarrollo posterior del concepto del producto y permita, a su vez, desarrollar más a fondo el diseño en función de la tecnología elegida por la parte promotora. El desarrollador de producto deberá facilitarle información detallada sobre el concepto de producto en que inicialmente se basó el encargo. Esto incluye los materiales y técnicas elegidas, las posibilidades de seguridad y la visión del desarrollador del producto respecto de cómo pueden integrarse los distintos elementos en el mismo.

La maqueta preparada por el productor ofrece una interpretación visual de las distintas posibilidades; en esa etapa, es muy útil poder visualizar el producto final. Por otro lado, al diseñador se le brinda la oportunidad de adquirir un conocimiento preciso de las técnicas y métodos con que cuenta la empresa, visitando el departamento de producción y el personal del proveedor, entre otros. Hay que recalcar que es importante conocer los parámetros de producción durante la producción en serie, los resultados de las pruebas realizadas durante el desarrollo del concepto del producto y, en particular, las posibilidades de convertir el proyecto de diseño en un producto seguro. Los proveedores de los distintos materiales deben participar en las primeras etapas del desarrollo del diseño gráfico.

2.4.2 Producto y costos

El productor debe tener una idea clara de las especificaciones a que ha de ajustarse el producto, así como las personas y los medios que deberá emplear para alcanzar ese objetivo. Antes de iniciar el desarrollo del producto, la parte promotora debe tener una idea muy clara del tipo de producto que desea y de cuánto costará. Entonces, las partes podrán acordar un precio adecuado y planificar la operación en función de los requisitos del cliente. Cualquier modificación posterior, inevitablemente afectará al precio y los plazos de entrega.

2.4.3 Planificación y gestión de cambios

A menudo el productor se encuentra en una situación incómoda: por un lado, desea satisfacer al cliente, pero, por otro, debe proteger los

intereses de su empresa. Además, suele llevar mucho tiempo aceptar pedidos de gran envergadura que implican la fabricación de productos importantes y complejos. La parte promotora, que tiene menos experiencia en grandes pedidos, con frecuencia cree que hay tiempo de sobra para proponer cambios. Es posible hacer cambios, pero siempre hay que analizar sus efectos. Sería desafortunado para ambas partes descubrir que una modificación ha provocado un fallo. También hay que examinar cualquier modificación realizada con posterioridad que afecte al precio o a los aspectos técnicos, así como sus efectos en la planificación. Cabe señalar que pequeñas alteraciones suelen tener efectos importantes en la planificación. Si se aceptan los cambios, sus efectos en la planificación tienen que ser claros y aceptables para la parte promotora.

■ 2.5 Cuestiones esenciales

La parte promotora, que está integrada principalmente por las autoridades que expiden el documento, debe ser consciente de lo que implica elaborar un nuevo documento. Los aspectos siguientes son esenciales:

- aceptación pública del documento
- verificabilidad del documento
- riesgo político si el producto es desprestigiado

Estas "cuestiones sutiles" deben tenerse presentes a la hora de adjudicar el contrato. Una vez adjudicado, el productor procederá a elaborar el documento basándose en su propuesta y cotización.

2.5.1 Aceptación pública

Generalmente, se subestima el riesgo que se corre al encargar un producto que no es aceptado por la ciudadanía. Las autoridades expedidoras y los clientes no deben despreciar las opiniones de los futuros usuarios. Con frecuencia, ciertos organismos de expedición asumen erróneamente que saben lo que piensan los usuarios sobre sus productos, y, como resultado, éstos simplemente ignoran el producto en cuestión. Ese riesgo puede ser menos importante en el caso de productos con una vida útil corta, pero no debe pasarse por alto.

Por ejemplo, poner en circulación un producto que no tenga aceptación por el público puede ser desastroso. A finales de la década de 1990, varias instituciones financieras de los Países Bajos pusieron en circulación diferentes tarjetas bancarias, que dieron origen a los productos "*Chipper*" y "*Chipknip*". Esas tarjetas contenían un microprocesador que el usuario podía utilizar además de la banda magnética tradicional. Sin embargo, por una u otra razón, los titulares de tales tarjetas se negaron a utilizar el microprocesador. Eso hizo que las tarjetas "*Chipper*" y "*Chipknip*" tuvieran que ser sustituidas por una tarjeta bancaria que aceptara el público. Una operación de esas características puede tener enormes consecuencias financieras, dado el desprestigio sufrido por las organizaciones expedidoras y el despilfarro de dinero.

En el caso de la administración pública, que a menudo tiene el monopolio de la expedición de determinados documentos para los que no hay productos alternativos o competidores, es importante que se tenga en cuenta a la opinión de la población a la hora de desarrollar un documento. Si el gobierno elabora un producto que satisface los deseos de los ciudadanos, lo más probable es que se sientan orgullosos de éste y tengan una actitud más favorable.

2.5.2 Controlabilidad

Diseñar y producir un documento seguro es sumamente importante y no debe tomarse a la ligera. Es un proceso que se rige por normas y procedimientos aceptados internacionalmente, que abarcan la totalidad del proceso. Esas normas garantizan el mejor control posible de los documentos de identidad y de viaje, y de los permisos de residencia, con independencia de la nacionalidad, el tipo y el modelo, o el lugar donde se realice la inspección o verificación.

El actual estado de la tecnología a menudo permite a los productores equipar a los productos con los últimos avances tecnológicos. Esas aplicaciones tienen por objetivo aumentar la seguridad de los documentos. Aunque muy atractivos, su verdadera utilidad debe evaluarse en función de la cadena del documento. Por consiguiente, importante determinar de antemano qué ofrece cada una de las aplicaciones y qué aporta en términos de seguridad.

La eficacia y el desempeño de un documento seguro también dependen del grupo destinatario. Podríamos distinguir entre dos grupos de destinatarios: entidades que necesitan comprobar información personal para prestar un servicio y el ciudadano de a pie. Un estudio realizado por el Banco de los Países Bajos (de Heij, 2000) reveló que el público, que también incluía a los inspectores, únicamente es capaz de recordar algunos de los rasgos del documento. Sería conveniente que los desarrolladores de documentos consideraran las restricciones que afectan ambos grupos destinatarios.

A. Los organismos

Los primeros organismos que nos vienen a la mente son las autoridades policiales, los servicios de inmigración, las empresas de transporte y las líneas aéreas, los servicios administrativos locales y regionales, las instituciones bancarias y financieras, etc. A ese respecto, también hay que tener en cuenta los factores siguientes:

- los materiales de referencia y el equipo disponibles para verificar la autenticidad de un documento
- la logística y las condiciones físicas de trabajo en que se llevan a cabo las inspecciones
- los riesgos de fraude mencionados anteriormente

Además, hay que recordar que cada uno de los grupos destinatarios mencionados *supra* requiere distintos métodos de capacitación y redes de información, así como prácticas y procedimientos bien diferenciados para afrontar los problemas. Ahora bien, en el caso de cada uno de los grupos no sólo es esencial que los documentos sean seguros y fiables, sino que, en caso de duda, sea posible hacer un examen forense.

B. Los ciudadanos

Si bien la formación es una cuestión fundamental para las entidades anteriormente citadas, lo más importante para el ciudadano de a pie es recibir información exacta. Independientemente de la manera en que se facilite la información, ésta siempre debe ser precisa, concisa, oportuna, actualizada y basada en la "necesidad de saber". Aunque ese último principio se aplique a ambos grupos destinatarios, es particularmente pertinente para los ciudadanos, dado el enorme número de personas afectadas.

Ante todo, el suministro de información debe potenciar la confianza de la población en el sistema e inducirla a contribuir al bienestar común y la seguridad de la sociedad. La información facilitada debe limitarse a los rasgos más elementales de seguridad (primer nivel de seguridad), y a los datos básicos relativos al valor legal del documento.

El objetivo primordial es que, siempre que exista sospecha, la parte o partes interesadas sepan a dónde dirigirse, cómo actuar, con quién hablar, etc., siempre y cuando la infraestructura de apoyo oficial esté en marcha. A fin de cuentas, la existencia de canales de información y estructuras adecuadas contribuirán a optimizar el sistema.

2.5.3 Riesgo político

La administración pública es la única responsable de la puesta en circulación de determinados productos. Desde un punto de vista económico, ese monopolio puede ser interesante, pero tal posición a menudo entraña enormes riesgos. Productos como los billetes bancarios y los documentos de identidad reciben una gran atención política, de forma que si algo falla, la tensión es inevitable. El "*Paspoortaffaire*"[1] holandés es un ejemplo de ello. En 1984, el Gobierno holandés empezó a desarrollar un nuevo pasaporte europeo antifraude. El contrato fue adjudicado a una empresa mixta integrada por tres entidades: Kodak, Elba (una empresa de artes gráficas) y Philips. Juntas formaron la sociedad de riesgo compartido KEP. Cuatro años después se puso de manifiesto que KEP no era capaz de cumplir con sus obligaciones. La consiguiente investigación parlamentaria buscó las razones del fracaso y descubrió que el proceso de toma de decisiones relacionado con el pasaporte tenía defectos y no funcionaba. Todo ello dio lugar a la dimisión de dos ministros (*Parlementair Documentatie Centrum*, 2006).

La entidad promotora debe ser consciente de los riesgos políticos que entrañan determinadas decisiones. Es, pues, esencial que haya un equilibrio adecuado entre las decisiones adoptadas y la creación de una base de apoyo suficiente. A veces esto puede generar conflictos de intereses entre la parte promotora y el productor. Así, por ejemplo,

Figura 2-3
Prototipo del pasaporte holandés antifraude de KEP
(Cortesía de Fons Knopjes, Países Bajos)

una decisión que en principio parece lógica por razones técnicas, podría valorarse de un modo muy diferente si la propuesta se enfrenta a resistencia. En tales casos, es aconsejable que la parte contratante aumente el apoyo para esa propuesta, o, si no, considere una solución alternativa.

Proponer técnicas o materiales que no gozan de apoyo suficiente podría provocar riesgos políticos, con independencia de lo justificadas que estén las aplicaciones propuestas desde el punto de vista técnico de la producción y la seguridad.

■ 2.6 Normas

En toda la historia de los documentos seguros, no hubo una necesidad aparente de normalización internacional de los documentos de identidad y de viaje expedidos por un gobierno hasta recientemente. Sin embargo, el aumento de los viajes internacionales por aire, mar y carretera exige que sea necesario tramitar con mayor velocidad la identidad de las personas que cruzan las fronteras internacionales. También se estima necesario que la policía de tráfico pueda inspeccionar con eficacia un

permiso de conducir expedido por otro país, posiblemente en un idioma diferente al suyo. Esas necesidades fueron detectadas en un principio por los órganos pertinentes de las Naciones Unidas.

2.6.1 Introducción de normas internacionales para los documentos expedidos por el gobierno

El primer intento de llegar a un acuerdo sobre un estilo uniforme en los pasaportes se remonta a principios del siglo XX. El Comité de disposiciones sobre comunicaciones y tránsito de la Sociedad de las Naciones en Ginebra convocó una conferencia internacional sobre pasaportes, trámites de aduana y pasajes en 1920. El Comité preparó una resolución que se adoptó en octubre de 1920 y fijaba la fecha para introducir el nuevo pasaporte normalizado en julio de 1921. El documento consistía en un cuadernillo de 15,5 cm por 10,5 cm, con 32 páginas numeradas y en al menos dos idiomas (la lengua nacional y el francés) (Lloyd, 2003).

En el caso de los documentos de viaje, las Naciones Unidas elaboraron dos convenios tras la Segunda Guerra Mundial con el fin de establecer los derechos de los refugiados y los apátridas. La Convención de las Naciones Unidas sobre el Estatuto de los Refugiados, adoptada el 28 de julio de 1951, establece que "los Estados Contratantes expedirán documentos de identidad a todo refugiado que se encuentre en el territorio de tales Estados y que no posea un documento válido de viaje" (Artículo 27) y "[…] expedirán a los refugiados que se encuentren legalmente en el territorio de tales Estados documentos de viaje que les permitan trasladarse fuera de tal territorio […]" (Artículo 28). En el Anexo A de la Convención se definen las características del nuevo documento de viaje para los refugiados. El documento lleva dos bandas en el ángulo superior derecho de la portada.

En cierto modo, ese documento de viaje para refugiados es sucesor del pasaporte Nansen utilizado en la década de 1920 e introducido por Fridtjof Nansen, diplomático noruego y antiguo Alto Comisionado para los Refugiados de la Sociedad de las Naciones, a quien se le concedió el premio Nobel de la Paz en 1922 por su labor humanitaria. En 1954, las Naciones Unidas adoptaron la Convención sobre el Estatuto de

los Apátridas, que se ocupa de la expedición de los documentos de identidad y de viaje de las personas apátridas en la misma medida que la Convención de 1951. La cubierta de este tipo de documento lleva las palabras "documento de viaje" en inglés y francés (y a menudo en el idioma del país expedidor) junto con la fecha de la Convención.

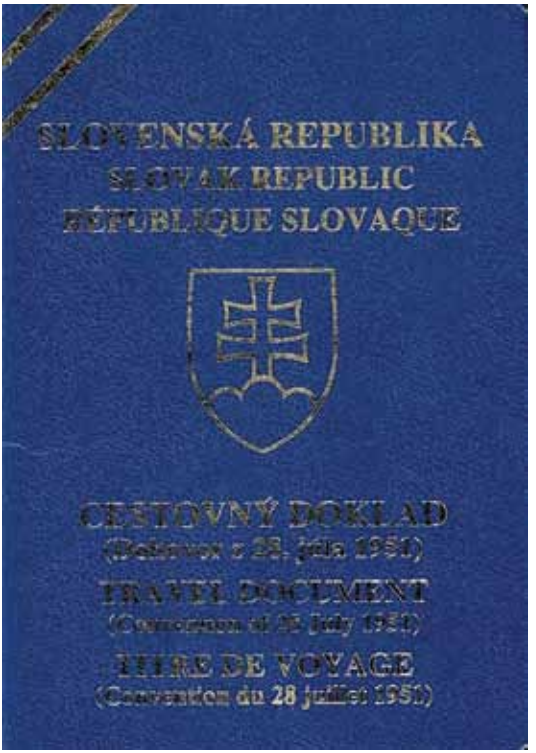


Figura 2-4
Documento para refugiados de la República de Eslovaquia
(Cortesía del Servicio Nacional de Inteligencia Criminal, Países Bajos)

Los permisos de conducir también fueron objeto de un proceso parcial de normalización internacional tras la Segunda Guerra Mundial. Las Naciones Unidas celebraron una reunión sobre transporte en 1949 y de nuevo en 1968. Esas reuniones abarcaron un amplio espectro de cuestiones relativas al transporte, incluidos los permisos de conducir, y dieron origen a dos convenios. Ambos convenios concibieron el

permiso de conducir como un cuadernillo donde figurarían los datos del conductor, los distintos tipos de vehículos que éste estaba autorizado a conducir y cualquier requisito especial, como llevar gafas. El problema del idioma fue resuelto presentando los datos del conductor según una secuencia preestablecida y los tipos de vehículos y los requisitos especiales mediante símbolos estándar. La Convención de 1949 establecía que el permiso de conducir debía ser de color rosa. Se pidió a los Estados que expidieran permisos con un diseño nuevo que lo presentaran a una agencia de mantenimiento de las Naciones Unidas con sede en Ginebra para su aprobación.

2.6.2 La Organización de Aviación Civil Internacional y los documentos de viaje

El Convenio sobre Aviación Civil Internacional, firmado en Chicago en 1944 por 52 Estados, establece la Organización de Aviación Civil Internacional (OACI), con sede en Montreal, con el fin de promover la cooperación internacional y el máximo grado de uniformidad en materia de reglamentos, normas y procedimientos, así como en el modo en se organizan los asuntos de la aviación civil (OACI, 2006). En la década de 1970, los viajes aéreos empezaron a hacerse más frecuentes, y la OACI empezó a preocuparse por los retrasos sufridos en los aeropuertos debido al tiempo que los inspectores necesitaban para examinar una amplia variedad de pasaportes de tamaños diferentes y con distintas formas de presentar los datos relativos al titular, su nacionalidad y su derecho a entrar en el país de destino. Como consecuencia, la OACI creó un grupo consultivo técnico sobre documentos de viaje (TAG-MRTD), al prever la necesidad de simplificar la tramitación de los documentos de viaje por los servicios de inmigración.

En 1980, la OACI estableció una norma para los pasaportes de lectura mecánica, conocida como el Documento 9303 de la OACI (posteriormente denominada OACI Doc 9303 parte I). Ese documento proponía un pasaporte de tipo tarjeta, como el que ya había sugerido la OACI 20 años antes en la conferencia de las Naciones Unidas sobre pasaportes y trámites fronterizos. El formato tarjeta nunca fue adoptado, principalmente porque los gobiernos insistieron en que había que reservar un espacio en el documento para poner los visados.

Los esfuerzos realizados con miras a desarrollar esa norma inicial se toparon con un obstáculo importante, pues varios países tenían leyes de confidencialidad que impedían exigir a sus ciudadanos que llevasen documentos con información sobre sí mismos que no pudieran ver. Esto, junto con la tecnología disponible entonces, hizo que se optara por el reconocimiento óptico de caracteres para leer los datos de lectura mecánica. Cualquier ciudadano podrá comprobar fácilmente la información contenida en las dos líneas de caracteres OCR-B de la zona de lectura mecánica del pasaporte, siempre y cuando el formato de los datos sea explicado.

Posteriormente, la OACI amplió sus normas para incluir visados de lectura mecánica de dos tamaños (OACI Doc 9303 Parte 2) y lo que ahora se conoce como documentos oficiales de identidad utilizados para viajar, que son tarjetas de dos tamaños que pueden utilizarse en viajes transfronterizos acordados entre gobiernos (OACI Doc 9303 Parte 3). Si bien aún no hay ningún país que haya expedido un pasaporte en forma de tarjeta únicamente, está claro que éste podría ser el pasaporte del futuro. Se conservó el uso en caracteres OCR-B como medio de registrar información con el fin de que todos los documentos pudieran ser leídos por un único tipo de lector. Los datos se presentan en dos líneas, y el número de caracteres varía en función del tamaño del documento, a excepción del documento oficial de identidad de menor tamaño, donde los datos OCR-B están contenidos en tres líneas.

La tarjeta más pequeña, conocida como “Tamaño 1”, es similar a la ID-1, pero su tolerancia dimensional es mayor en su forma básica. Ello permite variaciones cuando, por ejemplo, la tarjeta se monta en una oficina donde no se dispone del equipo de perforación de alta precisión que normalmente se utiliza para hacer las tarjetas de formato ID-1. Ahora bien, si la tarjeta está dotada de un sistema adicional de almacenamiento de datos que exige que ésta sea insertada en un lector, se aplicarán las especificaciones dimensionales más estrictas de la ID-1.

Las normas para los documentos de viaje de lectura mecánica están publicadas en el Documento 9303 de la OACI y constan de tres partes:

- Parte 1 Pasaportes de lectura mecánica, volúmenes 1 y 2
- Parte 2 Visados de lectura mecánica
- Parte 3 Documentos de viaje oficiales de lectura mecánica que pueden utilizarse para viajes transfronterizos

La sexta edición de la parte 1 (volumen 1, Pasaportes con datos de lectura mecánica almacenados en formato de reconocimiento óptico de caracteres, y volumen 2, Especificaciones de los pasaportes electrónicos con capacidad para identificación biométrica) fue publicado en 2006; la Parte 2 fue publicada en 2005, y una segunda edición de la Parte 3 en 2002. Las normas para los certificados de los miembros de la tripulación se han incluido en un Anexo especial a la segunda edición de la Parte 3, publicada en primavera de 2002.

Durante una reunión celebrada en Nueva Orleans, en marzo de 2003, el Grupo de Trabajo de la OACI sobre Nuevas Tecnologías (NTWG, por sus siglas en inglés) preparó una resolución donde se establecía que la imagen facial era el principal elemento de identificación (incluso en el caso de imágenes faciales almacenadas digitalmente) y abrió la posibilidad a que los Estados miembros de la OACI pudieran utilizar huellas dactilares e imágenes del iris normalizadas y almacenadas digitalmente como biometría adicional interoperable a nivel mundial para reforzar la verificación o identificación asistida por maquinas. Además, el Grupo de Trabajo pidió que utilizaran circuitos integrados (CI) sin contacto como medio para almacenar información digital. La Resolución fue adoptada en la 14ª Reunión del TAG-MRTD (2003).

En su siguiente Reunión (TAG-MRTD 15, 2004) se eligió un símbolo para el pasaporte electrónico.

A raíz de varias decisiones adoptadas por el TAG/MRTD en los últimos dos años, la sexta edición de la Parte 1 del documento 9303 ha sido totalmente reestructurada. El documento se divide en dos Partes: la primera proporciona las especificaciones para el pasaporte de lectura mecánica básico, mientras que la segunda presenta las especificaciones

necesarias para convertir ese pasaporte en un pasaporte electrónico (despliegue de la biometría, estructura lógica de los datos, infraestructura de clave pública (ICP).

Las ventajas de la interoperabilidad planetaria podrán facilitar la tramitación segura de la inmigración, únicamente si se aceptan de forma generalizada. El papel de la OACI es asistir y asesorar a los Estados miembros en la implantación de las normas elaboradas.

En marzo de 2007, se decidió que el TAG-MRTD debía formar dos grupos de trabajo para realizar el minucioso trabajo encomendado por el TAG-MRTD. Los dos grupos son el Grupo de Trabajo sobre Nuevas Tecnologías (NTWG) y el Grupo de Trabajo sobre la Implantación Universal de Documentos de Viaje de Lectura Mecánica (UIMRTDWG, por sus siglas en inglés).

El Grupo de Trabajo sobre la Implantación Universal de Documentos de Viaje de Lectura Mecánica debe ayudar a la Secretaría a implantar el proyecto en los Estados, en particular en materia de formación, asistencia técnica y fuentes de ayuda financiera en el marco del proyecto de implantación universal de los documentos de viaje de lectura mecánica, con el fin de cumplir el plazo que vence en 2010, y llevar a cabo actividades de creación de capacidad de proyección exterior en colaboración con los Estados, otras organizaciones internacionales y el sector privado.

El Grupo de Trabajo sobre Nuevas Tecnologías debe examinar todos los aspectos de las nuevas tecnologías que puedan ser de utilidad para los documentos de viaje. Evalúa las tecnologías y recomienda las que considera adecuadas para su inclusión en futuras ediciones o enmiendas del documento 9303 de la OACI. En los últimos años, esa labor ha incluido el endurecimiento de las normas relativas al retrato del titular; además, ha introducido normas de seguridad mínimas recomendadas. Su trabajo actual incluye el desarrollo de un medio normalizado de identificación biométrica de los titulares de los documentos de viaje, sistemas de almacenamiento de datos biométricos en el documento, y métodos mediante los cuales el documento de viaje puede ser autenticado

por medios mecánicos. Eso supone la manipulación y almacenamiento de importantes cantidades de datos. Se ha creado una Estructura Lógica de Datos (ELD) para que los Estados puedan registrar la información de forma normalizada con el fin de que otros Estados puedan acceder a ella fácilmente.

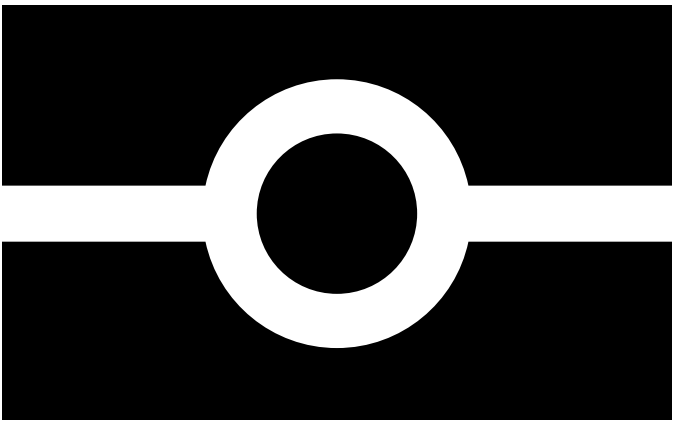


Figura 2-5
Símbolo de la OACI en documentos de viaje electrónicos
(Cortesía de Sdu Identification, Haarlem, Países Bajos)

2.6.3 Organización Internacional de Normalización

La Organización Internacional de Normalización (ISO), con sede en Ginebra (Suiza), elabora normas relativas a prácticamente todos los campos de la actividad humana. La mayoría de los países cuenta con un órgano nacional de normas, asociado a la ISO. La mayor parte de las normas de la ISO son establecidas por grupos de trabajo compuestos por miembros de un sector concreto. Los especialistas que integran esos grupos suelen ser empleados de empresas industriales cuya actividad se desarrolla en la producción y el uso de los productos objeto de normalización. Normalmente, la necesidad de normalizar un tipo determinado de productos queda determinada por el subcomité de la ISO pertinente; posteriormente, se crea un grupo de trabajo con el fin de proponer una norma adecuada que satisfaga las necesidades de los productores y los usuarios del producto. No obstante, el grupo de trabajo puede preparar únicamente un proyecto de norma y proponer su

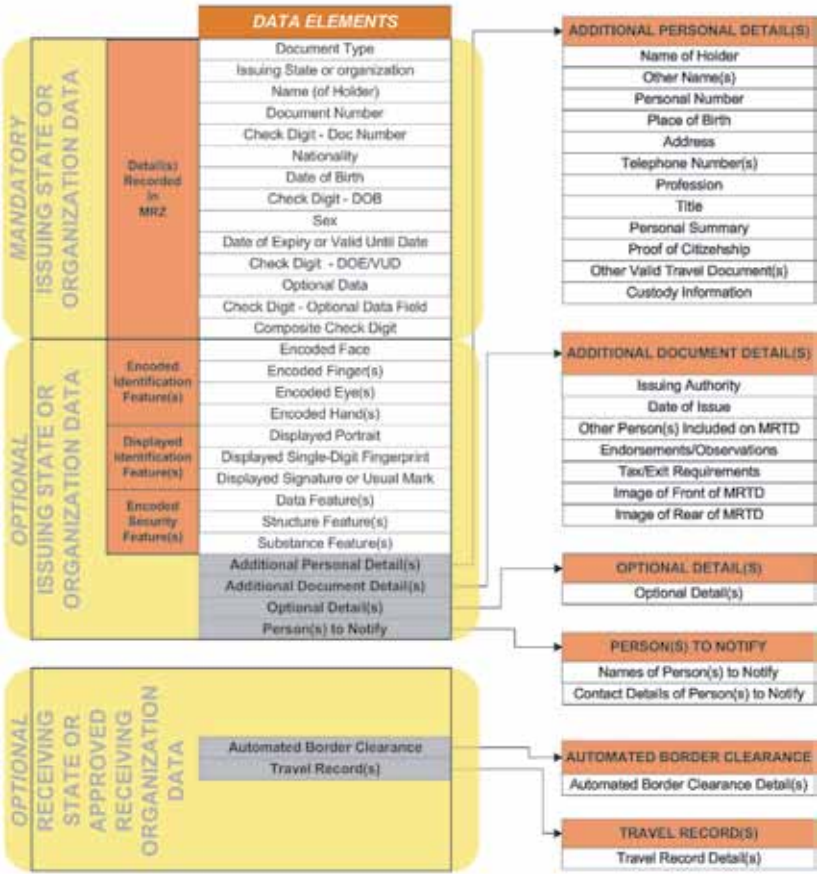


Figura 2-6
Estructura de datos lógicos de la OACI (Cortesía de la Organización de Aviación Civil Internacional, Montreal, Canadá) – ***Versión oficial de OACI***

adopción. Para convertirse en norma internacional, el proyecto debe someterse a una votación internacional en que los órganos de normas nacionales que cumplan las condiciones votan para apoyar, rechazar o enmendar la propuesta. Seguidamente, suele haber un periodo de deliberaciones en que se examinan las objeciones o reservas.

En algunos países, los documentos de viaje y los permisos de conducir también se utilizan como documentos de identidad. Ahora bien,

inicialmente la ISO concibió los documentos de identidad como tarjetas de plástico para transacciones financieras y transacciones conexas. La necesidad de normas internacionales en materia de tarjetas financieras se puso de manifiesto a medida que fue aumentando el uso de tarjetas de crédito a nivel internacional. Fue necesario elaborar normas relativas a sus dimensiones y otras propiedades físicas, crear sistemas de prueba para verificar esas propiedades y establecer la ubicación y estructura de los datos codificados almacenados en la tarjeta. Inicialmente, los datos codificados estaban grabados en relieve en la tarjeta. Posteriormente, se introdujeron las bandas magnéticas. Como cada tarjeta tiene un número específico, hubo que establecer un sistema para gestionar la emisión de los números. Y a medida que ha ido avanzando el almacenamiento de datos y ha pasado de una banda magnética a un microprocesador de contactos -algunos tipos de tarjetas ya utilizan microprocesadores sin contacto y memoria óptica – ha sido necesario acordar y aplicar normas adecuadas.

La participación de la ISO en los documentos de identidad expedidos por los gobiernos se produjo relativamente tarde, algunos años después de que se estableciesen las primeras normas sobre pasaportes y permisos de conducir. Aunque la primera norma de las Naciones Unidas para permisos de conducir se remonta a 1949, no fue hasta 1997 cuando la ISO empezó a participar. El interés de la ISO por los documentos de viaje se remonta a finales de la década de 1980, algunos años después de que la OACI publicase su primera norma. En un principio, el objetivo de la ISO se limitaba a examinar el documento de la OACI para ver si podían suscribirlo como norma ISO.

Como ya se ha mencionado, ambas normas fueron elaboradas bajo los auspicios de las Naciones Unidas. Una de las normas por las que se rigen los organismos de las Naciones Unidas es que los únicos que pueden ocupar un cargo en sus comités son los empleados del gobierno. Cuando se elaboraron las normas originales, los gobiernos concernidos tenían empleados que intervenían en la expedición y el uso de los documentos, además de la producción del documento, a través de las imprentas estatales. La situación ha cambiado considerablemente en los últimos años. Muchos gobiernos han privatizado sus imprentas, y debido a

ello, sus empleados ya no pueden tener un puesto en los comités de las Naciones Unidas. Muchos más Estados han empezado a intervenir, a menudo subcontratando la producción de sus documentos de identidad a imprentas de seguridad reconocidas. En la actualidad, las tecnologías que se contemplan son mucho más complejas y requieren verdaderos conocimientos especializados, de los que únicamente dispone el sector comercial. Esos conocimientos también pueden encontrarse en la estructura de la ISO. De modo que, si bien la participación inicial de la ISO en los documentos de viaje consistió en examinar las normas establecidas por los organismos especializados de las Naciones Unidas para determinar si podían refrendarlas, en este momento, la relación entre las organizaciones funciona en beneficio de todos.

A. DOCUMENTOS DE VIAJE

Con el fin de garantizar la disponibilidad de los conocimientos especializados pertinentes, la ISO funciona de acuerdo a una estructura integrada por comités, subcomités y grupos de trabajo que se ocupan de los distintos tipos de normas. El comité encargado de los documentos de identidad es el Comité Técnico Conjunto 1 (JTC1), del que depende el subcomité conocido como SC17. Aunque en la actualidad la ISO trabaja en documentos de identidad, su experiencia en el campo de las tarjetas financieras se refleja en el hecho de que el sindicato británico de pagos, la *Association of Payment and Clearing Services* (APACS), con sede en Londres, proporciona la Secretaría del SC17. El SC17 tiene su propio sitio Web, www.SC17.com.

Hay nueve grupos de trabajo que dependen del SC17, de los que el Grupo de Trabajo 3 (WG3), encargado de los documentos de viaje de lectura mecánica, y el Grupo de Trabajo 10 (WG10), encargado de los permisos de conducir de vehículos de motor, están relacionados con los documentos de identidad expedidos por la administración pública. No obstante, hay otros grupos de trabajo cuya aportación tiene interés para los documentos de viaje y los permisos de conducir, a saber:

- WG1: Características físicas y métodos de prueba para las tarjetas de identificación
- WG4: Tarjetas de contacto con circuito integrado (CI con contacto)

- WG8: Tarjetas sin contacto con circuito integrado (CI sin contacto)
- WG9: Tarjetas y sistemas de memoria óptica
- WG11: Aplicación de la biometría a las tarjetas y la identificación personal

Aunque los grupos de trabajo 1, 4, 8 y 9 hayan elaborado normas para las tarjetas financieras y los datos codificados en esas tarjetas diferentes respecto de lo que se necesita para los documentos de viaje o los permisos de conducir, el objetivo es hacer el mayor uso posible de las normas en vigor para los documentos de identidad expedidos por los gobiernos con esas tecnologías avanzadas. Los documentos de viaje y los permisos de conducir suelen tener un periodo de validez mucho mayor que las tarjetas financieras. Eso significa que los métodos de prueba de las tarjetas financieras únicamente pueden proporcionar una idea de su futuro funcionamiento.

Debido a que los códigos de barras se emplean en muchos ámbitos, aparte del de la identidad, un subcomité diferente, el SC31, se ocupa de los códigos de barras de una y dos dimensiones.

Todo el que participa en la elaboración de normas internacionales lo hace a tiempo parcial, utilizando el tiempo de trabajo de su empleador (gobierno o empresa). La labor del Grupo de Trabajo 3, que empezó siendo modesta, ha crecido para incluir los diferentes documentos de viaje que están elaborándose, la actualización de las normas para incorporar los nuevos avances, y proporcionar asistencia a los gobiernos que deseen introducir documentos de viaje de lectura mecánica. Para hacer frente a la creciente carga de trabajo, el Grupo de Trabajo 3 estableció, hace varios años, distintos equipos de tareas. El Equipo de Tareas 1 (TF1) sigue de cerca y evalúa los nuevos avances tecnológicos. El Equipo de Tareas 2 (TF2) fue creado originalmente para velar por la armonización entre diferentes partes del documento 9303 de la OACI, pero ahora supervisa la actualización de las normas y garantiza que se ajusten a las directrices de la ISO. El Equipo de Tareas 3 (TF3) proporciona asesoramiento a los gobiernos y se ocupa de los problemas derivados de convertir los caracteres nacionales al limitado conjunto de

caracteres permitidos en la zona de lectura mecánica de los documentos de viaje. El Equipo de Tareas 4 (TF4) tiene por objeto elaborar un protocolo de RF y una norma de pruebas para la aplicación de los pasaportes electrónicos y un protocolo para pruebas de durabilidad. Los dos protocolos tienen como objetivo mejorar la interoperabilidad de los pasaportes electrónicos y los lectores, y verificar la conformidad funcional con las normas de la ISO y las recomendaciones de la OACI (véase la sección 5.5.3 Compatibilidad con las normas). El Equipo de Tareas 5 (TF5) está trabajando en el área de la infraestructura de clave pública.

Si bien las reuniones del Grupo de Trabajo 3 solían centrarse en los detalles de cada aspecto de las normas, ahora son los equipos de tareas quienes se ocupan de esa labor. En la actualidad, las reuniones del Grupo de Trabajo 3 consisten en recibir y aprobar informes de la labor de los equipos de tareas, y en planificar estrategias para responder a los retos de lo que se ha convertido en un entorno en constante evolución.

B. Permisos de conducir

Al haberse creado con posterioridad, el Grupo de Trabajo 10 ha podido aprovechar considerablemente la experiencia de las actividades del Grupo de Trabajo 3. Muchos de sus miembros forman parte de ambos grupos. El Grupo de Trabajo 10 ha creado diez equipos de tareas sobre diversos temas. Al igual que el Grupo de Trabajo 3, hace un amplio uso de los conocimientos técnicos de los grupos de trabajo 1, 4, 8 y 9 de la ISO.

El SC17 de la ISO creó el Grupo de Trabajo 10 en una reunión en 1998. Al igual que con el Grupo de Trabajo 3, a las reuniones del Grupo de Trabajo 10 asisten empleados del gobierno y personal del sector empresarial. Japón, Sudáfrica y varios países europeos y norteamericanos están plenamente representados. La *American Association of Motor Vehicle Administrators* (AAMVA) desempeña un papel fundamental, y en la actualidad uno de sus miembros está actuando como coordinador del Grupo de Trabajo 10. La AAMVA representa a los organismos públicos expedidores de premisos de conducir de los Estados Unidos, el Canadá y México.

Solamente en Europa hay 640 permisos de conducir diferentes; en el mundo entero la cifra es enorme. El Grupo de Trabajo 10 ha empleado una cantidad considerable de tiempo tratando de hacer balance de las prácticas utilizadas en los distintos países del mundo con el fin de determinar el punto de partida para la elaboración de una norma.

Hay un documento que técnicamente queda fuera de la competencia del Grupo de Trabajo 10: el permiso internacional para conducir . Ese documento, reconocido por la Convención de las Naciones Unidas, se expide al titular de un permiso de conducir como prueba de que éste tiene permiso para conducir, lo cual queda establecido en una norma reconocida por las autoridades de otros países. En su forma actual se trata de un documento en papel al que se pega una fotografía del titular. No hay ninguna medida de seguridad contra la falsificación o la alteración fraudulenta. En muchos países la expedición del permiso internacional para conducir se subcontrata a entidades no oficiales, tales como las asociaciones automovilísticas.

El permiso internacional para conducir es deficiente en muchos aspectos. Sin embargo, es el único permiso de conducir reconocido internacionalmente. Por consiguiente, el Grupo de Trabajo 10 ha decidido preparar un proyecto de norma para un nuevo permiso de conducir internacional.

La nueva norma ISO 18013-1 establece el formato del diseño y el contenido de los datos de un permiso de conducir que se ajuste a las normas ISO, en lo tocante a las características de lectura humana (visuales) y la ubicación de las tecnologías de lectura mecánica ISO en la tarjeta. El permiso internacional para conducir con formato ID-1 tiene por objeto proporcionar un documento que sirva de lo que las autoridades otorgantes conocen como permiso de conducir nacional, y de permiso de conducir internacional. De ese modo, el permiso de conducir ajustado a las normas ISO supliría la necesidad de tener dos documentos diferentes. No obstante, los países que decidan conservar su diseño nacional específico podrán emitir una segunda tarjeta (con o sin tecnologías de lectura mecánica de la ISO), es decir, un permiso de conducir nacional, en tanto que el permiso de conducir ajustado a las

normas ISO únicamente sustituiría al actual documento en papel del permiso internacional para conducir (ISO, 2006).

2.6.4 Colaboración entre la OACI y la ISO

La OACI emite y supervisa las normas de los documentos de viaje de lectura mecánica. La función de la ISO con relación a esas normas es verificar que cumplen los estrictos requisitos establecidos por la ISO en materia de normas internacionales. El cometido original y primordial del Grupo de Trabajo 3 es velar por que las normas de la ISO sean observadas y recomendar a la Organización que apruebe las nuevas ediciones de cada parte del Documento 9303 de la OACI. Los distintos órganos de normas de los Estados miembros de la ISO votan para refrendar su aprobación. Si hay algún órgano que vote en contra, deberá explicar sus razones, que posteriormente serán examinadas, aun cuando el resultado de la votación haya sido positivo.

La aprobación de la ISO se plasma en la Norma ISO/IEC 7501 partes 1, 2 y 3. Se trata de un documento muy sencillo donde se deja constancia de la aprobación de las distintas ediciones de las partes 1, 2 y 3 del Documento 9303 de la OACI.

2.6.5 Actividades de normalización en la Unión Europea

A. Pasaportes, visados y permisos de residencia

En los últimos años, la Unión Europea ha establecido algunas normas propias. Al principio esas normas se fijaban con el propósito de dotar a los pasaportes de los Estados miembros de la UE de una "identidad corporativa". Posteriormente, las directivas europeas relativas a pasaportes, visados y permisos de residencia se han complementado con las normas de la OACI y la ISO mencionadas anteriormente con el fin de integrar las nuevas tecnologías y alcanzar la interoperabilidad planetaria.

En la década de 1980, Europa introdujo un diseño común para los pasaportes de lectura mecánica, que en gran medida se ajustaba a la norma de la OACI. Sin embargo, había un punto divergente, que se está

corrigiendo con una modificación a la norma de la OACI, en virtud de la cual el nombre del Estado expedidor y la palabra "pasaporte" debían figurar en el idioma pertinente en la parte superior de la página donde figuran los datos del pasaporte. El pasaporte europeo no se ajustaba a esto, pues la página anterior contiene el nombre del país expedidor y la palabra "pasaporte" en todos los idiomas comunitarios. La OACI, en consulta con los representantes de la UE, acordó modificar su norma para especificar que, cuando el nombre del Estado y la palabra "pasaporte" aparezcan en la página anterior a la página de los datos, no será necesario que se repitan en la página de los datos. Algunos Estados europeos han preferido observar ambas normas y facilitan esa información en ambas páginas

En la década de 1990, Europa introdujo un visado común de lectura mecánica conocido como el visado Schengen, que, en términos generales, se ajusta a la norma de la OACI salvo por el hecho de que el nombre del titular del documento aparece únicamente en la zona de lectura mecánica y no en la zona visual. Además, en el visado europeo original no se había previsto un lugar para la fotografía, lo que fue modificado con posterioridad. El hecho de que el nombre no aparezca en la zona visual no suele plantear problemas. Ahora bien, cuando el nombre se ha truncado para encajarlo en la zona de lectura mecánica o cuando se produce una transliteración para resolver el problema de los caracteres nacionales que no están permitidos en dicha zona, el nombre del titular no aparece correctamente escrito en ningún otro lugar del visado. Podría argumentarse que el nombre correcto figura en la página de datos del pasaporte donde está el visado.

Durante la reunión celebrada por el TAG en 2000, Alemania puso en marcha la normalización de las normas de seguridad contra la falsificación y alteración de los documentos de viaje. Los distintos gobiernos europeos celebraron varios debates que culminaron en el establecimiento de esa norma en 2001, que también fue adoptada por la OACI. En un momento dado, era necesario que el Documento 9303 de la OACI incluyera normas de seguridad más detalladas, pues en éste únicamente se advertía a los Estados expedidores de la necesidad de emitir documentos seguros, dejando la incorporación de elementos de

seguridad a decisión de cada uno de ellos, si lo estimaban necesario. El TAG-MRTD de la OACI pidió al Grupo de Trabajo sobre Nuevas Tecnologías y al Grupo de Trabajo sobre Contenido y Formato de Documentos (disuelto) que trabajaran en colaboración para preparar una norma de seguridad, tomando como base las normas de la UE. Esto dio lugar al Anexo de la sección III de la parte 1 del documento 9303 en su quinta edición.

Uno de los problemas era asegurar que la norma fomentase una evolución futura y no la obstaculizase. Un ejemplo de esto fue cuando la página que contiene los datos se colocó en la tapa del pasaporte. Esa estructura dio lugar al peor de los fraudes en un pasaporte, a saber, la sustitución de la fotografía, lo que se resolvió añadiendo una fotografía digital al microprocesador del pasaporte.

A principios de la década de 1990, la INTERPOL formuló una recomendación según la cual la página de los datos debía estar en el interior y no en la tapa del documento. Esa recomendación se convirtió en una norma de seguridad obligatoria en la Unión Europea. Colocar los datos en una de las páginas interiores tiene ciertas ventajas, pues cualquier intento de sustituir la fotografía impresa en bromuro u otros datos son mucho más difíciles; además, permite aumentar la seguridad mediante una marca de agua visible en el papel. Ahora bien, también tiene sus desventajas: la página de datos es menos robusta y puede dañarse más fácilmente cuando se presenta para su lectura, en particular si la lectura se efectúa por deslizamiento. Una vez que la página se arruga, existe la posibilidad de que la zona de lectura mecánica quede ilegible. Para resolver esto, a menudo la página se fabrica más robusta, lo que hace que sea más vulnerable a cualquier intento de sustituir la fotografía. Algunos gobiernos resuelven el problema adoptando sistemas mediante los cuales se colocan los datos en una tarjeta de plástico ID3 que se encuaderna al pasaporte. Así pues, la norma de seguridad de la OACI ofrece a los Estados expedidores la posibilidad de utilizar nuevas soluciones, garantizando, al mismo tiempo, que si se emplea la estructura de la cubierta tradicional se adopten las medidas de precaución pertinentes.

Más recientemente, la Unión Europea se ha beneficiado de las investigaciones realizadas por el Grupo de Trabajo sobre Nuevas Tecnologías de la OACI en materia de confirmación de identidad asistida por máquinas, y, en diciembre de 2004, el Consejo adoptó un reglamento para la implantación de la biometría en los pasaportes y los documentos de viaje de la UE. El 28 de junio de 2006, quedó establecida la segunda parte de las especificaciones técnicas. Se dio a los Estados miembros un plazo máximo para la aplicación del nuevo reglamento: 18 meses para la imagen facial (28 de agosto de 2006, fecha límite para su introducción en los documentos) y 36 meses para las huellas dactilares (28 de junio de 2009, fecha límite para su introducción en los documentos) (Unión Europea, 2006).

La Unión Europea también ha aprobado un reglamento que establece un formato uniforme para los permisos de residencia de ciudadanos de terceros países. El formato uniforme puede utilizarse en forma de pegatina o como un documento independiente. En el Anexo de ese reglamento se describe el diseño, la disposición, el contenido y los materiales que han de utilizarse en la fabricación de los permisos. Existen otras especificaciones técnicas secretas que definen las características de seguridad y los detalles de expedición.

B. Permisos de conducir

La Unión Europea ha colaborado estrechamente con las Naciones Unidas para promover la elaboración de un permiso de conducción común para Europa. Se trata de algo necesario, pues, en la actualidad, hay 640 permisos diferentes en uso en Europa, 84 de los cuales están siendo expedidos en este momento. La Unión Europea ha tenido que publicar un manual donde se muestran las 640 permutaciones.

A principios de la década de 1990, la Unión Europea recomendó, en su directiva 91/439/ECC del Consejo, la expedición de un permiso de conducir normalizado en papel. No obstante, el rápido crecimiento de las tarjetas de plástico dio lugar a que el Consejo emitiera una directiva, la 96/47/EC, para introducir una versión en forma de tarjeta. Esa directiva también hace referencia a la posible puesta en marcha de un sistema de almacenamiento de datos común, por ejemplo, mediante un

microprocesador. Con el fin de garantizar que, cuando se produzca tal implantación, haya interoperabilidad entre los Estados, se ha prohibido que los Estados empiecen a aplicar esa tecnología de forma unilateral. Pueden utilizarse códigos de barras, pero únicamente para duplicar la información que ya es legible en la tarjeta de forma visual o para facilitar el procedimiento de expedición.

La directiva especifica la información que debe incluirse sobre el Estado expedidor y el conductor, incluido un retrato. También se estipula que los distintos tipos de vehículos que el titular pueda conducir se indiquen mediante los símbolos de las Naciones Unidas. Además, se establecen especificaciones con respecto al color de fondo y al texto, así como a los colores del símbolo de la Unión Europea.

El color de fondo que se especifica es el rosa, de conformidad con la Convención de las Naciones Unidas de 1949. Es desafortunado que siga utilizándose ese color, pues el rosa está muy cerca del magenta, color primario que utilizan las fotocopiadoras y las impresoras de color. Hay numerosas pruebas de la explotación de ese punto flaco y de la simplicidad del diseño en la producción de las falsificaciones. Hubiera podido hacerse mucho más para lograr una combinación de diseño y colores que hubiera generado un permiso de conducir con un aspecto característico y difícil de falsificar o alterar. La directiva permite a los Estados añadir elementos de seguridad que ofrezcan protección contra el fraude.

Otra directiva del Consejo emitida en 1997 (97/26/EC) establece medidas adicionales para normalizar las condiciones en que el titular de un permiso puede conducir un vehículo de motor. Éstas incluyen la corrección de defectos de la vista y el oído, así como las modificaciones al vehículo para adaptarlo a cualquier discapacidad del conductor.

En 2003, la Comisión Europea preparó una nueva directiva sobre permisos de conducir, que fue aprobada por el Parlamento Europeo en 2007. Contiene numerosas medidas contra el fraude. En primer lugar, el nuevo modelo que se expedirá será una tarjeta de plástico similar a las de crédito, ya utilizada en algunos países de la UE, que ofrece una mayor protección contra el falseamiento. En segundo lugar, para

aumentar la protección contra el fraude, el permiso de conducir podrá contener un microprocesador. La Unión Europea estima que reproducir la información impresa en la tarjeta en el microprocesador aumenta la protección contra el fraude, y, al mismo tiempo, garantiza la protección de los datos. En tercer lugar, la renovación administrativa obligatoria y periódica del permiso de conducir garantiza que todos los documentos en circulación puedan actualizarse con los elementos de seguridad más modernos. Además, la renovación tendría un efecto positivo con respecto al parecido entre el titular y la fotografía que aparece en el documento. En la Figura 2-7 se ilustra cuál será el diseño del nuevo permiso de conducir europeo.

Figura 2-7
Permiso de conducir europeo de Portugal (anverso)
(Cortesía de *Imprensa Nacional-Casa De Moeda S.A.*, Lisboa, Portugal)

C. Documentos de matriculación de los vehículos

También hay una directiva de la Unión Europea sobre la armonización de la forma y el contenido de los documentos de matriculación de vehículos, con el fin de facilitar su comprensión y, así, contribuir a la libre circulación. La primera directiva del Consejo sobre documentos de matriculación de los vehículos fue emitida por la Unión Europea en 1999. Más recientemente, el Consejo emitió otra directiva, la 2003/127/EC, que modifica la anterior, y proporciona a los Estados miembros de la UE especificaciones relativas a la expedición de los documentos de matriculación de los vehículos en una tarjeta inteligente con microprocesador en lugar de papel (Stauffer y Bonfanti, 2006).

2.6.6 Actividades de normalización en África y América

El primer pasaporte de África oriental fue implantado oficialmente en abril de 1999 a raíz de una iniciativa de la Comunidad del África Oriental (CAO) (www.africa-union.org/root/AU/recs/eac.htm). La Comunidad Económica de los Estados de África Occidental (CEDEAO) estableció en mayo de 2000 nuevas normas para los pasaportes comunes de sus Estados miembros (Resolución C/DEC.1/5/2000 firmada en Abuja en mayo de 2000 relativa a la adopción de un pasaporte CEDEAO).

Los Estados miembros del MERCOSUR (Argentina, Brasil, Paraguay y Uruguay) aprobaron las características de un pasaporte común en 1994 (Resolución No. 114/94).

Más recientemente, la Comunidad del Caribe (CARICOM) elaboró el pasaporte común de la CARICOM. En 2005 Surinam se convirtió en el primer Estado miembro pleno en implantar oficialmente el nuevo pasaporte de la CARICOM (Wikipedia, Comunidad del Caribe).

2.6.7 La Organización Internacional del Trabajo y la tarjeta de identidad de la gente de mar

La Organización Internacional del Trabajo (OIT), creada en 1919, es un organismo especializado de las Naciones Unidas. Es una organización tripartita, en que los representantes de los gobiernos, los empleadores y los trabajadores participan en igualdad de condiciones. A consecuencia del terrorismo internacional y para compensar los intereses de los trabajadores marítimos, la OIT adoptó en 2003 el Convenio sobre los documentos de identidad de la gente de mar (revisado), que entró en vigor el 9 de febrero de 2005.

El Convenio incluye varios aspectos de la cadena del documento, tales como la expedición de los documentos de identidad de la gente de mar, su contenido y forma, el control de calidad y la facilitación. El documento de identidad de la gente de mar es un documento de lectura mecánica que se ajusta a las especificaciones contenidas en el documento 9303 de la OACI. Los Estados miembros de la OIT pueden incluir un patrón biométrico en el documento, si lo consideran oportuno.

La OIT probó una gran cantidad de productos diferentes y finalmente eligió el patrón de la huella dactilar, que se almacenaría en un código de barras como componente biométrico interoperable a nivel mundial para la gente de mar.

Referencias

A continuación figura una lista de normas que están directamente relacionadas o guardan relación con los documentos expedidos por el gobierno.

Naciones Unidas
Convenio de las Naciones Unidas sobre Aviación Civil Internacional – Anexo 9 Facilitación (Convenio de Chicago), 7 de diciembre de 1944.
Convención de las Naciones Unidas sobre el Estatuto de los Refugiados, 28 de julio de 1951.
Convención de las Naciones Unidas sobre el Estatuto de los Apátridas, 28 de septiembre de 1954.
Convención de las Naciones Unidas sobre la circulación por carretera, Viena, 8 de noviembre de 1968 (incluye especificaciones sobre permisos de conducir en papel)

Organización de Aviación Civil Internacional
OACI. Documento 9303, Documentos de viaje de lectura mecánica, parte 1, Pasaportes de lectura mecánica.
OACI. Documento 9303, Documentos de viaje de lectura mecánica, parte 2, Visados de lectura mecánica
OACI. Documento 9303, Documentos de viaje de lectura mecánica, parte 3, Documentos de viaje oficiales, incluidos los pasaportes en formato tarjeta y los certificados de los miembros de la tripulación.
OACI TAG MRTD/NTWG Informe técnico, Aplicación de la ICP para los documentos de viaje de lectura mecánica que permiten únicamente la lectura de microprocesadores, v 1.1 (último disponible en enero de 2005)
OACI TR Desarrollo de una estructura lógica de datos v 1.7 (último disponible en enero de 2005)
OACI TAG MRTD/NTWG Informe técnico, Empleo de biometría en los documentos de viaje de lectura mecánica v 2.0 (último disponible en enero de 2005)
OACI Informe técnico, Utilización de circuitos integrados sin contacto en los documentos de viaje de lectura mecánica v 4.0 (último disponible en enero de 2005)
OACI Informe técnico, Utilización de firmas digitales para los DVLM v 4 (último disponible en enero de 2005)

Normas de la ISO
ISO 7501 partes 1 – 3, Refrendo de la ISO del documento 9303 partes 1 – 3 de la OACI.
ISO 1073 parte 2, Conjuntos de caracteres para reconocimiento óptico de caracteres (OCR-B) – formas y dimensiones.
ISO 1831, Especificaciones de impresión para reconocimiento óptico de caracteres.
ISO 3166 parte 1, Códigos para los nombres de países.
ISO/IEC 7810, Tarjetas de identificación - características físicas.
ISO 7816, Diversas partes que engloban diferentes aspectos de las tarjetas inteligentes con contactos.

ISO 8601, Elementos de datos y formatos intercambiables — Intercambio de información — Representación de fechas y horas.
ISO 10373, Diversas partes que engloban métodos de prueba para diversos tipos de tarjetas.
ISO/IEC 14443, Diversas partes que engloban tarjetas electrónicas de proximidad sin contacto (la proximidad supone la lectura a una distancia máxima de 10 cm).
ISO 18031-1 Permiso de conducir conforme a la ISO — Parte 1: Características físicas y conjunto de datos básicos.

Legislación de la UE sobre pasaportes y documentos de viaje
El Reglamento 2004/2252/CE del Consejo se amplía con la adición de la segunda parte (introducción de identificadores biométricos (impresiones dactilares)).
Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros (2004/L 385/01).
Resolución de los Representantes de los Gobiernos de los Estados miembros, reunidos en el seno del Consejo de 17 de octubre de 2000 que completa las Resoluciones de 23 de junio de 1981, 30 de junio de 1982, 14 de julio de 1986 y 10 de julio de 1995 en lo relativo a la protección contra la falsificación de los pasaportes y otros documentos de viaje (2000/C 310/01)
Resolución de los representantes de los gobiernos de los Estados miembros, reunidos en el seno del Consejo de 10 de julio de 1995 complementaria a las Resoluciones de 23 de junio de 1981, 30 de junio de 1982 y 14 de julio de 1986, relativas a la introducción del pasaporte de presentación uniforme (1995/C 200/01)
Resolución de los Representantes de los gobiernos de los Estados miembros, reunidos en el seno del Consejo, de 14 de julio de 1986, complementaria a las Resoluciones de 23 de junio de 1981 y de 30 de junio de 1982, relativas a la introducción del pasaporte de presentación uniforme (1986/C 185/01)
Resolución complementaria de la Resolución de 23 de junio de 1981 relativa al establecimiento de un pasaporte basado en un modelo uniforme de los representantes de los Gobiernos de los Estados miembros de las Comunidades Europeas, reunidos en el seno del Consejo de 30 de junio de 1982 (1982/C 179/01)
Resolución del 23 de junio de 1981 (1981/C 241/01) sobre el establecimiento de un pasaporte basado en un modelo uniforme.

Legislación de la UE sobre visados
Reglamento (CE) Nº. 1683/95 del Consejo, de 29 de mayo de 1995, por el que se establece un modelo uniforme de visado (1995/L 164/01)
Reglamento (CE) N°. 334/2002 del Consejo, de 18 de febrero de 2002, que modifica el Reglamento (CE) n° 1683/95 por el que se establece un modelo uniforme de visado (2002/L 53/07)

Legislación de la UE sobre premisos de residencia
Reglamento (CE) N° 1030/2002 del Consejo, de 13 de junio de 2002, por el que se establece un modelo uniforme de permiso de residencia para nacionales de terceros países.

Legislación de la UE sobre permisos de conducir
COM (2003) 621, 2003/0252/COD. Propuesta de directiva del Parlamento Europeo y del Consejo sobre el permiso de conducir.
Directiva 97/26/CE del Consejo de 2 de junio de 1997 por la que se modifica la Directiva 91/439/CEE sobre el permiso de conducir.
Directiva 1996/47/CE del Consejo de 23 de julio de 1996 por la que se modifica la Directiva 91/439/CEE sobre el permiso de conducir.
Directiva 91/439/CEE del Consejo, de 29 de julio de 1991, sobre el permiso de conducir.

Legislación de la UE sobre documentos de matriculación de los vehículos
Directiva 2003/127/CE de la Comisión, de 23 de diciembre de 2003, por la que se modifica la Directiva 1999/37/CE relativa a los documentos de matriculación de los vehículos.
Directiva 1999/37/CE del Consejo, de 29 de abril de 1999, relativa a los documentos de matriculación de los vehículos.

Organización Internacional del Trabajo
C185 Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003.
C108 Convenio sobre los documentos de identidad de la gente de mar, 1958.
Informe ILO SID-0002, Perfil biométrico creado a partir de minucias dactilares para los documentos de identidad de la gente de mar.

Bibliografía

de Heij, H.A.M.
2000 "*The design methodology of Dutch banknotes*", proceedings of SPIE, 3973, San José, EE.UU.

ISO
2006 "ISO 18031-1 ISO-*compliant driving licence — Part 1: Physical characteristics and basic data set*", resumen, http://www.iso.org/iso/en/CatalogueListPage.CatalogueList.
ISO, Ginebra.

Lloyd, M.
2003 *The Passport: The History of Man's Most Travelled Document*, Sutton LTD, Stroud, Reino Unido.

Mastenbroek, N. et al.
1995 "*Identiteitsvervalsing*", *Studiereeks Recherche*, 4, Editors van Vliet, A., Knopjes, A., Broekhaar, J.M.J., Dutch National Police Agency, Zoetermeer, Países Bajos.

OACI
2006 Fundación de la OACI (en inglés), http://www.icao.int/icao/en/hist/history02.htm OACI, Montreal.

Parlementair Documentatie Centrum
2006 "*Parlementaire enquête paspoortproject (*1984-1988)", *Parlement & Politiek*, http://www.parlement.com/9291000/modules/g8pdhdiw, *Parlementair Documentatie Centrum*, La Haya.

Renesse, Rudolf L. van
1996 "*Security design of valuable documents and products" Proceedings of the Conference on Optical Security and Counterfeit Deterrence Techniques.* San José, California, EE.UU., SPIE vol. 2659, pp. 10-27.

Stauffer, E., Bonfanti, M.S.
2006 "*Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles", Examination of Vehicle Registration Documents, Academic Press, Burlington*, EE.UU.

Unión Europea
2006 Comunicado de prensa IP/06/872, *New Secure Biometric passports in the EU, strengthen security and data protection and facilitates travelling.*

Wikipedia
2007 Comunidad del Caribe, http://www.wikipedia.com.

CAPÍTULO 3

■ LA ENTIDAD PRODUCTORA

■ 3.1 ¿Productor o integrador de sistemas?

Hemos llegado a la etapa en que la entidad o autoridad expedidora busca un socio competente que le ayude a producir el producto final deseado.

Como ya mencionamos en el Capítulo 1, la complejidad de la cadena del documento exige ciertos conocimientos técnicos para garantizar el funcionamiento adecuado de los puntos de contacto. Ésa es la razón por la que se utiliza con frecuencia el término integrador de sistemas. El integrador de sistemas supervisa la totalidad de la cadena y se cerciora de que todas las partes sean compatibles. Así pues, debe ser capaz de trabajar en colaboración con otras partes. Esa cooperación es un requisito indispensable e importante para poder dotar al producto de calidad y lograr el nivel de seguridad previsto. Del mismo modo, es esencial que los acuerdos alcanzados entre el integrador de sistemas y otras empresas respecto de todas las cuestiones pertinentes queden plasmados en un contrato.

■ 3.2 Procedimiento de licitación

Hay distintas formas de elegir a la entidad productora. Ahora bien, en la mayoría de los países, el Estado y las entidades que dependen de éste tienen elaboradas políticas de contratación destinadas a obtener un aprovechamiento óptimo de los fondos empleados.

Con el fin de aumentar la transparencia, los organismos contratantes han decidido aplicar tales políticas, en especial en materia de documentos de seguridad, cuya producción se considera, en cierta medida, un secreto

de Estado (por ejemplo, los pasaportes). Los documentos seguros suelen ser productos de alta tecnología que requieren conocimientos especializados o técnicos. Ahora bien, dado que únicamente un número limitado de expertos puede proporcionar ese servicio, las entidades contratantes están empezando a fijarse cada vez más en proveedores extranjeros, a fin de encontrar productos que se adapten mejor a sus necesidades.

No obstante, el valor económico de los mercados públicos está directamente afectado por la política. Los contratistas pueden estar sometidos a fuertes presiones para favorecer a proveedores nacionales frente a competidores extranjeros. Sin embargo, el enfoque moderno que, en gran medida se basa en el principio de la libre competencia, exige alejarse de esas posiciones.

La dimensión política, social y económica de los contratos públicos adjudicados por los organismos públicos es cada vez mayor. Por tanto, esencial que las personas que intervengan en la elaboración de un documento seguro conozcan bien el procedimiento de contratación pública pertinente, a saber:

- la normativa y los procedimientos aplicables
- el momento en que el organismo debe elegir contratante entre las distintas ofertas presentadas y
- las cuestiones que hay que abordar antes de que el proceso se ponga oficialmente en marcha

Con ello todas las partes interesadas podrán planificar la licitación con eficacia y llevar el proceso a feliz término.

Fuentes jurídicas mencionadas de ahora en adelante:
Organización Mundial del Comercio (OMC):
Acuerdo sobre Contratación Pública (1994) (ACP).

Legislación europea:
Directiva 93/36/EEC del Consejo de 14 de junio de 1993 sobre coordinación de los procedimientos de adjudicación de contratos públicos de suministro, y Directiva 2001/78/EC de la Comisión sobre la utilización de formularios normalizados en la publicación de los anuncios de contratos públicos.

■ 3.3 Acuerdo sobre contratación pública

3.3.1 Fuente

El Acuerdo de la OMC sobre Contratación Pública (ACP 1994) fue firmado en Marrakech, el 15 de abril de 1994, durante lo que se denomina la Ronda Uruguay[1], y entró en vigor el 1º de enero de 1996. El acuerdo figura en el Anexo 4(b) del Acuerdo por el que se establece la Organización Mundial del Comercio. Se trata de un tratado **plurilateral** y no multilateral; no todos los Estados miembros de la OMC han de adherirse al acuerdo, sino únicamente 39 partes[2]. Al ratificar el ACP (1994), las partes firmantes expresaron su deseo de armonizar su legislación, normativa y procedimientos administrativos con lo dispuesto en el acuerdo antes de su entrada en vigor, lo que ocurrió a varios niveles. Así, la Unión Europea transpuso el acuerdo específicamente a la Directiva comunitaria 93/36/EEC, que es vinculante para los Estados miembros de la UE.

3.3.2 Objetivo del acuerdo

El principal objetivo de los países firmantes era crear un nuevo instrumento jurídico que permitiera alcanzar una mayor liberalización y expansión del comercio mundial y mejorar el marco internacional en que éste se desarrolla (preámbulo del ACP (1994).

3.3.3 Principios

El Acuerdo sobre contratación pública de 1994 se sustenta en tres principios básicos: el principio del trato nacional, el principio de no discriminación y el principio de transparencia (Senti, 2000).

El principio del trato nacional exige que "cada Parte conceda de forma inmediata e incondicional a los productos, servicios y proveedores de

1 El texto del ACP (1994) puede descargarse del sitio http://www.wto.org/spanish/docs_s/legal_s/final_s.htm o consultarse en http://www.wto.org/spanish/docs_s/legal_s/gpr-94_01_s.htm

2 Los países firmantes son: el Canadá, la Unión Europea (27 Estados miembros), Hong Kong (China), Islandia, Israel, el Japón, Corea, Liechtenstein, los Países Bajos con respecto a Aruba, Noruega, Singapur, Suiza y los Estados Unidos de América. El calendario completo de firmas está publicado en el sitio Web http://www.wto.org/spanish/tratop_s/gproc_s/memobs_s.htm

las demás Partes (*léase* países) que ofrezcan productos o servicios de las Partes, un trato no menos favorable que el otorgado: a) a los productos, servicios y proveedores nacionales; y b) a los productos, servicios y proveedores de cualquier otra Parte". (véase el Artículo III (1), y el segundo párrafo del preámbulo del ACP (1994)).

El principio de no discriminación exige que cada Parte se asegure de que "sus entidades no den a un proveedor establecido en su territorio un trato menos favorable que a otro proveedor establecido en dicho territorio, por razón del grado en que se trate de una filial o sea propiedad de extranjeros. Es más cada Parte se asegurará de que "sus entidades no ejerzan discriminación, por razón del país de producción del producto o servicio suministrado, contra proveedores establecidos en su territorio, siempre y cuando el país de producción de conformidad con las disposiciones del Artículo IV sea Parte en el Acuerdo". (véase el Artículo III (2) y el segundo párrafo del preámbulo del ACP (1994)). Ahora bien, ese principio no es absoluto. La Comisión Europea tuvo la idea de adoptar un sistema flexible con el fin de promover que otros países no firmantes se convirtieran en partes del ACP (1994) (King et al., 1994).

El principio de transparencia establece que toda Parte alentará a las entidades a que indiquen las condiciones y formalidades que rigen la aceptación y adjudicación de un contrato (véase el tercer párrafo del preámbulo y el Artículo XVII del ACP (1994)).

3.3.4 Aplicación

Todas las entidades que desarrollen su actividad en el territorio de los Estados firmantes estarán sujetas al Acuerdo sobre contratación pública (1994). En especial, se aplica a los pedidos emitidos por las entidades adjudicadoras que se especifican en el Anexo I del Apéndice I (entidades de los gobiernos centrales que contratan con arreglo a lo dispuesto en el acuerdo); el Anexo 2 (entidades de los gobiernos subcentrales); y el Anexo 3 (todas las demás entidades que se rigen en sus contratos por las disposiciones del acuerdo)[3].

[3] Puede consultar los Anexos íntegros de los países firmantes en el sitio Web http://www.wto.org/spanish/tratop_s/gproc_s/gp_gpa_s.htm

El Acuerdo sobre contratación pública (1994) no contiene ninguna disposición que regule la adjudicación de contratos públicos por organizaciones internacionales. El Anexo del Apéndice I tampoco hace ninguna referencia en ese sentido[4]. En consecuencia, los contratos adjudicados por esas entidades no están sujetos al acuerdo. En todo caso, organizaciones como el Fondo Monetario Internacional o la Organización de las Naciones Unidas adjudican sus pedidos con arreglo a los principios básicos de transparencia, eficiencia y uso eficaz en función de los costos de los fondos públicos, del mismo modo que los países firmantes acordaron realizar sus intercambios comerciales en el ACP (1994). Asimismo los procedimientos son similares a los del ACP (1994)[5].

Además, el ACP (1994) regula el proceso de adjudicación de contratos de suministros públicos y contratos de servicios y obras de construcción públicas.

3.3.5 Valores de umbral

El acuerdo se aplica a los contratos de un valor superior al valor de umbral establecido. Esos valores, indicados en Anexo del Apéndice I (párrafo 4 del Artículo I del ACP (1994)), son específicos para cada Estado firmante. La contratación de bienes y servicios por el gobierno central tiene un valor umbral de 130.000 DEG (Derechos especiales de giro)[6]. En el caso de la contratación de bienes y servicios realizada por entidades de los gobiernos subcentrales el valor umbral varía, pero suele situarse en los 200.000 DEG. Para las empresas de servicios públicos, el valor umbral de la contratación de bienes y servicios suele ser de 400.000 DEG y para los contratos de construcción el valor umbral es de 5.000.000 DEG.

3.3.6 Procedimiento de licitación

El ACP (1994) prevé tres tipos de procedimientos: licitaciones públicas, licitaciones selectivas y licitaciones restringidas.

4 Algunas organizaciones internacionales son observadoras. Para más detalles puede consultar: http://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm

5 Puede consultar la definición de los DEG (derechos especiales de giro) en http://www.imf.org/external/np/exr/facts/spa/sdrs.htm

6 El Método A ha sido rechazado por el Tribunal Cantonal suizo de Friburgo. El Método B es una guía sobre contratación pública publicada por un cantón suizo. El método C fue elaborado por dos expertos suizos, Pictet y Bollinger.

En una licitación pública, se invita a todos los proveedores a presentar ofertas (Artículo VII 3. a) del ACP (1994)). En las licitaciones selectivas, únicamente pueden presentar ofertas los proveedores a quienes la entidad adjudicadora invite a hacerlo (Artículo VI 3. b) ACP (1994)). "A fin de lograr una óptima competencia internacional efectiva en las licitaciones selectivas, para cada contrato previsto las entidades invitarán a licitar al mayor número de proveedores nacionales y de las demás Partes que sea compatible con el funcionamiento eficaz del sistema de contratación. Las entidades seleccionarán de manera justa y no discriminatoria a los proveedores que pueden participar en la licitación" (véase el párrafo 1 del Artículo X ACP (1994)).

En las licitaciones restringidas el organismo adjudicador se pone en contacto con cada proveedor por separado. Ese procedimiento sólo podrá efectuarse con sujeción a las condiciones estipuladas en el Artículo XV del ACP (1994): "cuando por tratarse de obras de arte o por razones relacionadas con la protección de derechos exclusivos, tales como patentes o derechos de autor o cuando por razones técnicas no haya competencia, los productos o servicios sólo puedan ser suministrados por un proveedor determinado y no haya otros razonablemente equivalentes o sustitutivos" (véase el párrafo 1, inciso b Artículo XV del ACP (1994)).

■ 3.4 Aspectos del procedimiento de licitación

A continuación figura una lista de los pasos que hay que seguir en un proceso de licitación:

- Seleccionar el procedimiento de licitación adecuado.
- Definir los criterios de selección cuando se trate de una licitación selectiva.
- Preparar el pliego de condiciones (definir productos/servicios), incluida la lista de requisitos.
- Definir los criterios de adjudicación y el sistema de cálculo de asignación de puntos.
- Establecer unos plazos de acuerdo con las fuentes jurídicas.
- Preparar la convocatoria de licitación o notificación del concurso.
- Establecer un Comité de adjudicación.

- Preparar un informe
- Preparar el anuncio de la adjudicación

En las secciones que figuran *infra*, se dan ejemplos del ACP (1994) y del derecho comunitario europeo.

3.4.1 Seleccionar el procedimiento de licitación adecuado

Por lo general, el organismo contratante suele preferir bien una licitación pública o una licitación restringida. En Europa, el procedimiento negociado (similar a la licitación restringida del ACP) sólo puede utilizarse en los casos previstos en el Artículo 6 (2) y (3) de la Directiva 93/36/CEE.

El carácter tecnológico de los documentos seguros los convierte en especiales. Con el fin de evitar la falsificación y la alteración, se elaboran a partir de materias primas únicas con procedimientos tecnológicos muy sofisticados. Su proceso de producción se caracteriza por la discreción y el secreto. Ésa es la razón por la que en algunos casos los organismos contratantes optan por un procedimiento negociado.

Ahora bien, los organismos contratantes a menudo eligen la licitación selectiva, pues ofrece transparencia tanto en cuanto al producto como al precio. Ese procedimiento también se conoce como licitación pública en dos etapas. En la primera etapa o de precalificación, los posibles proveedores presentan su solicitud de participación. En la segunda etapa, se pide a los proveedores que cumplen las condiciones que presenten una oferta una vez que hayan recibido la lista de requisitos.

3.4.2 Licitación selectiva

En una licitación selectiva, sólo pueden presentar ofertas los proveedores que cumplan las condiciones. El Comité de adjudicación selecciona a los proveedores que cumplen los criterios de selección especificados en la convocatoria de licitación. La selección puede producirse en cualquier momento antes o durante la etapa de adjudicación. El ACP (1994) recomienda que "en el proceso de calificar a los proveedores, las entidades se abstendrán de hacer discriminación entre los proveedores de las demás Partes o entre éstos y los nacionales".

Cuando la selección se produce antes de la adjudicación, la entidad adjudicadora anuncia cuáles son los licitantes precalificados en la convocatoria. Al final de esa etapa, se invita a los proveedores seleccionados a que presenten sus ofertas.

Cuando la selección se produce durante la etapa de adjudicación, la precalificación de los licitantes se produce justo antes de la evaluación de las ofertas. El Comité de adjudicación verifica si los licitantes cumplen los criterios de selección. El procedimiento es el siguiente: cada proveedor presenta dos sobres: el primero contiene información relativa a su idoneidad y el segundo información técnica relativa a la oferta. Las ofertas que no cumplan los criterios de selección no son abiertas.

La decisión se basa en criterios de "idoneidad" (también denominados criterios de selección cualitativa), que han de publicarse en la convocatoria de licitación. La Directiva 93/36/CEE de la Unión Europea especifica las condiciones en que un proveedor podrá quedar excluido de la participación en el contrato (Artículo 20).

La Directiva también ordena que las autoridades contratantes evalúen la idoneidad de los candidatos basándose en criterios relacionados con su capacidad económica, financiera y técnica. Para poder evaluar la idoneidad, las entidades adjudicadoras pueden pedir a los candidatos que faciliten una serie de documentos con arreglo a los Artículos 22 y 23 de la Directiva. Éstos deben incluir lo siguiente: balances o extractos de balances bancarios, una declaración sobre la cifra global de negocio y la cifra de negocio referente a los suministros objeto del contrato realizados por el proveedor en los últimos tres ejercicios, una relación de las principales entregas efectuadas o servicios prestados en los tres últimos años, una descripción de las instalaciones técnicas del proveedor, las medidas empleadas por éste para asegurar la calidad y los medios de estudio y de investigación de su empresa, detalles sobre el personal técnico o los organismos técnicos pertinentes, muestras, descripciones y/o fotografías de los productos que vayan a suministrarse y certificados expedidos por institutos oficiales de control de calidad.

Entre los criterios de selección también puede figurar una comprobación de la seguridad, que, por ejemplo, podría incluir la seguridad física de las instalaciones del proveedor.

3.4.3 Documentación

El Artículo XII y el Artículo VI del ACP (1994) aportan información en materia de especificaciones técnicas y documentación, que el organismo contratante ha de incluir en el procedimiento. Los párrafos siguientes fueron extraídos del acuerdo.

La lista de requisitos (o especificaciones técnicas) define "las características de los productos o servicios objeto de contratación, como su calidad, propiedades de uso y empleo, seguridad y dimensiones, embalaje, marcado y etiquetado, o los procesos y métodos para su producción, y las prescripciones relativas a los procedimientos de evaluación de la conformidad establecidas por las entidades contratantes" (Artículo VI del ACP). Las especificaciones técnicas no se elaborarán, "con miras a crear obstáculos innecesarios al comercio internacional", sino que "se basarán en normas internacionales, cuando existan, y de lo contrario, en reglamentos técnicos nacionales o normas nacionales reconocidas. No se requerirán determinadas marcas de fábrica o de comercio o nombres comerciales, patentes, diseños o tipos particulares, ni determinados orígenes, fabricantes o proveedores, ni se hará referencia a ellos, a menos que no haya otra manera suficientemente precisa o inteligible de indicar las características exigidas para el contrato y se haga figurar en el pliego de condiciones la expresión "o equivalente", u otra similar".

"El pliego de condiciones que se facilite a los proveedores contendrá toda la información necesaria para que puedan presentar correctamente sus ofertas, en particular la información que debe publicarse en el anuncio del contrato previsto, así como:

- la dirección de la entidad a la que deben enviarse las ofertas;
- la dirección a la que deben enviarse las solicitudes de información complementaria;

- el idioma o idiomas en que deberán presentarse las ofertas y la documentación correspondiente;
- la fecha y hora del cierre de la recepción de ofertas y el plazo durante el cual deberán estar abiertas a la aceptación;
- la indicación de las personas autorizadas a asistir a la apertura de las ofertas y la fecha, hora y lugar de dicha apertura;
- las condiciones de carácter económico y técnico, las garantías financieras y la información o documentos que se exigen a los proveedores;
- una descripción completa de los productos o servicios objeto de licitación o de los elementos exigidos, con inclusión de las especificaciones técnicas, los certificados de conformidad referentes a los productos y los planos, diseños e instrucciones que sean necesarios;
- los criterios en que se fundará la adjudicación del contrato, incluidos los factores, aparte del precio, que se tendrán en cuenta en la evaluación de las ofertas y los elementos del costo que se tomarán en consideración al examinar los precios de las ofertas, como los gastos de transporte, seguro e inspección, y, en el caso de productos o servicios de las demás Partes, los derechos de aduana y demás cargas a la importación, los impuestos y la moneda de pago;
- las condiciones de pago;
- cualesquiera otras estipulaciones o condiciones."

Las entidades entregarán el pliego de condiciones a todo proveedor que participe en una licitación pública, a todo proveedor que solicite participar en una licitación selectiva y a los proveedores a quienes se haya invitado a presentar ofertas en las licitaciones restringidas o negociadas.

Todas las condiciones contenidas en la convocatoria constituyen la *lex specialis* de la licitación y son preceptivas tanto para los licitantes como para el organismo contratante.

3.4.4 Criterios de adjudicación

Las ofertas son evaluadas de acuerdo con los criterios de adjudicación contenidos en el pliego de condiciones o en la convocatoria de licitación. Con arreglo al principio de publicidad, durante el proceso de adjudicación, el organismo contratante no podrá adoptar ningún criterio diferente a los establecidos en la convocatoria. Los criterios de adjudicación permitirán al Comité de adjudicación evaluar las ofertas de forma crítica.

A. Precio

La mejor oferta para un contrato puede ser la más barata (Artículo 26 (1) (a) de la Directiva 93/36/CEE) o la más ventajosa económicamente (Artículo 26 (1) (b) de la Directiva 93/36/CEE). Ahora bien, utilizar el costo como criterio es más adecuado para los productos estándar. Dada la complejidad tecnológica que entraña la producción de documentos seguros, aparte del precio, han de tenerse en cuenta otros criterios en la evaluación de las ofertas. Por ejemplo, podría establecerse la relación entre el costo y el nivel de tecnología.

B. Criterios Diversos

Siempre que se trate de documentos seguros, la evaluación deberá basarse en diversos criterios. El Artículo 26 (1) (b) de la Directiva 93/36/CEE de la Unión Europea propone, por ejemplo, el precio, el plazo de entrega, el costo de explotación, la rentabilidad, la calidad, las características estéticas y funcionales, el valor técnico, el servicio postventa y la asistencia técnica. La Comisión Europea publicó dos comunicaciones interpretativas relativas al derecho comunitario en materia de contratación pública y las posibilidades de integrar consideraciones medioambientales y sociales en los contratos públicos (Diario Oficial, 1993). El organismo contratante puede definir criterios de adjudicación específicos diferentes o complementarios, como por ejemplo, la facilidad de uso.

Los siguientes elementos podrían utilizarse como criterios de adjudicación:

- Nivel tecnológico del productor. ¿Se ha mantenido el productor al tanto de los avances tecnológicos? Por ejemplo, si la parte contratante decide que desea modernizar totalmente su documento, ¿cuenta la entidad productora con el equipo, los conocimientos técnicos y la tecnología adecuados para efectuar las innovaciones deseadas?
- Equipo de proyecto. Hubo casos en que las partes contratantes tuvieron que lidiar con equipos totalmente diferentes una vez adjudicado el contrato. Tales situaciones pueden generar retrasos o dar lugar a la fabricación del producto erróneo.

Sería desafortunado que los intereses nacionales impidieran que un contrato fuese adjudicado a un productor extranjero. La tecnología más avanzada de que se dispone hoy en día no es accesible a la población. Eso significa que el número de proveedores de tecnología sofisticada es limitado, y que a veces el tipo de tecnología que un productor desearía aplicar a su documento no está disponible en su país. Si las condiciones que ha de satisfacer el productor no están formuladas adecuadamente, los productores nacionales podrían quedar rápidamente excluidos de la licitación. Dicha exclusión a menudo desemboca en un debate político.

C. ADJUDICACIÓN DE PUNTOS

El método de asignar puntos para la clasificación o adjudicación de las ofertas es la parte del proceso que más atención recibe. ¿Cuántos puntos hay que conceder a una oferta por un criterio de adjudicación específico? Los siguientes ejemplos ilustran lo difícil que es dar con un método óptimo de asignación de puntos. He aquí algunos métodos de cálculo para el criterio del precio.

El número de puntos conseguido mediante los tres métodos varía considerablemente. El método de asignación de puntos puede mantenerse en secreto y no facilitarse a los licitantes. Eso ofrece al organismo contratante bastante flexibilidad a la hora de evaluar las ofertas. Por otro lado, si los licitantes conocen el método, es muy probable que la oferta refleje los criterios de adjudicación.

Tabla 1: Métodos de cálculo[7]

Método A

Oferta	Precio	Diferencia en % con respecto a la mejor oferta	Puntos
A	514.000	0,0	3
B	512.650	0,12	2,5
C	578.000	12,45	2

Método B

Oferta	Precio	Diferencia en % con respecto a la mejor oferta	Puntos
A	514.000	0,0	3
B	512.650	0,12	2,99
C	578.000	12,45	2,66

Cálculo de puntos: Precio más bajo x número máximo de puntos
Precios ofertados por los licitantes

Método C

Oferta	Precio	Diferencia en % con respecto a la mejor oferta	Puntos
A	514.000	0,0	3
B	512.650	0,12	2,96
C	578.000	12,45	0

Cálculo de puntos: (precio más alto – precio de la oferta) x máximo de puntos
precio más alto – precio más bajo

3.4.5 Plazos de licitación y entrega

Con el fin de garantizar la igualdad de trato entre los licitantes, es importante establecer plazos no discriminatorios. Éstos quedarán definidos para que cada candidato elabore una oferta en las mismas condiciones que sus competidores.

[7] El método A ha sido rechazado por el tribunal cantonal suizo de Friburgo. El método B ha sido extraído de una guía sobre contratación pública de un cantón suizo. El método C fue elaborado por dos expertos suizos, Pictet y Bollinger [Directiva del consejo, 1997].

Tabla 3.1: Plazos

Tipo de licitación	Directiva UE "Suministro"	Art. XI del ACP
Licitación abierta	El plazo de recepción de ofertas no será inferior a 52 días naturales a partir de la fecha de envío del anuncio al Diario Oficial de las Comunidades Europeas.	El plazo no será inferior a 40 días a partir de la fecha de la publicación del anuncio.
Licitación selectiva	El plazo de recepción de las solicitudes de participación no será inferior a 37 días naturales a partir de la fecha del envío del anuncio al Diario Oficial. Procedimiento acelerado: 15 días. El plazo de recepción de las ofertas no será inferior a 40 días naturales a partir de la fecha de envío de la invitación. Procedimiento acelerado: 10 días.	El plazo para la presentación de solicitudes de admisión a la licitación no será inferior a 25 días a partir de la fecha de publicación del anuncio. El plazo para la recepción de ofertas no será inferior a 40 días a partir de la fecha de la publicación de la invitación a licitar.
Licitaciones restringidas o negociadas	El plazo de recepción de las solicitudes de participación no será inferior a 37 días naturales a partir de la fecha del envío de la invitación al Diario Oficial de las Comunidades Europeas.	El plazo para la recepción de ofertas no será inferior a 40 días a partir de la fecha de la publicación de la invitación a licitar (con independencia de que esa fecha coincida o no con la publicación del anuncio).

El ACP también establece las circunstancias por las que esos plazos podrían reducirse (Artículo XI (3)).

3.4.6 Anuncio (convocatoria de licitación)

La convocatoria de licitación es un instrumento administrativo utilizado por el organismo contratante para invitar a posibles licitantes a que presenten sus ofertas. Contiene las normas y condiciones que regirán el procedimiento de adjudicación.

La convocatoria no sólo ha de contener información oficial necesaria para garantizar un procedimiento de adjudicación adecuado, sino también toda la información técnica que precisan los licitantes para elaborar una oferta adaptada a las necesidades del cliente. Los Estados miembros de la Unión Europea han de elaborar la convocatoria de licitación con arreglo a lo establecido en la Directiva 93/36/CEE (Artículo 9 (4)) y la nueva directiva sobre el uso de formularios normalizados para la publicación de anuncios de contratos públicos (2001/78/CE), que modifica el Anexo IV de la Directiva 93/96/CEE.

3.4.7 Establecimiento de un procedimiento de adjudicación

Durante el procedimiento de adjudicación, el Comité de adjudicación evalúa las ofertas presentadas por los proveedores con arreglo a los criterios de evaluación. Esa tarea culmina en la adjudicación del contrato al proveedor más adecuado.

El organismo adjudicador podrá organizar esa actividad del modo en que considere oportuno. Establecerá de forma independiente un Comité de adjudicación integrado por diversos expertos, tales como asesores jurídicos o financieros. En el caso de los documentos seguros no es infrecuente que haya representantes de los órganos encargados de hacer cumplir la ley o de los servicios de control de fronteras entre los miembros del Comité de adjudicación. Tales expertos evalúan los aspectos relacionados con la seguridad, analizando si las soluciones ofrecidas cumplen los requisitos técnicos relativos a las características de seguridad o la personalización, factores que podrían formar parte de los criterios de adjudicación.

3.4.8 Informe

El ACP exige que por cada contrato adjudicado, el organismo contratante elabore un informe escrito que incluya toda la información relativa al procedimiento de licitación. Fundamentalmente, el organismo contratante explica las razones por las que ha elegido una oferta en concreto entre todas las presentadas, y, si lo sabe, indica qué parte del contrato ha previsto subcontratar a terceros el adjudicatario.

3.4.9 Anuncio de adjudicación

El Artículo XVIII del ACP 1994 prevé que "las entidades insertarán un anuncio en la publicación correspondiente de las que figuran en el Apéndice II, dentro de un plazo máximo de 72 días contados desde la adjudicación de un contrato con arreglo a lo dispuesto en los Artículos XIII a XV.
En los anuncios figurará la información siguiente:

- la naturaleza y cantidad de los productos o servicios objeto de la(s) adjudicación(es) de contratos;
- el nombre y dirección de la entidad que adjudique el contrato;
- la fecha de la adjudicación;
- el nombre y dirección del adjudicatario;
- el valor de la oferta ganadora, o de las ofertas más alta y más baja tomadas en cuenta para la adjudicación del contrato;
- cuando proceda, los medios de identificar el anuncio publicado con arreglo a lo dispuesto en el párrafo 1 del Artículo IX; o justificación en virtud del Artículo XV para utilizar el procedimiento previsto en dicho Artículo y;
- el tipo de procedimiento utilizado.

Las normas europeas estipulan que los organismos contratantes que hayan adjudicado un contrato deberán dar a conocer el resultado por medio de un anuncio. "Sin embargo, en algunos casos podrá no publicarse determinada información relativa a la adjudicación de un contrato cuando su divulgación pudiere constituir un obstáculo a la aplicación de la legislación, o fuere contraria al interés público o perjudicare los intereses comerciales legítimos de empresas públicas o privadas, o pudieren perjudicar la competencia leal entre proveedores". El anuncio de la adjudicación del contrato se enviará a más tardar 48 días después de la adjudicación del contrato en cuestión y una vez que haya sido publicado *in extenso* en el Diario Oficial de las Comunidades Europeas (Directiva 93/36/CEE Art. 9 (3), Art. 9 (5), Art. 9 (6)).

3.4.10 Precios anormalmente bajos

En la Unión Europea, "si, para un contrato determinado, las ofertas resultan ser anormalmente bajas, con relación a los productos que deben

suministrarse, antes de rechazar dicha oferta, el poder adjudicador solicitará, por escrito, las precisiones que considere oportunas sobre la composición de la oferta, y verificará esta composición teniendo en cuenta las explicaciones recibidas" (Artículo 27 de la Directiva 93/36/CEE).

La Directiva especifica el tipo de explicaciones que el organismo contratante podrá tomar en consideración, a saber: "las justificaciones referidas a la economía del proceso de fabricación, o las soluciones técnicas adoptadas, o las condiciones excepcionalmente favorables de que disfrute el licitador para el suministro de los productos, o la originalidad del suministro propuesto por el licitador".

Ese procedimiento tan minucioso para comprobar las ofertas tiene un doble objetivo: por un lado, proteger a los licitantes de evaluaciones arbitrarias de los organismos adjudicadores; y por otro, proteger al organismo adjudicador de licitantes que podrían no ser capaces de garantizar un contrato a largo plazo.

■ 3.5 El contrato

3.5.1 Objeto y contenido del contrato

El contrato entre la parte contratante y el productor constituye una garantía legal y oficial de lo que ambas partes han acordado respecto del suministro de productos o prestación de servicios.

En efecto, dicho contrato se establece como salvaguardia contra la peor de las situaciones posibles. El contrato es fundamental, particularmente si surgen problemas en las relaciones contractuales, por ejemplo, si las partes no cumplen con sus obligaciones. En tales situaciones, es muy importante que cada una de las partes pueda recurrir a un contrato que prevea disposiciones claras e inequívocas.

Ahora bien, el contrato nunca sale del archivador si los servicios se prestan con arreglo a lo acordado, que suele ser el caso más frecuente. Cuando se trata de la gestión operativa de la prestación de servicios, un acuerdo sobre el nivel de los servicios (ANS) resulta un instrumento mucho más práctico.

Un contrato también estipula las condiciones que han de ajustarse al carácter específico de los servicios objeto del contrato y a la relación entre las partes interesadas. No obstante, la parte principal del contrato contiene una serie de disposiciones generales que también suelen aplicarse a los productos y servicios de los que trata este libro.

3.5.2 Del proyecto de contrato a la gestión del contrato

A. EL PROYECTO DE CONTRATO COMO PARTE DE LA LICITACIÓN

Como hemos visto en la sección 3.2, un nuevo productor suele seleccionarse por medio de una licitación. Con independencia del procedimiento exacto utilizado, la oferta debe estar basada en una lista de requisitos o en un pliego de condiciones. El proyecto de contrato también debe estar incluido en la lista. De este modo, la situación es más clara para ambas partes. La parte contratante recibe información sobre las disposiciones que podrían ser problemáticas, y el productor, o posible productor, se entera de cuáles son las condiciones de entrega de la parte contratante. El productor también tiene la oportunidad de indicar cuáles son las condiciones que no puede o no desea satisfacer, y ofrecer una alternativa en su lugar.

No es necesario elaborar en detalle todas las partes del proyecto de contrato antes de la licitación. Algunas disposiciones pueden desarrollarse con posterioridad, una vez que se conozca mejor la oferta del productor. A menudo es inevitable que el contrato definitivo se negocie únicamente después de que el contrato haya sido adjudicado.

B. NEGOCIACIÓN Y FIRMA DEL CONTRATO

Como ya se ha mencionado, después de la adjudicación, se celebran negociaciones sobre los detalles finales y cualquier cambio que el productor haya podido proponer durante el procedimiento de licitación. Aunque se haya llegado a un acuerdo respecto de una parte considerable del contrato en la etapa de prenegociación, en sí mismas las negociaciones pueden llevar mucho tiempo. Cuestiones como los derechos de propiedad intelectual e industrial, la responsabilidad o los daños y perjuicios suelen recibir la mayor parte de la atención.

Una vez que se ha adjudicado el contrato, hay una gran presión para iniciar inmediatamente las operaciones. Con el fin de evitar retrasos provocados por las negociaciones, la parte contratante y el productor pueden optar por firmar una declaración de intenciones inmediatamente después de la adjudicación, que prevea la obligación de concluir con celeridad las negociaciones y firma del contrato. A ese respecto es importante destacar que tal situación puede debilitar la posición negociadora de la parte contratante.

C. Contrato y gestión del acuerdo sobre el nivel de los servicios

Como hemos explicado anteriormente, suele ocurrir que un contrato se guarde una vez firmado y que no vuelva a sacarse hasta que se acerque la fecha de vencimiento.

Generalmente, se prepara un acuerdo sobre el nivel de los servicios (ANS) para utilizarlo en el control operativo de la prestación de servicios. Éste forma parte del contrato y se aplica a la etapa de ejecución. Únicamente podrá elaborarse una vez que se hayan ultimado y se conozcan todos los detalles relativos a los servicios. Normalmente, esto ocurre poco antes de que empiece la etapa de ejecución.

El productor da cuenta de los servicios prestados por medio de informes provisionales. Si se producen desviaciones con respecto a los niveles acordados, deberán seguirse determinados procedimientos encaminados a mejorar los servicios para que cumplan los criterios establecidos. En caso de que el productor no pudiera desempeñar sus funciones tal y como estaba dispuesto, la parte contratante podrá imponer una sanción.

3.5.3 Contenido del contrato

A. Disposiciones generales

Las disposiciones generales incluyen las definiciones, las partes que participan en el contrato y la materia objeto de éste. Además, los documentos que forman parte del contrato, tales como los utilizados en la convocatoria de licitación (europea), también deben ser mencionados, al igual que su orden de relevancia.

B. Etapa de desarrollo

El contrato se centra en la prestación de servicios por la entidad productora y, como regla general, entra en vigor en el momento en que se adjudica. Dada la naturaleza de los servicios específicos aquí tratados, la etapa de ejecución se ve precedida de un período de desarrollo, elaboración, prueba y aceptación de los productos y servicios. Por consiguiente, las disposiciones contractuales relativas a la etapa de desarrollo difieren de las de la etapa de ejecución. Es, por tanto, conveniente que el contrato establezca una diferencia entre ambas etapas.

En cuanto a la etapa de desarrollo, es preciso llegar a determinados acuerdos respecto del procedimiento que se seguirá en las reuniones y en la toma de decisiones, en especial, sobre la manera en que ello se pondrá por escrito. También debe especificarse cuáles serán los productos y servicios que se desarrollarán y ultimarán en esa etapa. Además, en los casos que entrañen más o menos trabajo del inicialmente previsto, también habrá que llegar a un acuerdo. Con frecuencia, suele discutirse largamente si determinadas cosas están o no incluidas en las especificaciones del contrato. El contrato también tendrá que reflejar lo acordado en materia de pruebas y la aceptación oficial de los productos y servicios por la parte contratante.

También es aconsejable preparar un conjunto similar de acuerdos para la etapa de ejecución. Siempre puede darse la situación en que haya que modificar los productos o servicios durante la etapa de ejecución, y haya de seguirse un procedimiento similar al aplicado en la etapa de desarrollo.

C. Derechos de propiedad intelectual e industrial

En el caso de una entidad productora o un tercero que hagan productos prefabricados, la cuestión de los derechos de propiedad intelectual e industrial es obvia. El asunto se complica cuando los productos y los servicios son concebidos y elaborados por un productor al que se ha contratado. La cuestión que se plantea es quién es el propietario legítimo del producto, concepto o sistema.

Por un lado, la parte contratante podría argumentar que el producto, concepto o sistema ha sido desarrollado de acuerdo a sus especificaciones técnicas, y que, por consiguiente, le corresponden los derechos de propiedad intelectual. Podría querer derechos exclusivos sobre el producto, por ejemplo, desde el punto de vista de la seguridad o, si el producto se reutiliza parcialmente o en su totalidad, podría pedir una compensación por la inversión en capital.

Por otro lado, el productor podría argumentar que sus perspectivas comerciales se verían gravemente limitadas, si se le prohibiera vender los productos y servicios que comercializa a otras partes. En el campo de los documentos seguros, eso afecta con frecuencia a la actividad central del productor.

Un modo de salir de ese atolladero es distinguir entre los conceptos y las soluciones generales, que pertenecerían al ámbito del productor, y, las aplicaciones específicas y exclusivas, que pertenecerían a la parte contratante, y no podrían venderse a un tercero sin su autorización. La experiencia muestra que este tema suele dar lugar a intensas negociaciones y discusiones.

D. PRODUCTOS Y SERVICIOS

El contrato debe incluir una descripción detallada de los productos y servicios que se proporcionarán. Podría ser útil distinguir entre la etapa de desarrollo y la etapa de ejecución. Por ejemplo, la etapa de desarrollo podría ir acompañada de una descripción del *modo* en que se organizará y se prestará el servicio, mientras que la etapa de ejecución podría indicar *cuáles* son las especificaciones del servicio.

E. SUMINISTRO DE INFORMACIÓN, SEGURIDAD Y OTROS REQUISITOS

Hay determinada información del productor acerca del servicio que podría ser importante para la parte contratante. Tal información podría incluir, por ejemplo, datos de producción necesarios para la facturación o la gestión. Es importante garantizar esa cláusula de información y cerciorarse de que está prevista en el contrato.

En función de la naturaleza de los productos y servicios, la parte contratante podría exigir que se cumplan determinadas condiciones relativas a la seguridad física, organizativa y de los datos. Es más conveniente que sea un tercero independiente (un auditor) quien se encargue de evaluar si el productor sigue cumpliendo las condiciones relativas a la organización administrativa y la responsabilidad sobre la seguridad física, organizativa y de los datos. El contrato deberá prever la obligación de realizar esas evaluaciones, que suelen ser anuales.

F. Cláusula de penalización

Al igual que ocurre con los derechos de propiedad intelectual, las disposiciones relativas a las penalizaciones, obligaciones económicas y la evaluación de daños también suelen ser causa de desacuerdo. El productor tratará de mantener al mínimo posible las sanciones por falta de rendimiento al nivel adecuado, e intentará ganar tiempo adicional para rectificar sus omisiones. Esto podría parecer un instrumento eficaz para que la parte contratante pueda obligar al productor a cumplir con sus obligaciones contractuales. La experiencia demuestra que tanto la prestación de los servicios como la relación entre las partes se benefician de la existencia de una cláusula de penalización eficaz. Después de todo, el objetivo primordial es alcanzar la calidad acordada en los servicios.

En la etapa de desarrollo, es preciso acordar determinados jalones a los que vayan ligadas una serie de penalizaciones en caso de no alcanzarse los resultados previstos. Toda la etapa de desarrollo debe estar dividida en tales jalones, que contribuirán a gestionar la realización progresiva de los productos intermedios y finales que necesita la parte contratante.

Los resultados obtenidos utilizando este método son variados. Por un lado, esta estrategia sirve para que los productos se terminen a tiempo, pero también supone grandes presiones para cumplir las obligaciones a toda costa, lo que a veces ocurre en detrimento de la calidad del producto o de la relación de trabajo entre el productor y la parte contratante.

G. Rescisión y disolución

Además de la rescisión del contrato por ministerio de la ley, hay otras razones por las que un contrato puede quedar rescindido o disuelto antes de lo previsto. En cualquier caso de rescisión, ya sea prematura o no, es importante llegar a un acuerdo respecto a la manera en que se va a realizar la transición a un nuevo producto, con el fin de que haya una continuidad en los servicios que recibe la parte contratante. De este modo, podrán determinarse las medidas que ha de adoptar el productor para que haya una transición sin tropiezos.

H. Controversias y resolución de conflictos

Es posible que surjan conflictos entre el productor y la parte contratante que no puedan ser resueltos por éstos. Aunque el derecho civil prevé soluciones (por ejemplo, acudir al tribunal competente) es conveniente acordar cuál va a ser el procedimiento que se adoptará en caso de litigio antes de llevar el caso a los tribunales. Esa cláusula ha de establecer los distintos niveles a los que elevar la controversia en la organización de la entidad productora y en la de la parte contratante, y estipular el procedimiento que debe aplicarse. Si pese a ello, las partes no logran resolver sus diferencias, podrán optar por el arbitraje o por llevar el conflicto a los tribunales.

I. Acuerdo sobre el nivel de los servicios (ANS)

El acuerdo sobre el nivel de los servicios es un instrumento útil para medir el desempeño del productor y equilibrarlo con las normas contractuales relativas al servicio. Puede incluir los aspectos siguientes:

- acuerdos relativas a la gestión del Acuerdo sobre el nivel de los servicios, a las consecuencias de la no conformidad con las normas definidas, y a los informes y las reuniones para examinarlos;
- normas y criterios para la terminación de los productos y la prestación de los servicios;
- normas y criterios respecto de la información que debe facilitarse en materia financiera y sobre aspectos relativos a la gestión;
- procedimientos para efectuar cambios en la gestión y la supervisión de las versiones.

■ 3.6 El papel de las entidades públicas en la cadena de calidad

Con el fin de supervisar la continuidad durante el período de vigencia del contrato, es importante que el cliente designe a un miembro del personal que se encargue del enlace con la entidad productora para seguir de cerca conjuntamente los aspectos relativos a la calidad previstos en el contrato. El representante del cliente se ocupará de la comunicación interna y externa, y emprenderá las medidas necesarias para que los documentos sean expedidos de forma ininterrumpida de conformidad con las condiciones establecidas en el contrato. Esa persona también se ocupará de vigilar el nivel de los componentes, de los productos parciales, las existencias del producto final y la planificación de la producción, con el fin de garantizar la continuidad durante el proceso de expedición.

El productor también deberá tener un departamento de garantía de calidad, responsable de la gestión del manual de calidad y de las auditorías internas de calidad. También supervisará la conformidad y la correcta aplicación de los procedimientos acordados, tomará la iniciativa para efectuar mejoras y dependerá directamente de la gerencia en un lugar independiente de la organización del productor para que haya una comunicación abierta. Todas esas medidas deberán asegurar la entrega de los productos previstos en el contrato de forma ininterrumpida, correcta y según criterios de calidad.

Asimismo, el productor tendrá que disponer de todo lo necesario para optimizar y mantener el proceso de producción durante el periodo de vigencia del contrato, de forma que pueda garantizar la calidad acordada con el cliente. Esas medidas de control se centrarán en las herramientas de producción, la organización de la producción y los materiales auxiliares, así como en aumentar y mantener los conocimientos del personal, con miras a mantener o ajustar de forma responsable los parámetros de los procesos observados y registrados durante la etapa de desarrollo.

Es más, durante la vigencia del contrato, deberá hacerse constar de forma inequívoca quién es la persona de la organización que se encarga específicamente de los componentes de producción con relación a las normas de calidad acordadas con el cliente. En una empresa moderna, ese cometido debe estar ubicado lo más cerca posible de la base de la organización; preferiblemente suele ser el empleado de producción encargado de la distribución de los componentes. El departamento de producción utilizará los equipos de medición y ensayo necesarios para sus procesos. Además, el productor deberá utilizar un laboratorio que pueda realizar otras pruebas que exijan conocimientos profesionales especiales o equipos de investigación específicos.

La dirección también debe velar por que el trabajo se organice de forma óptima con el fin de que la ejecución de los procesos se lleve a cabo sin tropiezos y con eficacia.

Referencias

Senti R.,
2000 *System und Funktionsweise der Welthandelsordnung*, Zurich, 2000, p. 671.

King M., De Graaf G.,
1994 *L'Accord sur les marchés publics dans le cadre de l'"Uruguay Round"*, RMUE 4/1994, p. 75-76.

1993 Diario Oficial de la Unión Europea L 199, 09.08.1993, p. 1-53.

1997 Directiva del Parlamento Europeo y el Consejo Europeo 97/52/EC de 13 de octubre de 1997 que modifica la Directiva 92/50/EEC, 93/36/EEC y 93/37/EEC sobre coordinación de los procedimientos de adjudicación de los contratos públicos de servicios y sobre la coordinación de los procedimientos de adjudicación de contratos públicos de suministro respectivamente; Diario Oficial de la Unión Europea L 328, 28.11.1997, p. 1-59.

CAPÍTULO 4

DE LA SOLICITUD A LA EXPEDICIÓN

El presente Capítulo trata de diferentes aspectos relativos al procedimiento de solicitud y expedición de documentos seguros, así como a la logística necesaria. Aunque esos procesos no forman parte del desarrollo tecnológico de un documento seguro, la experiencia nos enseña que la base del fraude, en el sentido más amplio de la palabra, a menudo está en la etapa de solicitud y expedición.

A continuación figura una breve descripción de un día en la vida de un empresario llamado Juan, que nos da una idea del tipo de documentos que utilizamos cotidianamente. Partiendo de esos documentos, procederemos, más adelante, a definir las entidades expedidoras.

> Juan tiene una cita con un posible cliente en otro país. Para desplazarse allí, Juan compra un *billete de avión*. Sale a las 5.30 horas de la mañana para llegar al aeropuerto a tiempo. Por supuesto, Juan lleva consigo su *permiso de conducir*, *la documentación de matriculación del vehículo* y *el certificado del seguro*.

Figura 4-1
Documento de registro de vehículos de los Países Bajos
(Cortesía de Fons Knopjes, Países Bajos)

Cuando llega al aeropuerto, Juan aparca el coche en el aparcamiento. Para entrar utiliza su *tarjeta de crédito*. En la terminal de salidas se dirige al mostrador de facturación, donde debe presentar su *documento de viaje* y responder a varias preguntas, después de lo que se emite una *tarjeta de embarque* a su nombre. Como Juan viaja muy a menudo es miembro de un programa de fidelización de clientes y tiene todos sus puntos almacenados en una *tarjeta de fidelización*.

Luego Juan se dirige al control de inmigración donde ha de presentar su documento y su tarjeta de viaje, y decir cuál es su destino. El oficial de inmigración comprueba su documento de viaje; lo introduce en un lector para que lea la zona de lectura mecánica y consulta la lista de vigilancia. Inmediatamente después, Juan es autorizado a cruzar la frontera y se dirige hacia el avión. Antes de embarcar, se toma rápidamente un café y un cruasán; paga con un billete de banco y mete el cambio en su monedero. Su vuelo se anuncia y Juan embarca en el avión.

Cuando llega a su destino, Juan presenta su documento de viaje al funcionario de inmigración, quien le permite entrar en el país. Toma un taxi y en breve llega al lugar acordado. Al entrar en el edificio de la empresa, le piden que muestre un *documento de identidad*. Juan presenta su cédula de identidad a la recepcionista, que introduce los datos en el sistema y le entrega una *tarjeta de acreditación de la empresa*. A continuación llega alguien para llevarle al lugar de la reunión.

Figura 4-2
Tarjeta de acreditación para visitantes de la Fábrica Nacional de Moneda y Timbre
(Cortesía de la Fábrica Nacional de Moneda y Timbre, Madrid, España)

La tarjeta de acreditación de la empresa contiene un procesador sin contacto que le permite entrar en distintas zonas de la compañía. La reunión llega a buen fin y los participantes se despiden tras almorzar.

Juan regresa al aeropuerto, donde vuelve a pasar por todo el proceso de facturación, cruzar la frontera y subir al avión. Tras aterrizar, recoge su coche, paga el aparcamiento con su tarjeta de crédito y se va. De vuelta a casa, Juan para en una gasolinera para repostar y paga con su *tarjeta de débito*. El costo del combustible se carga directamente en su cuenta bancaria y se transfiere a la cuenta del propietario de la gasolinera. Al llegar a casa, su mujer le espera con unas *entradas* para ir al teatro.

Figura 4-3
Entrada para un concierto de Cliff Richard
(Cortesía de Fons Knopjes, Países Bajos)

Van al teatro en transporte público, para lo que utilizan una tarjeta *especial con un procesador sin contacto* que contiene una cantidad determinada de dinero y donde se carga el costo de cada viaje.

Muchos de nosotros nos identificamos con este breve relato de un día en la vida de Juan, que ilustra con toda claridad la frecuencia con que utilizamos documentos valiosos.

La Figura 4-4 muestra distintas entidades expedidoras de documentos seguros e incluye dos de las categorías más protegidas (véase la Figura 1-1 del Capítulo 1).

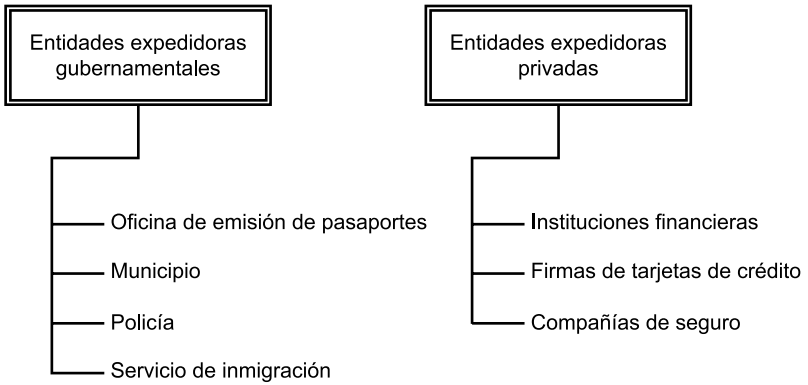


Figura 4-4: Expedidores
Entidades expedidoras privadas y otros

■ 4.1 Organismos públicos expedidores de documentos

Hay muchos organismos diferentes que expiden documentos seguros. Es importante distinguir entre los documentos expedidos por el Estado o la Administración pública y los expedidos por el sector privado. El Estado suele emitir documentos para beneficio de la sociedad en su conjunto, mientras el sector privado suele proporcionar documentos que liga a los usuarios con la entidad expedidora. Ahora bien, únicamente el Estado tiene el derecho exclusivo de expedir determinado tipo de documentos, lo que le da el monopolio. Esto es lógico, dado el importante valor social que tienen esos documentos, entre los que se incluyen los documentos de viaje, los documentos de identidad, los permisos de conducir, los documentos de extranjería y extractos del registro civil.

A continuación se presenta una breve exposición de los distintos organismos públicos encargados de expedir documentos.

4.1.1 Oficinas de pasaportes

Los países anglosajones suelen contar con oficinas de pasaportes, cuyo cometido es proporcionar a los ciudadanos un documento de viaje. Pero no todas las ciudades cuentan con una oficina de pasaportes, pues, normalmente, no hay más que algunas en todo el país. La dispersión geográfica tiene consecuencias logísticas a la hora de solicitar y suministrar los documentos de viaje. Por ejemplo, en el Reino Unido hay siete oficinas de pasaportes regionales. Esas oficinas cuentan con unos 2500 socios locales (actualmente, las oficinas de correos), que se ocupan de entregar a los ciudadanos el formulario de solicitud pertinente. Los ciudadanos cumplimentan el formulario y lo envían a las oficinas regionales. Con el fin de determinar si una solicitud es legítima, esas oficinas han de consultar varias bases de datos del Estado, tales como el registro de nacimientos, defunciones y matrimonios, el registro fiscal, etc. Consultar esas bases de datos es necesario para verificar la identidad del solicitante. Este método facilita la detección de solicitudes fraudulentas.

4.1.2 Los municipios

En muchos otros países, las autoridades locales, en particular los municipios, desempeñan un importante papel en la expedición de documentos. Esas entidades están cerca de la ciudadanía, y, por tanto, cerca de las personas que solicitan documentos. Es frecuente que los municipios gestionen los datos personales de la población local, lo que les permite comprobar la identidad de un solicitante antes de proceder al suministro de un documento. El nacimiento de un niño, por ejemplo, se registra en el municipio, que lo introduce en la base de datos del registro civil. En muchos casos, los datos de nacimientos son un medio de comprobar la identidad de un solicitante. Lo mismo ocurre con una persona que se haya mudado a otro municipio o haya fallecido. Todos esos datos han de manejarse cuidadosa y meticulosamente. El municipio, a menudo siguiendo las instrucciones de la Administración central, puede utilizar la base de datos del registro civil para expedir documentos de viaje o identidad. En otros casos, el certificado de nacimiento se utiliza como prueba de la identidad para expedir un documento de viaje o identidad. La mala gestión de la cadena de identidad constituye un posible riesgo de fraude de identidad.

Figura 4-5: La toma de fotos en el momento forma parte del proceso de solicitud de la tarjeta de identidad de Hong Kong. (Cortesía de Fons Knopjes, Países Bajos)

4.1.3 La policía

La policía también puede ocuparse de la expedición de documentos. En muchos países, los ciudadanos deben solicitar su permiso de conducir o su pasaporte en la comisaría de policía local. Al igual que con las oficinas de pasaportes, la policía también puede consultar las bases de datos del Estado, con el fin de comprobar la identidad del solicitante. Obviamente, la policía también cuenta con sus propias bases de datos con información sobre delitos o infracciones. Antes de expedir un documento seguro, es preciso consultar esas bases de datos. Si, por ejemplo, la persona que solicita un documento tiene una multa pendiente, la policía puede exigir su pago inmediato, o, en casos más graves, puede llegar a detenerla. Al asumir las funciones de organismo expedidor, puede evitar en gran medida que personas buscadas abandonen el país sin ser detectadas. La policía tiene las mismas competencias con respecto al suministro de permisos de conducir a personas que hayan demostrado tener una conducta dudosa en su conducción.

4.1.4 Servicios de inmigración

Muchas personas creen que la labor de los servicios de inmigración sólo se limita a comprobar los documentos de viaje en las fronteras y los aeropuertos. No saben que muchos servicios de inmigración de todo el mundo también expiden documentos. A veces únicamente expiden un número limitado de éstos, pero en algunos países documentos importantes como los pasaportes, los visados, los permisos de residencia y los permisos de trabajo, también son emitidos por los servicios de inmigración. Si los servicios de inmigración se ocupan de la expedición de todos los documentos, los medios para verificar la identidad de un solicitante han de ser comparables a los de la policía. Con frecuencia, los servicios de inmigración sólo se ocupan de la expedición de los documentos de viaje en situaciones de emergencia; en otros casos, pueden expedir los permisos de residencia. En esos casos, verificar la identidad del solicitante podría ser problemático, si los servicios de inmigración no tuvieran acceso a la información necesaria para verificar la identidad de un individuo. No obstante, el personal de inmigración suele tener conocimientos muy especializados en el campo del control de documentos y de la identidad. Antes de emitir un documento de forma imprevista se hacen numerosas preguntas y, siempre que sea posible, se solicitan documentos justificativos para poder verificar la identidad del solicitante.

En los últimos dos años, muchos países han puesto en marcha los denominados “programas de viajeros fiables”, en que la identidad de un viajero y su derecho a entrar en un país quedan determinados al instante por los servicios de inmigración. Ello requiere la expedición de una tarjeta que, en algunos casos, contiene rasgos biométricos para acelerar la verificación de la identidad (véase el Capítulo 7).

4.1.5 Oficinas de expedición de permisos de conducir

En muchos países, el departamento encargado de proporcionar los permisos de conducir es un órgano independiente. Con frecuencia, esa oficina no solamente expide permisos de conducir, sino también otros documentos relacionados con los vehículos de motor, tales como

los certificados de matriculación o de titularidad. Al igual que con los servicios anteriores, la oficina de expedición de permisos de conducir también puede consultar distintas bases de datos. Asimismo, son muy importantes los pasos previos a la solicitud de un permiso de conducir. Hay que tener suficientes medidas de salvaguardia que garanticen que las personas a cuyo nombre se expide un permiso de conducir auténtico han demostrado su capacidad como conductores. Esto puede sonar obvio, pero durante muchos años ha habido un intercambio de permisos de conducir sin que se haya comprobado que la persona que lo solicita es un conductor competente, lo que entraña riesgos para la seguridad vial.

Además de constituir un documento que certifica la competencia del conductor, el permiso de conducir también suele funcionar como documento nacional de identidad. En los países donde esto ocurre, el permiso de conducir es un documento muy importante que puede utilizarse para solicitar otros documentos. Por consiguiente, estas oficinas deben cerciorarse de que la identidad del solicitante se comprueba adecuadamente. En los Estados Unidos, la dirección de vehículos de motor de algunos Estados (como por ejemplo Oregón, California o Florida) se ocupa incluso de la expedición de las tarjetas de identidad.

■ 4.2 El sector privado como expedidor

Existe un gran número de entidades en el sector privado que también pueden expedir documentos. Éstas incluyen, organizaciones de gran envergadura, como las instituciones financieras, las compañías de seguros, las empresas de tarjetas de crédito, etc. En las secciones que figuran *infra* se hace una breve exposición sobre esas entidades.

4.2.1 Instituciones financieras

Hay un gran número de entidades financieras, tales como bancos e instituciones de crédito, que expiden sus propios documentos. Los criterios de expedición varían considerablemente dependiendo de la institución. Esos documentos, normalmente tarjetas bancarias, son un

eslabón importante de las transacciones financieras entre el banco y el usuario de la tarjeta bancaria. Aunque la verificación de la identidad del usuario no es uno de sus principales cometidos, normalmente, la entidad financiera quiere estar segura de la fiabilidad de su cliente. Además, la persona que ha de aceptar el documento exige a la entidad garantías de que el documento emitido avala todas las transacciones financieras realizadas. Es, pues, esencial que estos documentos sean fiables.

4.2.2 Compañías de tarjetas de crédito

Otro tipo de institución que también expide documentos financieros son las firmas de tarjetas de crédito. Al igual que las instituciones financieras, las distintas compañías de tarjetas de crédito tienen sus propias reglas de expedición. Generalmente, una compañía de tarjetas de crédito expide un documento tomando como base una solicitud escrita, sin haber visto jamás al solicitante o haber confirmado su identidad. A menudo una copia del documento de identidad sirve como base de la verificación. Ahora bien, es cierto que las compañías de tarjetas de crédito tienen sus propios métodos para determinar la fiabilidad y la situación financiera del solicitante.

4.2.3 Compañías de seguros

Otro tipo de organización totalmente diferente que también expide documentos valiosos son las compañías de seguros. Las compañías de seguros desarrollan su actividad en todos los sectores, entre éstos el sanitario. Las compañías de seguro médico emiten documentos a sus usuarios, normalmente una tarjeta, que proporciona al titular acceso a los servicios de atención sanitaria.

4.2.4 Otras entidades expedidoras privadas

La lista de otras entidades privadas que expiden documentos es muy larga e incluye supermercados, tiendas de venta al público, hoteles, compañías aéreas, periódicos, gimnasios, empleadores, etc. En su mayoría, los documentos emitidos muestran un número limitado de datos personales (muy pocos de ellos tienen una fotografía del titular

integrada) y tienen rasgos de verificación funcionales (diseño y color). El nivel de seguridad de esas tarjetas es, en su conjunto, muy bajo.

■ 4.3 Procedimiento de solicitud

El procedimiento de solicitud es el primer eslabón de la cadena del documento. Determina si quien solicita un documento concreto cumple o no los requisitos para su obtención. En ese sentido, la identidad del solicitante desempeña un papel importante, pues debe establecerse si, efectivamente, puede ser titular de un documento determinado, o si es un impostor o un farsante. En función del tipo y de la finalidad del documento, los organismos expedidores deberán estar constantemente alerta con respecto a un posible uso indebido. La usurpación de identidad es cada vez más frecuente y el uso indebido de la identidad de una persona a menudo tiene graves consecuencias para su propietario legítimo.

En el procedimiento de solicitud debe también distinguirse entre una primera solicitud y la ampliación de la vigencia de un documento ya existente. En el primer caso, habrá que verificar con más atención la identidad del solicitante y si éste tiene derecho a determinado documento. En el caso de una ampliación, muchos expedidores se conforman con una mera confirmación de los datos existentes. Esto puede plantear riesgos en contextos de segundo orden donde se gestiona la identidad.

Un documento puede solicitarse del siguiente modo:

- presentándose en persona en el organismo expedidor;
- cumplimentando un formulario de solicitud y entregándolo;
- por medio de entidades intermediarias;
- solicitándolo por Internet.

4.3.1 Presentarse en persona en el organismo expedidor

Dependiendo del tipo de documento y de la ubicación de las oficinas del organismo expedidor, podrá pedirse al solicitante que se presente en persona, que en sí mismo tiene muchas ventajas. Por ejemplo, puede confirmarse en el momento que esa persona está viva. El solicitante

también puede responder a preguntas directamente relacionadas con su solicitud, facilitando la verificación.

El organismo expedidor tiene acceso a distintos registros para llevar a cabo la verificación. Si se trata de un municipio, tiene acceso a las bases de datos del registro civil, es decir, al registro de nacimientos, defunciones y matrimonios. La policía y los servicios de inmigración tienen acceso a otras fuentes. Si el organismo expedidor está convencido de la identidad del solicitante y ha determinado que tiene derecho al documento que solicita, dicho organismo puede proceder a su expedición.

4.3.2 Cumplimentar y entregar el formulario de solicitud

Otro modo de obtener un documento es solicitarlo mediante un formulario de solicitud. A menudo utilizado en el sector privado, también se utiliza por la Administración pública. En los países donde hay oficinas de pasaportes, el formulario de solicitud siempre forma parte del procedimiento.

El solicitante puede pedir que el formulario de solicitud se le envíe a su casa; también puede recogerlo en un lugar designado al efecto, como una oficina de correos. Una vez cumplimentado, es posible que el formulario tenga que ser firmado por otra persona independiente, como por ejemplo un abogado, un notario, un clérigo u otro ciudadano destacado del municipio del solicitante. Esa persona emite un certificado en que declara que conoce al solicitante en cuestión. Se trata de un modo de verificar la identidad de éste. Es posible que con posterioridad haya que enviar al organismo expedidor el formulario de solicitud y demás documentos justificativos, como el certificado de nacimiento, extractos del registro civil o los documentos vencidos. La entidad expedidora podrá, entonces, utilizar la información facilitada para cotejarla con las bases de datos de que dispone. Si no hay nada en contra, podrá proceder a expedir el documento.

4.3.3 Entidades intermediarias

El organismo expedidor también puede servirse de una entidad intermediaria, como la oficina de correos. La persona que solicita un documento concreto se dirige a una oficina de correos, que cuenta con los formularios de solicitud y los conocimientos necesarios para asistir al solicitante.

El personal de correos está capacitado para ayudar a los ciudadanos con su solicitud y conoce los procesos de control. Ahora bien, no tiene acceso a ningún medio de consulta. No obstante, el hecho de que el solicitante se persone, entregue los documentos solicitados y firme el formulario en presencia de un funcionario público constituye una medida de control intrínseca que garantiza la verificación e impide la presentación de solicitudes fraudulentas. El organismo expedidor suele tener la posibilidad en un segundo momento de hacer más comprobaciones para garantizar la autenticidad de la solicitud.

4.3.4 Solicitud de documentos por Internet

En los últimos años, ha surgido un nuevo modo de solicitar un documento: por Internet. El uso de la autopista digital con ese fin está experimentando un rápido crecimiento, en especial en países de gran tamaño con ciudades y pueblos diseminados por todo el territorio, lo que permite al Estado llegar a regiones lejanas.

La "Administración pública electrónica" trata de ofrecer, por ese medio, el mayor número posible de servicios, entre éstos, la solicitud de un documento de viaje por Internet. El formulario se cumplimenta en la computadora y se acompaña de los documentos justificativos en formato electrónico, por ejemplo, una copia escaneada del pasaporte caducado del solicitante. Esos documentos son enviados de forma segura a la entidad expedidora, que, seguidamente, procede a evaluar y verificar la solicitud. Si ésta cumple todos los requisitos, el documento es expedido. Ahora bien, este tipo de solicitud está todavía en sus inicios, y, en este momento, corresponde a la Administración proporcionar en primer lugar instrumentos adecuados, tales como, medios seguros de

comunicación mediante una infraestructura de clave pública (ICP), tarjetas inteligentes o incluso elementos biométricos.

Figura 4-6: Pantalla de la oficina virtual de Malasia para la solicitud en línea de documentos donde los solicitantes pueden gestionar la solicitud de renovación de su pasaporte. (Cortesía de IRIS, Kuala Lumpur, Malasia)

■ 4.4 Tramitación de la solicitud

Además de integrar medidas de protección en el procedimiento de solicitud, también es fundamental que se adopten medidas para proteger los procedimientos internos de la tramitación de la solicitud. Suele decirse que la ocasión hace al ladrón. Con el fin de evitar el riesgo de fraudes internos, el organismo expedidor debe cerciorarse de que los procedimientos internos se sigan correctamente. Un aspecto importante del procedimiento es la división de tareas. En función del tipo de documento, el organismo expedidor y el valor del documento en el entorno del usuario, debe haber una separación clara, por ejemplo, entre el empleado que se ocupa de la solicitud y el que se ocupa de la personalización del documento. Incluso podría considerarse asignar la expedición a un tercer empleado. Otra forma de asegurarse aún más de que el procedimiento interno se sigue adecuadamente es mantener un registro de lo que hace cada empleado y de cuándo lo hace.

Además, hay que pensar muy bien dónde se van a almacenar los documentos en blanco. Esto depende en gran medida del sistema de expedición elegido, y habrá que concebir un procedimiento muy riguroso a tal efecto. Una regla de oro es el principio de los "cuatro ojos", según el cual está prohibido dar a un único empleado todo el acceso al almacén de documentos en blanco. Garantizando que no sólo uno, sino dos empleados saquen el suministro diario necesario del lugar en que están almacenados los documentos y que los devuelvan después del cierre, el riesgo de irregularidades se reduce significativamente. La manipulación de esos documentos también debe registrarse meticulosamente.

Una vez realizadas todas las comprobaciones, el empleado puede proceder a la elaboración del documento. La forma en que lo haga dependerá en gran medida del sistema de expedición y de la técnica de personalización elegida. El Capítulo 5 ofrece más información sobre los distintos sistemas de expedición y presenta una visión de conjunto sobre las técnicas disponibles.

■ 4.5 Personalización del documento

La personalización del documento consiste en integrar en éste los datos variables. Esos datos se refieren a la persona a nombre de quien se va expedir el documento. También pueden referirse a la validez del documento, o, si se trata de un documento financiero, pueden consistir en un número de cuenta. En el pasado, los datos personales solían incorporarse de forma manual, pero en la actualidad, hay muchas otras formas de añadir dichos datos. (Para los detalles técnicos sobre esta materia, véase la sección 5.4 *Técnicas de personalización*).

Una cuestión importante es quién debe personalizar los documentos. Al responder a esa pregunta, a menudo se pone de manifiesto dónde deben personalizarse. La calidad de la tecnología de personalización disponible en la actualidad varía considerablemente, y puede ser desde mala a excelente. Pero la calidad no queda determinada únicamente por la tecnología, pues los conocimientos técnicos necesarios para el proceso de personalización también influyen mucho. Además hay

una serie de factores que desempeñan un papel importante a la hora de decidir quién debe personalizar el documento. Desde el punto de vista de la seguridad, la personalización centralizada es preferible a la descentralizada. Pero desde el punto de vista del servicio, la personalización descentralizada es la opción más adecuada. En los sistemas de personalización centralizada, los datos del solicitante deben ser transferidos al lugar donde se lleva a cabo la personalización. Posteriormente, una vez personalizado, el documento ha de devolverse al organismo expedidor. Es evidente que ese proceso dilata los plazos de entrega. Además, puede haber grandes diferencias en la complejidad de manejo del equipo de personalización. Muchas entidades expedidoras utilizan máquinas de escribir e impresoras relativamente sencillas, pero la aplicación de técnicas de gran calidad de sublimación de colorantes o técnicas láser exige que el operador tenga muchos más conocimientos especializados y requiere una infraestructura informática.

■ 4.6 Expedición del documento

Una vez personalizado, el documento pasa al control de calidad, que, por lo general, es lo que menos atención recibe en todo el proceso de solicitud y tramitación. Tras personalizar el documento, es importante comprobar si el proceso se ha llevado a cabo adecuadamente y si las tecnologías de lectura mecánica contenidas en el documento, que permitirán la lectura electrónica de los datos, funcionan correctamente. Podría tratarse de una banda magnética, un código de barras bidimensional, un procesador de contacto o sin contacto, o una zona de lectura mecánica de caracteres OCR-B. Esas tecnologías desempeñan un importante papel en el uso del documento, y, por tanto, es preciso garantizar su adecuado funcionamiento.

Después de personalizar el documento, también es importante comprobar que la información introducida, como por ejemplo los datos personales del usuario, el número de documento, la validez y otros datos, es correcta y cerciorarse de que la calidad de la información se ajusta a las especificaciones técnicas dadas. Esa tarea debe realizarse con precisión para que el siguiente eslabón de la cadena pueda efectuar su labor con confianza en la fiabilidad y la integridad de los

datos incorporados al documento. Basándose en esa información, el siguiente eslabón de la cadena establece una relación con el usuario del documento. Si hay dudas sobre la autenticidad de éste, debido a que el organismo expedidor fue poco estricto con respecto a la calidad, ello tendrá consecuencias perjudiciales para el usuario, que pueden llegar incluso a su detención por sospecha de posesión de documento falso.

Una vez efectuados todos los controles de calidad, el documento puede ser expedido. La forma en que se expida el documento depende, en parte, del método de solicitud, la complejidad del procedimiento de personalización y la ubicación del organismo expedidor. Si hay un representante de dicho organismo en cada municipio, el usuario podrá recoger su documento personalmente. Ahora bien, si la entidad expedidora únicamente tiene oficinas regionales, entonces será necesario utilizar un método diferente de expedición. Lo mismo ocurre cuando solamente hay una única oficina nacional. La expedición puede realizarse del modo siguiente:

- personalmente mientras se espera;
- personalmente con un plazo de espera de varios días;
- por correo;
- por correo con restricciones de uso.

El método más rápido para el usuario es “mientras se espera”. En ese caso la solicitud se tramita de forma inmediata. Se realizan todas las comprobaciones, tras lo cual el documento es expedido. Dependiendo de cómo esté organizado el proceso, el solicitante puede tener el documento deseado en su posesión en un plazo de, por ejemplo, 15 minutos.

Hay otro método de expedición que exige más tiempo e implica tener que esperar varios días. En ese caso, el usuario solicita el documento en la forma requerida y, una vez concluido el proceso, va a recogerlo en persona después de varios días. En algunos países el solicitante recibe el documento por correo. En el plazo de espera se realizan las comprobaciones pertinentes y se personaliza el documento. Este sistema garantiza un procedimiento más seguro y sistemático. Al haber desaparecido la premura, la personalización puede efectuarse de forma centralizada.

Dependiendo del procedimiento de solicitud y personalización utilizado, también es posible enviar documentos íntegros al solicitante por correo. Muchos países utilizan los servicios postales ya sea aplicando o sin aplicar medidas extraordinarias de protección.

La última opción es similar a la anterior, pero con restricciones al uso del documento. Si el solicitante desea utilizar el documento, tendrá que hacer una operación adicional para activarlo. Por ejemplo, en el caso de una tarjeta de crédito, la empresa en cuestión debe ser informada antes de nada de que el documento ha sido recibido, tras lo cual hará una serie de preguntas concretas que solamente pueden ser respondidas correctamente por el futuro usuario. Si todo va bien la compañía de tarjetas de crédito procederá a levantar la restricción, y el usuario podrá utilizar libremente su tarjeta.

4.6.1 Sistemas de expedición

Cada organismo expedidor emite documentos en la esfera de sus competencias. Hemos visto que existe una amplia variedad de documentos, desde los pasaportes hasta las tarjetas de las compañías de seguros, los permisos de conducir o las tarjetas de crédito. Todos esos documentos tienen una característica en común, y es que solamente una vez impresos o fabricados, pueden ser emitidos a nombre del usuario durante el proceso de personalización. Dependiendo del tipo de documento y del organismo expedidor, se elegirá un sistema concreto de personalización y expedición, a saber:

- personalización y expedición descentralizadas;
- personalización descentralizada y expedición centralizada;
- personalización centralizada y expedición descentralizada;
- personalización y expedición centralizadas.

Si desea más información y recomendaciones sobre el tema, véase el Apéndice informativo 3 de la sección III del Documento 9303 de la OACI “Prevención del fraude relacionado con el proceso de expedición”.

4.6.2 Personalización y expedición descentralizadas

A la hora de expedir documentos el organismo expedidor deberá que tener en cuenta varios factores: la distribución geográfica de los usuarios: local, regional, nacional o internacional; la entidad que produce el documento; la base de datos de la que hay que extraer la información para el documento; y la frecuencia con la que hay que sustituir un documento o ampliar su vigencia. Esos factores influyen en el método de personalización y expedición que se elija. En función del método y equipos necesarios, la personalización podría realizarse fácilmente en uno o más lugares. Ahora bien, si el organismo expedidor opta por un método que exija equipos avanzados y costosos, ello será más difícil. Si la entidad expedidora elige un sistema descentralizado de personalización y expedición, deberá disponer de más de un centro o encontrar una organización dispuesta a facilitar ese servicio (por ejemplo, el ayuntamiento o una entidad similar).

4.6.3 Personalización descentralizada y expedición centralizada

Otra opción es personalizar los documentos en más de una ubicación. El organismo expedidor podría elegir esta alternativa con la intención de distribuir el riesgo ligado a la vulnerabilidad del proceso de personalización. Si hay un problema en uno de los centros, siempre es posible recurrir a otros que tengan los mismos conocimientos técnicos y equipos. Una vez personalizados, los documentos se envían a los servicios centrales, que con frecuencia deberán reforzar la seguridad de los documentos o prepararlos para su envío.

4.6.4 Personalización centralizada y expedición descentralizada

Otro sistema de expedición consiste en personalizar el documento de forma centralizada y expedirlo de modo descentralizado. Este sistema permite al organismo expedidor utilizar equipos muy avanzados, que, por lo general, suelen ser costosos. Al organizar el proceso de personalización en un único lugar, es más fácil introducir nuevos elementos de seguridad, en el caso de que haya un aumento del riesgo

ligado a algún documento concreto. Además, este sistema garantiza mayor calidad y sistematización en el proceso de personalización, por la sencilla razón de que el documento se comprueba en un único lugar y no en 550 centros distintos distribuidos por todo el país.

En octubre de 2001, los Países Bajos optaron por este sistema de expedición al introducir, cuando se introdujo el nuevo pasaporte holandés. El usuario solicita un nuevo pasaporte en el municipio de la ciudad en que resida. Ahí se registran y comprueban todos los datos, tras lo que la solicitud se digitaliza y se envía a la entidad productora a través de una línea segura. El productor procesa la solicitud y devuelve el pasaporte personalizado al municipio en un plazo previamente fijado. El pasaporte es entonces expedido a nombre del usuario, después de haber comprobado los datos una segunda vez.

4.6.5 Personalización y expedición centralizadas

La personalización y expedición centralizadas implican un eslabón menos en la totalidad del proceso. En ese caso una vez personalizado, el documento es expedido o enviado al usuario de forma inmediata. Este sistema suele ser utilizado por las instituciones financieras. Las tarjetas bancarias se envían directamente al usuario con o sin restricciones de uso.

Referencias

OACI
2006 Documento 9303, *Documentos de viaje de lectura* mecánica, Parte 1, Pasaportes de lectura mecánica, sexta edición.

CAPÍTULO 5

■ DESARROLLO DEL PRODUCTO

■ 5.1 Introducción

En el desarrollo del producto hay que tomar muchas decisiones sobre aspectos como el diseño gráfico y de seguridad, los materiales, las técnicas de personalización y las pruebas del producto y la producción. Es un proceso difícil, en el que el diseñador tiene que conocer diversos hechos y requisitos operativos. Los apartados siguientes ofrecen una visión detallada de los mismos.

■ 5.2 Diseño

La selección de los materiales que se utilizarán en el producto depende de varios factores. Además, determina las técnicas que se aplicarán. Hay factores importantes que a menudo influyen en la selección de materiales concretos, como son la vida útil del producto y el entorno de utilización (véase el Capítulo 2).

En el caso de un documento de identidad, el material seleccionado debe garantizar una vida útil prolongada. Algunos plásticos ofrecen una vida útil de 10 años. Sin embargo, la utilización del plástico restringe las técnicas que pueden aplicarse a la producción y personalización. Por otro lado, la elección del papel para un producto que tiene que durar 10 años implica riesgos evidentes. Lamentablemente, aún hay gobiernos que siguen emitiendo documentos de identidad que al cabo de algún tiempo se desintegran por completo. Estas opciones erróneas se convierten en una carga para el inspector de documentos, que, confrontado con documentos deficientes, tiene que decidir si confía o no en las personas que los presentan.

Un conocimiento exhaustivo de las soluciones técnicas disponibles y de las limitaciones del proceso de producción puede reducir el riesgo de incompatibilidad de los materiales y las técnicas. Se anima a los productores de documentos a explorar las diferentes combinaciones posibles y probar nuevos productos que podrían resultar adecuados para satisfacer los requisitos especiales de los documentos. En la actualidad, las técnicas de personalización elegidas influyen considerablemente en la selección de un material de base. La tecnología de impresión por chorro de tinta, por ejemplo, es inseparable del substrato de papel, en tanto que el grabado por láser requiere un substrato de polímero sensible al láser (véanse las secciones 5.3 Materiales, y 5.4 *Técnicas de personalización*).

En este momento, los polímeros están sustituyendo progresivamente al substrato de papel, debido a una preferencia creciente por la durabilidad. Además, los polímeros requieren y permiten la integración de nuevos elementos de seguridad[1] y de medios de almacenamiento electrónico de datos para el procesamiento automático de documentos. El desarrollo del documento adquiere una dimensión enteramente nueva cuando se añade un componente de ingeniería al diseño gráfico tradicional.

El diseño gráfico conlleva la elección de estructuras, colores, tintas y técnicas de impresión, pero al mismo tiempo depende de la combinación de elementos de seguridad y del proceso de fabricación. El diseñador de seguridad recibe instrucciones para coordinarse con el director de desarrollo del producto con objeto de alcanzar la mejor solución.

En el marco de su programa de desarrollo de la producción, una empresa profesional especializada en la producción de documentos seguros puede explorar por su cuenta nuevos conceptos para su línea de productos. Para saber dónde buscar, el productor tiene que ser capaz de recurrir a las redes de usuarios mencionadas anteriormente y a sus productos, así como a las organizaciones de lucha contra el fraude y a los proveedores de materiales. Además, en el desarrollo del producto también pueden estudiarse las técnicas aplicadas en campos afines para ver si podrían ser útiles para mejorar los propios productos.

[1] Actualmente, los polímeros no pueden utilizar las marcas al agua, rasgo de seguridad específico del papel.

Las bases del desarrollo consisten en una lista de requisitos y la metodología del proyecto. Eso permite controlar el desarrollo del proyecto, en términos de calidad, costo y tiempo. El proyecto abarca un área extensa, pues engloba la selección de materias primas, la elaboración de diversos elementos de seguridad específicos, las tecnologías de producción que habrá que aplicar, y, en el caso de documentos de viaje o de identidad, las opciones de personalización. A lo largo del proceso se evalúa la relación entre el costo y el resultado, y se seleccionan diversas soluciones, dependiendo del entorno de uso al que se destine el documento.

La impresión desempeña un papel menos destacado en la tarjeta de identidad electrónica. En este caso, se hace mayor hincapié en confeccionar un soporte de plástico duradero para los componentes electrónicos integrados.

El desarrollador del producto es quien tiene que definir exactamente qué nuevos materiales, procesos y equipos se necesitan, y consultar a diversos proveedores sobre esas tecnologías. A partir de las propuestas de soluciones recibidas, se puede seleccionar a un socio para que colabore en esta parte del desarrollo del producto. Es necesario explorar desde el principio del proceso cómo se pueden aplicar esas tecnologías a la futura producción en serie de los documentos.

La selección de los elementos de seguridad que se incluirán en el documento dependerá de la susceptibilidad de éste a la falsificación. Lo ideal es elegir los elementos que cubran más riesgos simultáneamente, y que además se integren armoniosamente en el diseño gráfico del documento. Eso impide tanto su reproducción como su alteración. Por ejemplo, se puede utilizar un dispositivo ópticamente variable para impedir la duplicación. Si se ubica inteligentemente en el documento, ese mismo dispositivo también puede ser un poderoso elemento de disuasión contra la manipulación de los datos variables.

En el diseño de documentos de seguridad existen diversas tendencias. Un extremo consiste en reducir al mínimo el número de elementos de seguridad con objeto de evitar el efecto de árbol de navidad, mientras que el opuesto consiste en incluir todos los elementos de seguridad actualmente disponibles. Sin embargo, el productor que considera el

análisis de riesgos del documento hará una elección práctica: la que impida la duplicación y deje la posibilidad de incluir otras opciones.

■ 5.3 Materiales

En esta sección se describen algunos de los materiales de base (o substratos) actualmente utilizados en los documentos seguros, los criterios de selección específicos y las combinaciones posibles entre distintos materiales. Aunque sin duda el futuro traerá nuevas soluciones y materiales, los materiales que se presentan aquí han dado buenos resultados, y se confía en que sigan haciéndolo en el futuro. Muchos de ellos llevan largo tiempo utilizándose en el sector.

5.3.1 Papel

El papel, uno de los materiales más accesibles, ha sido históricamente el preferido para los documentos seguros. Es económico, flexible, fácil de adquirir, y las técnicas de utilización del mismo están muy extendidas. Ahora bien, los documentos de papel son vulnerables a los ataques de falseadores y falsificadores (Fahrmeir, 2001). Por consiguiente, antes de optar por él, el productor tendrá que decidir si la solución de papel aporta la seguridad necesaria.

Para los billetes de banco y otros medios de pago seguros, como cheques y talones, lo más utilizado es el papel. Las tecnologías de impresión y fabricación de esos billetes de banco con frecuencia también se utilizan en pasaportes, documentos de identidad, permisos de conducir y etiquetas de visado.

El rango de precio de los substratos de papel varía enormemente. Las materias primas, los tipos de marca de agua, las fibras o planchetas de seguridad adicionales y las posibles amenazas a la seguridad pueden incrementar significativamente el costo de este material.

Los productos de papel suelen proporcionar una solución masiva eficaz para lo que se ha dado en llamar “soluciones descentralizadas”, donde la última parte del proceso, es decir, la personalización del documento de identidad o la consignación del valor en un cheque o talón, se lleva

a cabo localmente en la comisaría de policía o en la sucursal bancaria (véase la sección 4.6.2 Personalización y emisión descentralizadas). Suponiendo que se controle toda posibilidad de robo de documentos en blanco, habrá que centrar la atención en los elementos que garantizan la mejor protección contra el falseamiento y la falsificación. En los documentos seguros de papel que no requieren ningún proceso de personalización, como por ejemplo los billetes de banco impresos, la comprobación de la autenticidad es de suma importancia.

A continuación se presenta una lista de elementos de seguridad a efectos de ordenar las diversas soluciones para el papel en función del grado de seguridad que ofrecen. Estas se enumeran por orden descendente, de mayor a menor vulnerabilidad a la alteración, falsificación o falseamiento:

- A disposición de terceros distintos de los impresores de seguridad: el papel de los billetes bancarios, por ejemplo, está restringido a los impresores de billetes solamente.
- Tipos de marca de agua: (por ejemplo, lineal, de tono único o de tonos múltiples, que es la marca de agua óptima para la impresión de seguridad). La elección del nivel de detalle del diseño y el uso de una marca de agua registrada depende de la funcionalidad requerida, del nivel de seguridad y de las limitaciones presupuestarias.

Marca de agua lineal | Marca de agua de tono único | Marca de agua de tonos múltiples

Figura 5-1: Distintos tipos de marcas de agua en documentos de viaje auténticos (Cortesía del Servicio Nacional de Inteligencia Criminal, Países Bajos)

- Hilos de seguridad y bandas holográficas: estos elementos ofrecen un amplio rango de seguridad adicional, a saber, la seguridad visual o de lectura mecánica. Ahora bien, incluso con estos elementos de seguridad, resulta muy difícil elevar un papel no seguro al rango de papel sumamente seguro.
- Fibrillas de seguridad (visibles con rayos UV, visibles con rayos infrarrojos, mates o invisibles): estos elementos de seguridad, muy fiables, se aplican con gran frecuencia, aunque son menos conocidos y utilizados por el público. El análisis forense (es decir, por medio de marcadores secretos) a menudo se lleva a cabo mediante este tipo de elementos.
- Reacción a los productos químicos: los intentos de alterar o falsificar la información aplicada previamente mediante la utilización de disolventes o de otros productos químicos, deja una mancha o punto en el documento. La colocación de esta característica en el último lugar de la lista sería discutible.

Además, hay toda una serie de distintas soluciones para la identificación y verificación. Requieren un lector o una longitud de onda de luz específicos. Este tipo de papel resulta útil para aplicaciones relativamente sencillas, como entradas o pases, pero sobre todo para las aplicaciones masivas con un número limitado de puntos de control. El efecto de ciertos materiales sobre el medio ambiente es un tema polémico muy de actualidad. A este respecto, el papel tiene mucho a su favor. Existe un debate delicado sobre si se atribuye más valor al reciclaje y a los recursos naturales renovables que a atractivos procesos que suponen un consumo intensivo de energía o productos químicos, dado que por cada argumento en favor del papel, suele haber varios en su contra.

Con independencia del papel de seguridad elegido, hay que insistir en que el papel, como casi todos los demás substratos, sólo constituye el soporte del documento seguro. El productor debe recordar que la elección de un papel con una seguridad mínima o inexistente influirá en los procesos subsiguientes, que difícilmente podrán compensar las carencias de la elección inicial.

5.3.2 Substratos de plástico: Cloruro de polivinilo (PVC)

En tanto que el papel es el material de uso más común en los documentos de seguridad, el plástico de cloruro de polivinilo (PVC) probablemente sea el material más utilizado en las tarjetas de plástico, y en especial en las tarjetas bancarias y de crédito, las tarjetas de fidelidad y las tarjetas de identidad.

El PVC tiene ventajas obvias. Su fabricación se presta a una producción en serie relativamente sencilla, lo cual brinda una calidad estable y mantiene bajos los costos. Además, la superficie es suave y brillante, lo que proporciona una buena base para la impresión y los efectos especiales.

Su mayor desventaja reside en su reacción a los cambios de temperatura. A temperaturas bajo cero pierde su flexibilidad y se vuelve quebradizo. A altas temperaturas, se deforma con relativa rapidez. Incluso en circunstancias ideales, conviene renovar las tarjetas al cabo de tres años. Normalmente, los grandes bancos renuevan las tarjetas cada dos años, para protegerse.

Como ocurre con otros materiales, el PVC industrial casi siempre es una mezcla de polímeros que contiene en torno a un 50 % de PVC. El resto de los componentes es un secreto industrial, si bien su objetivo principal consiste en mejorar la durabilidad y otras propiedades de la tarjeta de plástico.

Desafortunadamente, las ventajas de seguridad del PVC son limitadas, y a menudo se basan en los procesos de personalización y en elementos de seguridad añadidos. No obstante, el PVC tiene propiedades excepcionales para el grabado en relieve, sigue siendo funcional en los dispositivos mecánicos de tarjeta de crédito, y hace las veces de sistema de salvaguarda cuando fallan los medios electrónicos. El grabado del PVC es estable y tolera mejor el desgaste que la mayor parte de los demás substratos de plástico.

Además, el PVC permite la aplicación industrial de hologramas, bandas magnéticas, bandas de firma y microprocesadores de tarjeta inteligente (véase la sección 5.4.3 Tecnologías de lectura mecánica). El PVC también es adaptable a muchos métodos avanzados de impresión por impacto y sin impacto. Pese a todas sus restricciones, sus propiedades complementarias en los procesos de acabado, es decir, en los procedimientos de personalización y de control, pueden justificar su utilización.

La flexibilidad del PVC en la impresión de tarjetas sueltas también es otro motivo que lo convierte en un material de uso frecuente en las tarjetas de identificación y de acceso. Al tratarse de un material estable en entornos de oficina, los procedimientos de impresión que se llevan a cabo de forma descentralizada (o en los puntos de venta) producen resultados relativamente buenos. Sin embargo, la variedad de tóneres y tintas de color, por ejemplo, y las preferencias personales en cuanto a imágenes (colores y tonos), pueden dar lugar a grandes diferencias de calidad. El descarte potencial puede ser inaceptable, aunque en principio, una tarjeta de PVC corriente es una materia prima barata y poco segura.

Además, el PVC parece estar manteniendo su posición relativamente segura desde el punto de vista medioambiental, por mucho que el término "cloruro" que contiene su nombre pueda sugerir lo contrario. Las tarjetas de plástico de PVC permanecen relativamente intactas a menos que se quemen o se expongan a bajas temperaturas. En una clasificación ecológica de las materias primas, sin embargo, el PVC pierde buena parte de sus ventajas. Además, la vida útil prevista puede ser bastante modesta en circunstancias más exigentes, como en el caso de las soluciones de identificación. A pesar de todo, se puede decir que aunque el PVC llegue a perder terreno en la industria, seguirá siendo un material ampliamente utilizado en las tarjetas de pago seguras, aunque su seguridad se base en factores extrínsecos al propio material.

5.3.3 Substratos de plástico: Tereftalato de polietileno (PET)

Otro laminado de plástico ampliamente utilizado es el tereftalato de polietileno (PET o PET-G, donde G significa glicol – añadido

originalmente para mejorar las propiedades de laminado). En muchos casos, el PET se utiliza en lugar del PVC o en combinación con éste. En el campo de los documentos seguros, se utiliza sobre todo en las soluciones bancarias y de identificación. Las propiedades de impresión del PET no siempre son tan claras como en el PVC, por lo que en general las tarjetas de PET se laminan con PVC. En ese caso, el PVC confiere a la tarjeta muchas de las propiedades de impresión, como por ejemplo la impresión por sublimación, por choro de tinta o mediante difusión de tinta por transferencia térmica (D2T2).

El PET tiene la ventaja de una mayor vida útil que el PVC, pues dura hasta dos o tres años, o incluso más en condiciones ideales.

Sus desventajas residen en sus limitaciones de grabado en relieve, y en una posible sensibilidad a la deslaminación si la adherencia entre hojas es desigual. El PET también se puede grabar por láser, que en el PVC produce imágenes grises, pero en el PET suele producir un resultado parduzco.

Con frecuencia se considera que el impacto medioambiental de las tarjetas de PET es menos perjudicial que el del PVC. No obstante, resulta difícil evaluar si se debe uso extendido de PET reciclable en el envasado de refrescos, o a que tiene una mayor vida útil.

5.3.4 Substratos de plástico: Acrilonitrilo butadieno estireno (ABS)

El acrilonitrilo butadieno estireno (ABS) no es una alternativa realmente viable para los documentos de alta seguridad. Sin embargo, se utiliza de soporte por ejemplo para las tarjetas SIM de los teléfonos móviles. Proporciona a los teleoperadores un buen medio de gestión de la marca durante el breve periodo de tiempo en que lleva el microprocesador del teléfono. Y una vez retirado el microprocesador de la misma, la tarjeta ABS se puede eliminar con menos preocupación por sus efectos futuros sobre el medio ambiente que el PVC o el PET.

El ABS también tiene a su favor la ventaja del precio, así como el hecho de que resulta muy fácil de modelar mecánicamente.

Una desventaja del ABS es su acabado. Sólo puede ser imprimida la superficie de la tarjeta. Las tarjetas ABS se suelen producir por moldeo, y son muy sensibles a las temperaturas elevadas. Una vez que se han expuesto al calor, estas tarjetas no pueden recuperar su forma original. Todo ello contribuye a una vida útil modesta, estimada en torno a un año, incluso en las condiciones más favorables.

5.3.5 Substratos de plástico: Policarbonato

El policarbonato es otro polímero industrial, que a principios de la década de 1990 se utilizó en documentos de identificación como la cédula de identidad suiza o el permiso de conducir alemán (Fahrmeir, 2001). Tiene numerosas características que lo hacen sumamente atractivo para los documentos seguros, aunque, por otra parte, el procesamiento del policarbonato requiere conocimientos especializados y dispositivos especiales para que resulte una alternativa viable.

Una ventaja es que cuando se combina con el grabado por láser, proporciona una solución difícil de falsificar o de falsear. Dicho de otro modo, si se ha utilizado únicamente policarbonato como substrato, la tarjeta no se puede deslaminar, ni se pueden borrar los datos. El proceso de grabado por láser descompone el material del policarbonato en partículas de carbono, que en la tarjeta están rodeadas de policarbonato sólido (Billmeyer, 1984). Además, el policarbonato soporta la mayor parte de los métodos de impresión de seguridad, de las tecnologías de procesamiento de imagen y también el grabado en relieve, por ejemplo por luz. Asimismo, pueden utilizarse muchos elementos de seguridad adicionales (imagen láser cambiante (CLI, *Changeable Laser Image*®) e imagen múltiple a láser (MLI, *Multiple Laser Image*®), alfagrama (*Alphagram*®), kinegrama (*Kinegram*®), movigrama (*Moviegram*®), pixelgrama (*Pixelgram*®),[2] y por ejemplo tinta ópticamente variable (OVI). Por otro lado, una tarjeta de policarbonato es prácticamente insensible a las variaciones ambientales, y tolera la mayor parte de los productos químicos generalmente utilizados para intentar suprimir o alterar las imágenes impresas en las superficies de PVC o PET. Y dado que tiene una vida útil de al menos 10 años, ofrece seguridad a largo

[2] Marcas registradas de Giesecke & Devrient, Hologram Industries, OVD Kinegram.

plazo. También es una plataforma muy duradera para las antenas y los microprocesadores de las tarjetas inteligentes.

Pero también tiene sus inconvenientes. Su proceso de laminación es más complicado que el de los plásticos mencionados anteriormente. Para asegurar que una tarjeta de policarbonato no se pueda abrir, el proceso de laminación debe llevarse a cabo en condiciones muy estrictas. Además, tiene limitaciones tanto de diseño como de aplicación de ciertos microprocesadores o elementos de seguridad. Por otro lado, la inversión inicial en equipos de personalización puede ser varias veces superior a la necesaria para el PVC o para otros plásticos menos seguros. Además, las ventajas del policarbonato sólo se pueden aprovechar si la personalización se lleva a cabo a nivel central. Si esta técnica se extiende en tres a cinco años, el costo unitario puede pasar a ser muy competitivo, y el mayor plazo de expedición se puede compensar mejorando la efectividad de los servicios logísticos. En algunos casos, su principal inconveniente es que no permite producir una fotografía en color, al menos hasta que los avances futuros hagan posible el grabado de imágenes en color en el policarbonato.

Con todo, a medida que vayan aumentando los requisitos exigidos para los documentos de viaje se puede producir un saludable crecimiento del mercado del policarbonato. Las ventajas previstas a largo plazo y la mayor seguridad justifican las fuertes inversiones iniciales. La personalización centralizada reduce la necesidad de disponer de varias instalaciones de alta seguridad, aunque, por otra parte, puede prolongar los plazos de espera de los clientes.

5.3.6 Otros plásticos y combinaciones de materiales

Los billetes de banco de polímeros han sido periódicamente contemplados como posibles sustitutos de los billetes de banco de papel. Se eligen los polímeros debido a su mayor resistencia y a su vida útil más larga. Se han registrado experiencias tanto positivas como negativas de aplicación del polímero (Wikipedia, 2006), y no cabe duda de que se producirán nuevos avances. En Internet se puede encontrar información sobre los países que utilizan billetes de polímeros (Polymernotes.org, 2006).

Una nueva área interesante de utilización de documentos seguros es la de las soluciones a gran escala y bajo costo, que se han desarrollado combinando diversos materiales. Los denominados laminados y etiquetas de identificación por radiofrecuencia (RFID, por sus siglas en inglés), que se basan por ejemplo en un soporte constituido por una lámina de papel o de plástico y electrónica, hoy en día se prestan a la fabricación industrial. En la actualidad, esas soluciones se usan en etiquetas de precio, billetes de transporte y otras aplicaciones similares. Son más seguras y producen mejores resultados que la mayor parte de las soluciones de código de barras, y son mucho menos costosas que las tarjetas procesadoras o de memoria tradicionales (la tecnología de proximidad se examinará más a fondo en la sección 5.4.3, Tecnologías de lectura mecánica, punto F. microprocesadores sin contacto).

■ 5.4 Técnicas de personalización

La personalización es la última etapa de la producción del documento. El proceso de personalización convierte un documento "básico" genérico, impreso y fabricado por un impresor de seguridad, en un documento único.

También se le pueden añadir elementos de seguridad que dificultan su alteración y falsificación, que son únicos para cada documento en concreto y que completan los elementos de seguridad incluidos en el proceso de fabricación del documento base.

Muchas personas consideran que el proceso de personalización es una actividad independiente, sin relación con el resto. Sin embargo, ha de considerarse como una etapa más de un proceso de producción integral que abarca desde el diseño hasta la expedición y la reexpedición. De hecho, la mayor parte de las decisiones relativas a las técnicas de personalización requieren materiales y procesos de fabricación de documentos específicos. Esos materiales y procesos a menudo afectan a las opciones de seguridad de la impresión.

No entra dentro del alcance de este libro exponer a fondo todas las tecnologías mencionadas en esta sección. Si se desea acceder a un tratamiento más profundo de ellas, conviene consultar una o varias

de las referencias citadas. Esta sección trata de ofrecer al lector un panorama general sobre lo siguiente:

- los factores que hay que tener en cuenta al elegir una tecnología de personalización;
- los tipos habituales de personalización de lectura humana – gráficos e imágenes;
- los tipos habituales de personalización de lectura mecánica;
- la tecnología que conlleva, el costo y el uso de cada método.

Existen diversas tecnologías de personalización a disposición del expedidor. Cada tecnología presenta sus propias ventajas e inconvenientes. Para los expedidores, lo más difícil es llegar a un compromiso entre las tecnologías disponibles y los requisitos que se hayan impuesto a un documento. Esto ya sería todo un logro de por sí si la tecnología fuera estática, pero como además evoluciona rápidamente, los expedidores tienen que mantenerse al día de los avances más recientes.

5.4.1 Factores que hay que tener en cuenta

Con el fin de determinar cuál es la tecnología más adecuada, el expedidor tiene que considerar diversos factores, entre los cuales destacan el uso, las amenazas y los costos. Con respecto al uso y las amenazas, véanse las secciones 2.1 Evaluación general, y 2.2 Análisis del riesgo de fraude. Por lo que se refiere a los costos, hay que recordar que cada proceso de personalización conlleva costos diferentes. A continuación se enumeran algunos de los factores que inciden en los costos totales de personalización y de uso:

- Costos de los materiales: del documento base suministrado por el impresor de seguridad, los colorantes utilizados durante la personalización, los revestimientos de seguridad y resistencia al desgaste aplicados durante la personalización;
- Costos de producción: la amortización de los equipos, la mano de obra, las tasas de descarte;
- Lectores: los elementos de seguridad de lectura humana y mecánica, los datos cifrados, por ejemplo, banda magnética, circuito integrado;

- Seguridad: protección física y auditorías de destrucción de los descartes – documentos defectuosos, suministros no utilizados y documentos semiterminados entre diversos procesos de producción (trabajo en curso); personal de personalización.

En aras de la brevedad, sólo se examinarán las tecnologías digitales más difundidas de entre las que se disponen en la actualidad. Con respecto a las tecnologías de lectura humana (texto, logotipos, imágenes) se tratarán las siguientes: transferencia térmica, electrofotografía, chorro de tinta, grabado por láser y perforación por láser. El examen de las tecnologías de lectura mecánica incluirá la considerada por el Grupo de Nuevas Tecnologías (NTWG) de la Organización de Aviación Civil Internacional (OACI), los circuitos integrados sin contacto, que tienen reconocida su interoperabilidad planetaria, así como otras tecnologías que podrían utilizarse para aplicaciones regionales o nacionales, tales como el reconocimiento óptico de caracteres (OCR, por sus siglas en inglés), la banda magnética, los códigos de barras bidimensionales, la banda óptica y los circuitos integrados con contacto.

5.4.2 Tecnologías de lectura humana

Todos los procesos de impresión utilizan un sistema que consta de tres partes, a saber un colorante, un material receptivo (receptor) y un aplicador. Para conseguir los mejores resultados, estas tres partes deben ser compatibles. Por ejemplo, una estilográfica cara (aplicador) que contenga tinta permanente (colorante), da buenos resultados sobre un substrato de gran calidad parcialmente poroso, como el papel de carta 100% textil, pero da resultados inaceptables cuando se aplica sobre plástico o sobre papel de embalaje muy poroso y de baja calidad.

A. Transferencia térmica

La transferencia térmica, como su nombre indica, utiliza el calor para transferir un colorante de un material “donante”, como una cinta, a un material receptor (substrato). El aplicador o “cabeza impresora” suele ser una formación lineal de puntos (elementos) tratables individualmente. Los elementos se calientan mediante una corriente eléctrica. El aplicador también puede ser un rodillo caliente con un patrón grabado. La transferencia puede ser directa o indirecta; esta última se lleva a cabo a través de un medio interpuesto. La transferencia

puede ser un proceso de “todo o nada”, comúnmente denominado transferencia de masa. Por otro lado, también se puede transferir una cantidad determinada de colorante, dependiendo de la energía calorífica aplicada a cada elemento. Más adelante se ofrece una breve descripción de cada proceso.

La densidad de la transferencia térmica de los elementos de impresión actualmente varía entre 3 puntos/mm (75 puntos/pulgada) y 24 puntos/mm (600 puntos/pulgada). En las aplicaciones destinadas a la identificación, la densidad más frecuente es de 12 puntos/mm (300 puntos/pulgada). Cada elemento se puede tratar individualmente, de forma similar al tratamiento de una “aguja” de una impresora matricial. Además, también se puede controlar la cantidad de energía eléctrica enviada a cada elemento. La energía eléctrica se convierte en calor en el extremo del cabezal de impresión, lo más cerca posible de la cinta y del substrato.

El colorante consiste en una cinta revestida. El proceso y la configuración del revestimiento varían en función de cada proceso de impresión específico.

Con una cinta se pueden crear textos e imágenes gráficas monocromáticos, o de “color plano” (con un único nivel de tonalidad). Una lamina donante fina, normalmente de 6 micras de grosor, se reviste con un material consistente en una combinación de aglutinante (cera, resina o una mezcla de ambas) y pigmentos o tintas. Los pigmentos tienen mejores propiedades de ligereza y rapidez. El material aglutinante hace las veces de portador del pigmento y de adhesivo para fijar el pigmento a la superficie receptora. La composición química del material aglutinante se puede optimizar en función del material receptor al que se destine.

Figura 5-2: Texto negro con un único nivel de tonalidad de un documento de identidad (Cortesía de *Bundespolizeidirektion,* Koblenz, Alemania)

También se pueden utilizar cintas pigmentadas multicolores. Una cinta multicolor va revestida por "segmentos" o "paneles". Cada segmento lleva un revestimiento de distinto color. La longitud del segmento suele coincidir con la longitud del documento. Contiene los colores primarios del proceso de impresión substractiva (opaca) a cuatro colores: amarillo (Y), magenta (M), cian (C) y negro (K). La cinta también puede disponer de segmentos reservados a materiales de seguridad y/o una capa protectora.

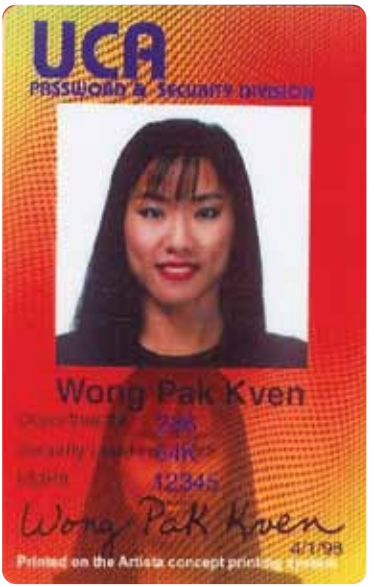


Figura 5-3: Muestra de una tarjeta multicolor
(Cortesía de Fons Knopjes, Países Bajos)

Las cintas de transferencia de tinta, también denominadas cintas de "difusión de tinta", son más habituales. Estas cintas tienen la misma configuración que las cintas pigmentadas multicolores. La cinta está segmentada e incluye al menos los colores YMC. El "color" negro se puede crear utilizando una combinación de estos tres colores. A pesar de todo, se suele incluir negro pigmentado (K) para imprimir códigos de barras u otra simbología que tenga que absorber iluminación por infrarrojos. Aunque no son de uso frecuente, también son posibles las cintas monocromas basadas en tintas.

Los pigmentos o tintas deben ir cubiertos para evitar pérdidas de intensidad y la migración secundaria. Por consiguiente, la cinta debe incluir uno o varios revestimientos protectores, a menudo denominados "paneles T" o "paneles de revestimiento externo". Si no se incluye un panel, habrá que aplicar una capa protectora en una operación independiente.

Las secuencias específicas de las cintas de tinta y pigmentadas multicolores pueden ser muy complejas, dependiendo de las capacidades de la impresora que se utilice. Por ejemplo, una impresora capaz de imprimir un documento por las dos caras puede utilizar una cinta con una secuencia YMCKSYMCK (donde S = Seguridad, como un barniz holográfico). En ese caso, se pueden imprimir imágenes de color pigmentado por las dos caras, y se podría aplicar un material de seguridad en el anverso. En otro caso, la secuencia podría ser YMCKTK y, por lo tanto, la impresión en color por tinta se reduciría al anverso del documento.

La transferencia térmica requiere un substrato compatible. La aplicación más corriente es una tarjeta de identidad de formato ID-1, en la que el material receptor suele ser una tarjeta de plástico pretroquelada. La transferencia de tinta requiere una superficie de polivinilo, o una superficie revestida con una capa receptora. Los materiales de transferencia de masa se pueden aplicar a una gran variedad de materiales, como PVC, PET-G y ABS (véanse las secciones 5.3.2, 5.3.3 y 5.3.4).

El receptor también puede ser una cinta revestida, que hace las veces de soporte intermedio. El colorante se transfiere primero a la cinta revestida. Luego, mediante la aplicación de calor y de presión, se transmite al substrato final destinatario. Este proceso se utiliza cuando el substrato final tiene una superficie irregular o no es receptor de las tintas o del colorante pigmentado contenido en una cinta de transferencia térmica. Con este proceso, se puede personalizar una página de papel para datos de un documento de identificación de formato ID-3 (pasaporte). En este caso, el papel de la página de datos va revestido para favorecer la adherencia, y la transferencia al receptor se realiza a partir del soporte intermedio.

Algunos soportes indirectos sólo transfieren el colorante y la capa receptora. También se puede adherir o laminar el colorante, los soportes revestidos y la cinta portadora. En ese caso, la cinta portadora intermedia hará las veces de lámina protectora.

El proceso de impresión propiamente dicho se describe en las Figuras 5-4 y 5-5.

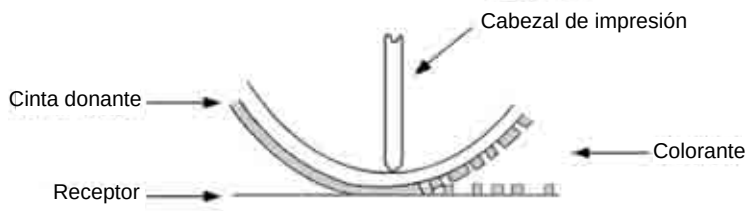


Figura 5-4: Proceso de impresión por transferencia térmica: transferencia de colorante

La Figura 5-4 ilustra que cuando se aplica calor, el colorante se separa de la cinta donante y se transfiere a la superficie del receptor. Mientras no se aplica calor, el colorante permanece en la cinta donante.

Figura 5-5: Impresión por transferencia térmica: diferencia entre la transferencia de masa y la transferencia de nivel tonal

La Figura 5-5 ilustra la diferencia entre la transferencia de masa y la transferencia de nivel tonal. Una cinta de transferencia de masa tiene un único umbral de temperatura. Se aplica energía al cabezal de impresión. La energía térmica se transfiere a través de la cinta donante. Una vez alcanzado el umbral de temperatura, todo el color situado frente al cabezal de impresión se “libera” de la cinta donante y se adhiere al substrato.

Se utiliza un proceso de “oscilación” para crear imágenes de nivel tonal con cintas de transferencia de masa. Para lograrlo se combinan grupos de puntos para crear un “píxel”. Los puntos individuales son demasiado pequeños como para que se puedan percibir por separado. En su lugar, el ojo humano integra los puntos individuales de un píxel determinado en un nivel global de densidad de color. En la actualidad, la ciencia y el arte de la oscilación ya están muy avanzados. Existen numerosas consideraciones, como la relación entre el tamaño del píxel y el nivel tonal por píxel, la ubicación de puntos dentro de los píxeles para evitar efectos de interferencia y los métodos para reducir las gradaciones de color aparente (Kodak, 2006).

Las cintas de nivel tonal no tienen un único umbral de temperatura. En cambio, la cantidad de colorante transferido varía en función de la cantidad de energía aplicada a un elemento de impresión en concreto. Las imágenes de nivel tonal se crean mediante la variación de la densidad de color de cada punto. Por consiguiente, en el caso de las cintas de nivel tonal, cada punto es un píxel.

Las mejoras tecnológicas recientes han dado lugar a la creación de un proceso híbrido. Con la combinación correcta entre cabeza impresora, cinta y receptor, se puede hacer variar el tamaño de un punto creado con una cinta pigmentada. En ese proceso, los niveles de tono se crean mediante una combinación entre la oscilación y el tamaño de los puntos.

La impresión térmica puede ser un proceso rápido y totalmente automatizado, con altas tasas de producción (de varios cientos de unidades por hora), dependiendo de la configuración de la máquina. Se pueden crear imágenes a todo color de gran calidad para incluir imágenes faciales. Durante la personalización, se pueden aplicar gráficos en color característicos, reduciendo con ello los costos de impresión del documento base. Se pueden crear documentos de larga duración mediante tarjetas compuestas, por ejemplo de polivinilo y poliéster y capas de acabado resistentes al desgaste. Dependiendo del formato del documento, la impresión térmica permite crear o coexistir con un gran número de tecnologías de almacenamiento de datos de lectura mecánica.

Los costos de suministro de los colorantes para la impresión térmica pueden ser más altos que en el caso de otras tecnologías. Si se utilizan tintas a modo de colorantes, éstas deben sellarse con una lámina o capa de acabado no porosa para evitar la pérdida de color y la migración del tinte. Como la tecnología de impresión térmica es de fácil acceso, se requieren elementos que impidan la falsificación y pongan de manifiesto las alteraciones, que habrá que evaluar mediante un análisis de amenazas.

B. Electrofotografía

La electrofotografía, denominada asimismo Xerografía o "impresión por láser", comparte diversas cualidades con la impresión térmica. Al igual que esta última, esa tecnología se suele utilizar para crear imágenes de color utilizando colorantes cian, amarillo, magenta (CYM) y negro (K). También se pueden crear imágenes monocromáticas planas y a varios tonos. La impresión se puede llevar a cabo directa o indirectamente.
El proceso electrofotográfico es más complejo que la impresión térmica. Para disponer de una descripción completa de esta técnica, véase una de las referencias citadas (Canon, 2006). A continuación se ofrece una breve descripción del proceso tal como se aplica a los documentos de identidad.

En el modelo de tres componentes, el "aplicador" es una fuente de luz muy concentrada, como un láser o una formación lineal de fotodiodos. La fuente de luz crea una serie de puntos, o imagen latente, sobre una superficie fotosensible. La superficie puede ser un cilindro con un revestimiento rígido, o una correa flexible. Si se usa un láser como fuente de luz, un sistema óptico desplaza el láser hacia delante y hacia atrás sobre la superficie fotosensible a medida que ésta atraviesa el haz luminoso. El haz se "enciende" y "apaga" conforme atraviesa el receptor, de forma similar a una pantalla de la computadora. Si se utiliza una formación de diodos u otra configuración lineal, los elementos individuales se encienden y apagan al paso del receptor, de forma similar a un cabezal de impresión térmica.

La resolución puede variar considerablemente. Para las aplicaciones de identificación, lo normal son 24 puntos/mm (600 ppp). Ahora bien, existen impresoras a color con resoluciones de hasta 96 puntos/mm (2400 ppp). Algunas de las impresoras más recientes pueden modular el tamaño del punto para obtener niveles de tonalidad dentro de un punto determinado.

Habitualmente, la electrofotografía utiliza partículas de tóner como colorante. El tamaño de las partículas de tóner puede variar de menos de una micra a varias micras de diámetro. Los sistemas de alta resolución necesitan partículas de tóner de menor tamaño. La mayor parte de los sistemas utilizan "tóner seco", en el que el propio colorante está envuelto en un aglutinante que es atraído hasta la superficie fotosensible y, subsiguientemente, se funde con la superficie del substrato destinatario. La composición química del aglutinante se puede adaptar a diversos substratos destinatarios. Otros sistemas utilizan partículas finas de colorante suspendidas en un líquido.

Los colores de tóner son el amarillo, el magenta el cian y el negro. También existen materiales de seguridad y colores personalizados.

La electrofotografía es compatible con un amplio abanico de materiales receptores, siendo los más habituales el papel corriente o revestido. Además, se puede utilizar Teslin® y toda una gama de laminas de polímero. A veces se somete el polímero a un tratamiento superficial para mejorar la adherencia de las partículas de tóner y del material aglutinante. A diferencia de la transferencia térmica, las dimensiones del material receptor suelen ser las de una hoja de tamaño A4 o mayor, o una bobina continua, en lugar de una tarjeta pretroquelada.

Se han desarrollado numerosas variaciones, y la tecnología actual es muy compleja. Ahora bien, por lo general, todos los procesos constan de las etapas siguientes:

1. El sistema óptico crea una imagen latente sobre la superficie fotosensible.
2. El tóner es atraído a los lugares expuestos por el sistema óptico.
3. El tóner se transfiere al substrato destinatario o a una superficie interpuesta.

4. Los pasos 2 y 3 se repiten cuantas veces fuere necesario para obtener una imagen multicolor.
5. El tóner transferido se funde con el substrato mediante la aplicación de calor y de presión.
6. El material receptor se lamina y troquela en tarjetas individuales.

La electrofotografía permite crear imágenes en color de gran calidad. Al igual que la impresión térmica, permite crear fondos y gráficos con códigos de color para designar diversos privilegios. Los sistemas de impresión de alta resolución pueden crear microtextos limitados con un contenido único para cada documento específico. En conjunto, el colorante es menos caro que en el caso de la impresión térmica.

Como los colorantes se utilizan en forma de pigmento, no hay problema de pérdida de color. En cambio, la adherencia de las partículas de tóner al substrato receptor sí que puede suponer un problema. Los procesos de impresión previos, en especial los que implican rotograbado, cobertura de tinta, y también las características de los materiales pueden afectar a la adherencia. En cualquier caso, el tóner no penetrará en el substrato (papel), lo cual implica el riesgo de retirada deliberada del mismo por usuarios de mala fe. Por ese motivo, en el caso de documentos de seguridad, es aconsejable utilizar una capa de acabado o barniz protector que ponga de manifiesto las alteraciones. Ahora bien, hay que seleccionar con cuidado la capa protectora para asegurarse de que se adhiera con fuerza al documento impreso.

Para crear un documento acabado hay que efectuar operaciones de laminación y troquelado, puesto que las impresoras electrofotográficas suelen utilizar substratos en formato de hoja o de bobina continua. Esos procesos se pueden integrar en el sistema de impresión. Dependiendo del substrato destinatario, puede resultar problemática la compatibilidad con bandas ópticas, o con circuitos integrados con contacto o sin contacto incorporados en tarjetas de plástico. Al igual que la de impresión térmica, la tecnología electrofotográfica está fácilmente disponible para el consumidor. Por ello, son necesarios elementos contra la falsificación y resistentes a las alteraciones.

C. Chorro de tinta

Impulsados por la gran difusión de las computadoras personales, durante los últimos años se han realizado progresos extraordinarios en el campo de la de tecnología de chorro de tinta. Como ocurre con las demás tecnologías de impresión, en esta sección sólo podemos presentar una breve descripción. Quien desee una descripción más detallada puede consultar la página de tecnología de Canon o uno de los excelentes documentos publicados sobre este tema, como el de S. Ponds (Ponds, 2002).

Hasta hace poco, el uso de chorro de tinta para los documentos de identidad se limitaba a las aplicaciones en papel, como los pasaportes. Las tintas actualmente disponibles para los entornos de oficina no son compatibles con los substratos de plástico no porosos ni con los substratos muy porosos, como el Teslin®. Por ello, esta tecnología no ha ganado aceptación como sistema de impresión para los documentos de identidad de formato ID-1. Se ha investigado mucho para desarrollar revestimientos compatibles con el chorro de tinta que se puedan aplicar a superficies poliméricas. Utilizando esa tecnología, la impresión directa e indirecta por chorro de tinta en documentos formato ID-1 es viable.

Como los demás procesos de impresión, el chorro de tinta utiliza una combinación de colorantes cian, amarillo, magenta, negro y, si se desea, también colorantes especiales de seguridad. Los colorantes son tintes y/o pigmentos disueltos o suspendidos en una solución acuosa. Existen tintas de base no acuosa, pero suelen reservarse a aplicaciones industriales sobre soportes distintos del papel. También se combinan con todo un surtido de aditivos, como antioxidantes, biocidas, fijadores y bloqueadores de rayos UV. La mezcla resultante es bastante compleja.

Tanto los tintes como los pigmentos tienen sus respectivas ventajas. Por lo general, las tintas pigmentadas presentan una mayor inalterabilidad a la luz y al agua. En cambio, las tintas con base de tintura suelen tener mejor penetración y resistencia a la abrasión. Los pigmentos se utilizan para la simbología con absorbencia de IR, como el OCR-B. Las tintas fluorescentes al UV basadas en pigmentos tienden a ser más estables

con el paso del tiempo. Muchos mecanismos de impresión utilizan una combinación de tintes y pigmentos. Los equilibrios dependen de las aplicaciones y no son sencillos.

Figura 5-6: Tarjeta de identidad holandesa falsa impresa por chorro de tinta. Las características de los puntos de color se aprecian claramente (Cortesía de *Sdu Identification*, Haarlem, Países Bajos)

En los sistemas de chorro de tinta, el aplicador es un cabezal de impresión dotado de múltiples orificios. En los documentos de seguridad se utiliza un proceso de "flujo a petición". Otras tecnologías, como las de flujo continuo, son más adecuadas para las aplicaciones de impresión de alta velocidad sobre bobina continua. El cabezal de impresión atraviesa el substrato destinatario de forma similar a las impresoras de chorro de tinta domésticas o de oficina. La tinta se expulsa desde el cabezal de impresión utilizando diversos métodos, siendo los más corrientes la fusión en caliente y el piezoeléctrico.

Las resoluciones progresan rápidamente. Hace diez o quince años, la norma era una resolución de 300 x 300 ppp. En la actualidad, existen

resoluciones de 4800 x 1200 ppp, 4800 x 2400 ppp y 5760 x 1440 ppp. Ahora bien, esas resoluciones tan altas conllevan tanto amenazas como oportunidades para los emisores de documentos seguros.

Como ya se ha dicho, los rápidos avances de hoy en día responden a las necesidades reprográficas inducidas por las computadoras de oficina y domésticos. Sin embargo, nuestro examen en este contexto se centrará en los substratos de papel. La impresión de seguridad impone requisitos complejos en lo tocante a los materiales receptores. Para empezar, el receptor destinatario suele estar impreso mediante un proceso litográfico o rotográfico. Estos procesos de impresión alteran las características de absorción del papel. La impresión de seguridad también impone exigencias en materia de inalterabilidad a la luz y al agua.

Las características de absorción afectan a muchas características secundarias, como el tiempo de secado, la absorción lateral, la luminosidad y la dispersión de gotículas. Esas características influyen en factores críticos, como son la fidelidad del color, la velocidad del proceso y la definición de los contornos. La definición de los contornos, a su vez, es crítica para la simbología y la microimpresión de lectura mecánica.

Los efectos mecánicos, como el abarquillado y la formación de arrugas son menos problemáticos debido al grosor de la mayor parte de los papeles de seguridad. Aún así, hay que tenerlos en cuenta.

Como en otros procesos, el texto, los gráficos y las imágenes se crean mediante una serie de puntos. Los colores se crean a partir de combinaciones de puntos amarillos, magenta y cian. Los sistemas basados en partículas crean imágenes de tonos empleando técnicas de oscilación. Los sistemas basados en tintas ofrecen la posibilidad de compensar la resolución espacial del punto con los niveles de densidad del color. En ambos casos, se pueden (re)producir excelentes imágenes en color. Ese es el motivo por el que un diseño de seguridad consta (asimismo) de líneas de color.

La tecnología de chorro de tinta también es un ejemplo de tecnología impulsada por las exigencias reprográficas domésticas y de oficina. Los sistemas diseñados para la impresión de seguridad se benefician de los avances tecnológicos resultantes. Como también en este caso la tecnología es de fácil acceso, se recomienda incluir elementos contra la falsificación y la alteración.

Los costos de los colorantes de chorro de tinta son bajos, quizás los más bajos de todas las tecnologías mencionadas. Los ritmos de producción del proceso de impresión son moderados: probablemente más rápidos que el grabado por láser, pero más lentos que la impresión electrofotográfica o por transferencia térmica. La inalterabilidad al agua, la inalterabilidad de los colores y la estabilidad de la fluorescencia al UV pueden ser problemáticos con los sistemas basados en tintas, una peculiaridad que se debería poder remediar mediante antioxidantes adecuados y laminados que impidan el paso de los UV. A la inversa, la resistencia a la abrasión puede ser problemática en las tintas compuestas de partículas. Una vez más, un laminado adecuado lo puede resolver.

En todas las tecnologías de impresión en color mencionadas, es fundamental la compatibilidad entre los tres componentes del sistema. Habrá que llegar a compromisos que se verán impulsados por las necesidades de aplicación.

D. Grabado por láser

Últimamente se han conseguido varios avances en la tecnología láser. Los sistemas de grabado por láser se han beneficiado de esos progresos, y este método de personalización parece suscitar un interés creciente. A diferencia de otras formas de personalización, el grabado por láser altera físicamente el substrato del documento.

La descripción técnica siguiente dará una somera idea del proceso de grabado mediante tecnología láser.

El actual grabado por láser utiliza luz láser Nd:YAG (granate de itrio y aluminio dopado con neodimio) dirigida por un sistema óptico que hace las veces de aplicador. La potencia de los láseres utilizados varía de 3,5 a 50 vatios, es decir, considerablemente mayor que la utilizada en electrofotografía.

A diferencia de otras tecnologías, el "colorante"[3] es un elemento central del receptor. Para producir imágenes y otros gráficos de alta resolución, se lamina una capa sensible al láser YAG sobre la estructura del documento.

El receptor es una "tarjeta" laminada de policarbonato o compuesta, como se ilustra en la Figura 5-7. Para el grabado por láser se pueden utilizar otros materiales, incluido el papel. Sin embargo, las láminas de policarbonato de formulación especial reaccionan mejor con la luz del láser YAG para la creación de imágenes detalladas de gran contraste. El formato de la "tarjeta" puede ajustarse a los documentos de formato ID-1, ID-2 ó ID-3. Para la aplicación en pasaportes, se combina la "tarjeta" con el cuadernillo de papel mediante todo un surtido de métodos de ensamblaje.

En el caso de los documentos seguros, el fabricante de la tarjeta ya habrá aplicado la información de seguridad y decorativa pertinente (diseño de seguridad) antes de su laminación y troquelado.

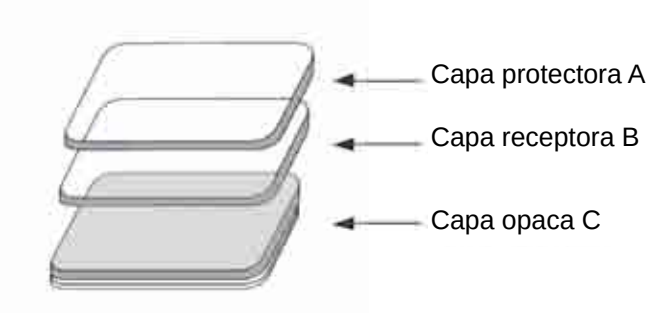


Figura 5-8: Proceso de grabación por láser de una tarjeta

Se puede conseguir toda una diversidad de efectos mediante variaciones de la potencia del láser, el enfoque del haz y la profundidad de enfoque. Para crear imágenes por debajo de la capa protectora, se utiliza un procedimiento similar al descrito en la Figura 5-8.

[3] No obstante, la imagen resultante no es en color.

Figura 5-8: Proceso de grabación por láser de una tarjeta

Se pueden conseguir efectos de superficie táctil empleando energía adicional. La energía luminosa del láser se convierte en energía térmica que, a su vez, hace que la capa protectora se levante lo suficiente (I) para ser detectable al tacto.

El láser también se puede utilizar para conseguir diversos efectos de seguridad. Los sistemas de imagen láser cambiante (CLI), creada por *Mauer Electronics*, y de Imagen múltiple a láser (MLI), creada por Gieseke y Devrient, utilizan una lente lenticular para crear dos o más imágenes bajo la lente. Al girar el documento sobre su eje vertical (en el caso de CLI) o sobre su eje horizontal (para MLI), se pueden observar las diversas imágenes.

E. Perforación por láser

Más recientemente, *Industrial Automation Integrators* (IAI) ha presentado *ImagePerf*® (Hospel, 1998). *ImagePerf*® utiliza un láser más potente para crear una matriz de finas perforaciones a través del substrato. Utilizando un proceso similar a la oscilación de la escala de grises, se puede crear una imagen adicional del titular del documento u otra información. A la luz normal reflectante, esas perforaciones apenas resultan visibles, pero bajo la luz transmitida, la imagen creada por las perforaciones resulta claramente visible.

Las perforaciones creadas mediante el proceso *ImagePerf*® no se pueden reproducir por medios mecánicos, pues son de forma cónica.

IAI y Sdu Identification han desarrollado la *Tilted Laser Image*® (TLI), que combina los efectos de CLI/MLI e *ImagePerf*® (*van der*

Berg y Augustinus, 2000). Con este sistema, se crean dos imágenes utilizando el proceso *ImagePerf*. Las imágenes se obtienen practicando perforaciones a ángulos distintos. Cuando se inclina el documento hacia la luz transmitida, se pueden observar las distintas imágenes.

5.4.3 Tecnologías de lectura mecánica

Las tecnologías de lectura mecánica ofrecen una amplia selección de medios de almacenamiento de datos. Estos medios pueden ser utilizados para la autenticación automatizada del documento o para la autenticación del titular del documento (véase el Capítulo 7, El uso de la biometría en los documentos de viaje).

En función de la tecnología utilizada, en el momento de la personalización se puede codificar información utilizando una o varias técnicas. Dichas técnicas pueden ser:

- el reconocimiento óptico de caracteres (OCR);
- las bandas magnéticas;
- los códigos de barras bidimensionales;
- las bandas ópticas;
- los microprocesadores con contacto;
- los microprocesadores sin contacto.

Los documentos con un alto grado de protección de seguridad técnica pueden combinar diversas tecnologías de almacenamiento de datos. Sin embargo, la Organización de Aviación Civil Internacional (OACI) anima a los Estados miembros a utilizar medios basados en circuitos integrados sin contacto con capacidad suficiente, como única tecnología de almacenamiento con interoperabilidad planetaria, con vistas a facilitar el almacenamiento sobre la marcha de datos e identificadores biométricos adicionales en los documentos de viaje de lectura mecánica (Nueva Orleans, Resolución del 21/03/2003). Es posible que los emisores de sistemas cerrados también deseen considerar otras opciones. Antes de optar por una u otra solución, es importante incluir también el precio de los lectores en el resumen de costos. A continuación se incluye una breve descripción de cada una de estas tecnologías.

Figura 5-9: Zona de lectura mecánica de una tarjeta de identidad sueca de formato ID-1. (Cortesía de la policía sueca, Estocolmo, Suecia)

A. Reconocimiento óptico de caracteres

En 1978, el Grupo de trabajo de la OACI sobre tarjetas de pasaporte adoptó el reconocimiento óptico de caracteres (OCR) como la primera opción tecnológica para codificar información de lectura mecánica (OACI, 2006). Desde entonces, se viene utilizando el tipo de fuente OCR-B para presentar información legible por máquina en la zona de lectura mecánica de los documentos de viaje. La zona de lectura mecánica está situada en la parte inferior de la página de datos del pasaporte, en los visados y en las tarjetas de identidad de formato ID-2 y en el reverso de las tarjetas de identidad de formato ID–1. La zona de lectura mecánica contiene una secuencia de letras de dos o tres líneas que representa información como el nombre, el número de documento, la fecha de nacimiento, etc. Es la misma información que aparece en la llamada zona visual del documento de viaje. Para mayor información, véase el Documento 9303 de la OACI.

Un estudio informativo presentado en el TAG/MRTD en 2004 por el Grupo de Trabajo sobre educación y promoción informaba sobre el estado de la expedición de documentos de viaje de lectura mecánica. Basándose en los datos recabados mediante una encuesta realizada por la secretaría de la OACI y a partir del *Keesing Document Checker* (base de datos de documentos en línea), el estudio destacaba que 100 partes

contratantes de la OACI en todo el mundo y otros tres países estaban emitiendo pasaportes de lectura mecánica.

B. Bandas magnéticas

La banda magnética es una de las tecnologías más antiguas aplicadas a los documentos de lectura mecánica. Las bandas se incorporaron a las tarjetas financieras nada menos que en la década de 1970. Casi al mismo tiempo, se incorporaron también a las libretas de ahorro de formato tipo ID-3.

La norma sobre la banda magnética prácticamente no ha experimentado cambios desde su introducción inicial en la década de 1960, es decir, antes de los discos flexibles. En 2001 se publicaron nuevas normas sobre las bandas magnéticas. Se suprimió el riesgo de que los falsificadores alterasen fraudulentamente los datos variables contenidos en las bandas magnéticas mediante la incorporación de una firma digital. A pesar de todo, el riesgo de falsificación o duplicación es alto. La duplicación o clonado es una forma de falsificación de la banda magnética mediante la cual los delincuentes consiguen copiar la información contenida en la pista de la banda magnética de una tarjeta válida (véase la Figura 5-10, dispositivo de duplicación).

Figura 5-10: Dispositivo de duplicación colocado en la parte frontal de un cajero automático. El dispositivo de duplicación está copiando y almacenando la información de la banda magnética de una tarjeta de pago.
(Cortesía de *VISA International*, Londres, Reino Unido)

A continuación, codifican la información en una tarjeta falsa o robada y la utilizan fraudulentamente (APCA, 2006). Se ha mejorado la seguridad de los cajeros automáticos del mundo entero para impedir que los estafadores consigan alterar la máquina para capturar los datos de la tarjeta sin que se entere el titular de la misma.

Esta forma de almacenar información digital probablemente se utilizará menos en los documentos de seguridad, pues el microprocesador sin contacto se ha convertido en la opción elegida para la interoperabilidad planetaria (al menos en los documentos de viaje). En un futuro próximo, cada vez serán más los emisores de tarjetas de crédito que se pasen a la tecnología de microprocesador.

C. Códigos de barras bidimensionales

Los códigos de barras bidimensionales de alta capacidad pueden almacenar al menos 10.000 bytes. La capacidad de un símbolo determinado (registrado) varía en función del espacio disponible, de la geometría del espacio, de la densidad de impresión, del nivel de corrección de errores y de la combinación de contenido alfanumérico y binario.

Figura 5-11: Código de barras bidimensional (2D) de una tarjeta.
(Cortesía de *Giesecke & Devrient*, Munich, Alemania)

La impresión de los códigos de barras resulta bastante económica. Si se utiliza la impresión térmica para la personalización, el código de barras se imprime al mismo tiempo que el resto de la información, utilizando el mismo segmento de tinta. Por lo tanto, no se requiere tiempo ni suministros adicionales. Si se utiliza tecnología electrofotográfica o de chorro de tinta, su inclusión no afecta a la velocidad, y el consumo adicional de colorantes es inapreciable. El grabado por láser no requiere ningún material adicional; en cambio, sí que podría afectar al tiempo necesario para la personalización.

D. Bandas ópticas

Las bandas ópticas ofrecen la mayor capacidad de almacenamiento en las tarjetas de formato ID-1. Las bandas, con una superficie mínima de 11,5 mm (0,45 pulgadas) por 85,6 mm (3,37 pulgadas) y una superficie máxima de 30,78 mm (1,21 pulgadas) por 85,6 mm, tienen capacidades de almacenamiento de 1,2 Mb y 2,8 Mb, respectivamente.

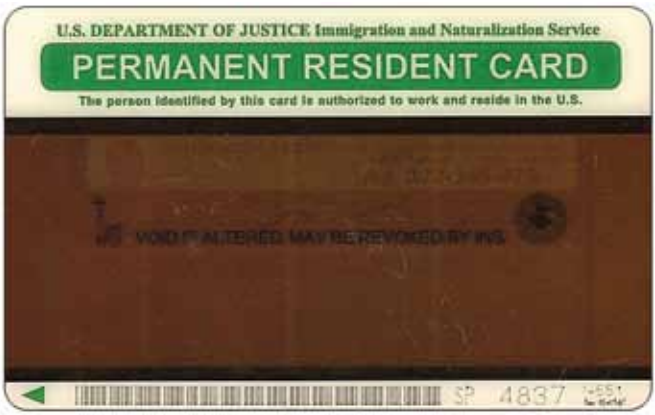


Figura 5-12: Banda de memoria óptica de un permiso de residencia permanente (tarjeta verde) de los Estados Unidos.
(Cortesía del Servicio de Inmigración de los Estados Unidos de América, Washington D.C.)

Las bandas ópticas son similares a los discos compactos (CD) en el sentido de que no son sobrescribibles de por sí. En cambio, se puede añadir nueva información y la información previa queda identificada como archivada. En vista de las grandes capacidades disponibles, este

enfoque no debería plantear problemas, y además incorpora una pista de auditoría que brinda seguridad adicional. Igual que en los CD, los datos de la banda óptica se almacenan en pistas. Se puede leer de una sola vez (secuencialmente) una pequeña cantidad de datos, del orden de unos miles de bytes. Para mayores cantidades de datos, es mejor leer elementos o grupos de datos específicos (acceso aleatorio).

Al igual que sucede en las bandas magnéticas y los códigos de barras, la información grabada en una banda óptica es visible y por consiguiente "clonable". No obstante, se pueden utilizar técnicas de grabado especializadas para obstaculizar dicha visibilidad sin el lector adecuado. Dada la cantidad de datos grabados, la interpretación manual sería tediosa en el mejor de los casos.

El costo de las bandas ópticas es comparable al de las tarjetas con microprocesador. Sin embargo, también hay que incluir en la ecuación los costos del lector, sobre todo cuando las aplicaciones requieren un gran número de lectores. La abrasión de la superficie puede mermar la fiabilidad de la lectura. Sin embargo, un lector lleva incorporado un elemento de corrección de errores para mantener la fiabilidad de la lectura. Aún así, puede merecer la pena proporcionar una funda protectora para las tarjetas ópticas.

Las velocidades de personalización pueden suponer un problema. Los tiempos de codificación varían de un minuto a más, dependiendo de la cantidad de datos.

E. Tarjetas con microprocesador de contacto

Como ocurre con las bandas ópticas, la tecnología de tarjeta con microprocesador sólo está disponible en tarjetas de formato ID–1.

La tecnología de los microprocesadores está avanzando rápidamente, impulsada por los avances en el campo de los circuitos integrados en general. Las capacidades aumentan en respuesta a las exigencias del mercado, y no por la necesidad de superar barreras tecnológicas. En la actualidad, existen microprocesadores de almacenamiento de datos de usuario con capacidades de 32 kb, 64 kb o más. Esas capacidades

Figura 5-13: Tarjeta de identidad electrónica de Bélgica con microprocesador. (Cortesía del Padrón Nacional del Ministerio del Interior, Bruselas, Bélgica)

son ampliamente suficientes para la mayor parte de las aplicaciones de identificación. Las aplicaciones biométricas, en cambio, podrían requerir mayores capacidades.

La ventaja principal de las tarjetas con microprocesador es la seguridad, más que la capacidad. Las tarjetas microprocesadoras pueden funcionar en un sistema operativo seguro. El acceso a la escritura de elementos de datos o grupos de datos específicos se puede controlar criptográficamente, por ejemplo, si alguien pretende modificar o añadir datos, debe responder correctamente a una comprobación criptográfica. El acceso de lectura se puede controlar de forma similar. En caso necesario, los datos se pueden configurar como secretos, en cuyo caso nunca se podrán leer a partir de la tarjeta.

Como en el caso de las bandas ópticas, los datos contenidos en una tarjeta microprocesadora se pueden leer todos de una vez (secuencialmente) o bien se pueden leer elementos o grupos de datos específicos, si los elementos pueden direccionarse y leerse individualmente (acceso aleatorio).

Muchas tarjetas con circuito integrado en realidad son microprocesadores. Como tales, se pueden programar con otras aplicaciones. Cuando se incorporan varias aplicaciones, el sistema operativo del microprocesador

suele aislarlas unas de otras, y no puede producirse comunicación o intercambio directo de datos entre aplicaciones.

Las velocidades de personalización varían en función de la cantidad de datos, de las velocidades de entrada/salida del microprocesador, de cómo están estructurados los datos, y de los protocolos de seguridad. Los tiempos de carga normales varían de 10 a 40 segundos. Por ello, los sistemas de personalización de alta velocidad suelen cargar varios microprocesadores en paralelo, lo que permite alcanzar un ritmo de producción de tarjetas razonable[4].

F. MICROPROCESADORES SIN CONTACTO

La tecnología de los microprocesadores sin contacto ha avanzado con gran rapidez. Para la mayoría de la gente, la tecnología sin contacto es sinónimo de las sencillas etiquetas de radiofrecuencia utilizadas para la vigilancia electrónica de Artículos o las tarjetas de control de acceso de proximidad. Los progresos tecnológicos ya permiten la producción de microprocesadores comparables a las tarjetas de contacto – CPU de 32 bits, hasta 1 Mb de memoria total, coprocesadores de cifrado asimétrico, intérpretes java y capacidades de comunicación dual (con y sin contacto). Los costos son similares a los de los dispositivos exclusivos de contacto.

En la actualidad existen dos normas para las tarjetas sin contacto: ISO 14443 para los dispositivos "de proximidad", e ISO 15693 para los dispositivos de "vecindad". Los dispositivos de proximidad se pueden comunicar a distancias de hasta 10 cm a velocidades superiores a 100 kb/seg, aproximadamente cinco veces más deprisa que la mayor parte de los microprocesadores de contacto. Actualmente la velocidad de comunicación de referencia de los dispositivos ISO 14443 es de 106 kb/seg (Finkenzeller, 2003). Los dispositivos de vecindad se pueden comunicar a una distancia de hasta un metro a velocidades de hasta 26.48 kb/seg (en "modo rápido") (Finkenzeller, 2003). La distancia y las velocidades de comunicación de los dispositivos de vecindad varían

[4] Debido a que cada sistema de producción posee características peculiares en cuanto al tipo de máquinas, datos, redes y soportes lógicos, no se puede predecir una velocidad definitiva del proceso.

en función del modo de funcionamiento – sólo lectura, autenticación, o escritura. Alcanzar mayores velocidades de comunicación puede reducir significativamente el tiempo necesario para cargar datos en el documento.

En 2003, en la reunión de Glasgow del Grupo de Trabajo sobre nuevas tecnologías, se suprimió la norma ISO 15093 como norma alternativa para los microprocesadores de circuito integrado en documentos de viaje de lectura mecánica. Esta decisión supone una reducción del riesgo de captación indebida. La captación indebida se produce cuando se puede grabar la comunicación hacia y desde un documento de viaje de lectura mecánica. La duplicación es un método de fraude que también es aplicable a los microprocesadores sin contacto. Por consiguiente, es necesario implantar un procedimiento de autenticación como contramedida. La OACI recomienda el control de acceso básico, que sólo permite el acceso al microprocesador después de haber leído la zona de lectura mecánica del documento de viaje. No obstante, según los expertos, esta medida sólo asegura una cobertura limitada de la protección contra el fraude (Fidis.net, 2006).

Figura 5-14: Microprocesador de proximidad de un pasaporte británico. (Cortesía del Servicio Nacional de Inteligencia Criminal, Países Bajos)

■ 5.5 Pruebas

Probar un concepto de producto implica evaluar su conformidad con las normas internacionales, la funcionalidad del documento, la eficiencia de las salvaguardas aplicadas y la durabilidad del producto. Todo ello se comprueba sometiendo los conceptos del producto a un programa intensivo de pruebas en el que cada aspecto debe alcanzar una puntuación mínima.

El productor tiene que recurrir a expertos y medios independientes para realizar estas pruebas de forma responsable y eficaz. Cuando haya aspectos que desborden el ámbito de conocimientos especializados y experiencia del productor, éste puede recurrir a la colaboración de expertos y laboratorios externos. Por ejemplo, se puede encargar la realización de las pruebas de toxicidad a un laboratorio especializado en materias primas, mientras que un grupo integrado por colectivos de usuarios puede evaluar la funcionalidad de uso de un documento durante la etapa de desarrollo del documento en cuestión. Para evaluar la resistencia al fraude, además de a sus propios especialistas, el productor puede recurrir a la ayuda de organizaciones de lucha contra el fraude.

Las pruebas realizadas en laboratorios dotados de equipos específicos se pueden dividir en tres categorías:

- pruebas para comprobar la compatibilidad de los materiales;
- pruebas para verificar la resistencia a las manipulaciones fraudulentas;
- pruebas para verificar la compatibilidad con las normas internacionales.

Estas pruebas no se llevan a cabo de acuerdo a una secuencia fija, sino que con frecuencia se realizan en paralelo para después proceder a una evaluación global de los resultados.

5.5.1 Compatibilidad de los materiales

Las pruebas relativas a los substratos, tintas y demás elementos que se van a integrar en el documento (funda, dispositivos ópticamente variables, etc.) sirven para comprobar la compatibilidad de los materiales, para estudiar las opciones de un proveedor y para definir las especificaciones definitivas del documento seguro que se va a producir. Un ejemplo típico es la prueba de compatibilidad del substrato con la técnica de personalización necesaria.

El programa de pruebas de compatibilidad puede incluir las pruebas siguientes (cuya enumeración no es ni mucho menos exhaustiva):

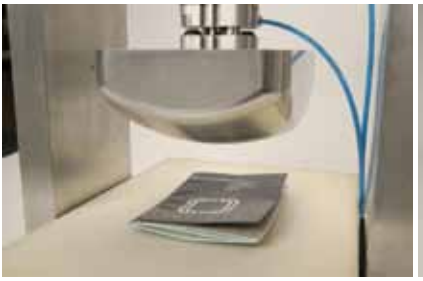
- pruebas ambientales;
- resistencia a la luz;
- abrasión;
- resistencia a los productos químicos;
- desgaste y rotura (por ejemplo, se simula que una persona lleva el documento en el bolsillo trasero del pantalón).

Durante las pruebas ambientales, se somete el documento (o partes del mismo) a diversas condiciones de luz, temperatura y humedad para simular el proceso de envejecimiento. Para ello, se utilizan equipos especiales y condiciones controladas. Al final del ciclo de envejecimiento, el personal de laboratorio anota todos los cambios de aspecto en relación con el color, la forma, las dimensiones, etc.

Hay que tener presente que un documento de viaje acompaña a su titular a todas partes. Por tanto, es importante que los materiales utilizados en la elaboración de ese tipo de documento sean resistentes a las condiciones climáticas extremas. Por otro lado, en condiciones de utilización y conservación normales, el aspecto no debe cambiar durante todo su periodo de validez. Piense, por ejemplo, qué le pasaría a su permiso de conducir si lo metiera en la lavadora con la ropa.

Otra prueba importante es la de resistencia a la luz. Los documentos de viaje pueden ser utilizados durante varios años. En algunos países, el pasaporte tiene un plazo de validez de hasta 25 ó 50 años. Ahora bien, las normas internacionales recomiendan un periodo de validez de 10 años[5]. Durante ese periodo no debe cambiar el color de algunos componentes: la cubierta, los datos personales y las tintas de impresión. En la prueba, se expone el material a una fuente de luz artificial equivalente a los rayos solares a una humedad relativa constante. Se somete una muestra de referencia al mismo tratamiento. En función del tiempo de exposición, el color de la muestra de referencia varía con arreglo a la escala lana azul. Un material con un valor de 3 en la escala lana azul es menos resistente a la luz que un material con un valor de 5.

La resistencia a la abrasión (mecánica) se determina con ayuda de un alfiler. Se fija el material a un soporte y se pone un alfiler envuelto en gasa nueva en contacto con la superficie sometida a prueba. Al cabo de cierto número de ciclos, se inspecciona a fondo el material sometido a prueba para detectar cualquier deterioro. Por lo general, esta prueba se realiza sobre la cubierta y la página de datos.



Prueba de plegado dinámico

Prueba de estampado por impacto

Figura 5-15: La prueba de plegado dinámico (bolsillo trasero) y la prueba de estampado por impacto fueron descritas por *Jan van den Berg en Keesing Journal Document & Identity* (pruebas en tres tipos de pasaportes electrónicos).
(Cortesía de *Sdu Identification*, Haarlem, Países Bajos)

Para comprobar la resistencia a los productos químicos, se sumerge el documento en soluciones químicas en forma líquida durante un periodo

[5] Esto permitiría verificar en la mayoría de los casos que la cara del titular todavía se asemeja a la imagen retratada en el documento de viaje.

de tiempo determinado, transcurrido el cual se inspeccionan los daños. Mediante otra prueba, se estudia la interacción entre el material de base y la técnica de personalización. En algunos casos, los documentos se someten a variaciones de presión y/o temperatura y posiblemente también de tensión mecánica (véase la Figura 5-14). El diseño de las máquinas de personalización ha de estar muy bien ajustado a los documentos que vayan a personalizarse, a fin de evitar problemas graves durante la implantación del concepto. Un ejemplo típico es la impresora de chorro de tinta. El papel del documento tiene que ser capaz de absorber las gotitas de tinta sin que se estropee la imagen impresa, pues de lo contrario podría dar lugar a una imagen borrosa.

5.5.2 Manipulaciones fraudulentas

También se analiza el riesgo de fraude de los materiales elegidos para la producción de documentos. Si la composición del documento y su personalización están expuestas a riesgos potenciales, se puede recurrir a un laboratorio especializado para que lleve a cabo manipulaciones químicas y mecánicas similares a las realizadas por los falsificadores profesionales. Dado que no existen normas que expliquen qué protocolos hay que observar, la fiabilidad y reproducibilidad de estas pruebas es proporcional a la experiencia y las aptitudes del examinador. El papel del experto en documentos es vital para el éxito de todo el proceso de prueba. En el laboratorio, debe examinar y ensayar la compatibilidad de los materiales y la forma en que interactúan, buscando las mejores soluciones para incrementar y mejorar la seguridad general de un documento. Hay que pensar bien la combinación de materiales, técnicas y elementos de seguridad para garantizar su plena compatibilidad y protección durante toda la vida útil del documento. Ésta suele estar subordinada al resto del proceso de fabricación del documento, pero desempeña un papel decisivo en la consecución de un comportamiento efectivo por parte del producto final – es decir, del documento seguro. El método de prueba supone un análisis de la forma en que reaccionan los documentos a diversas condiciones de manipulación. Esto incluye estudiar su respuesta a las pruebas de durabilidad, resistencia, fotosensibilidad, así como su reacción a la exposición deliberada a disolventes químicos, bases, ácidos, etc., con el objetivo último de ser falsificados.

5.5.3 Compatibilidad con las normas

Como se ha indicado en el Capítulo 2, las normas internacionales buscan la interoperabilidad. Las normas ISO describen las pruebas aplicables a las tarjetas de plástico de formato ID-1 (ISO/IEC 10373-1:2006).

Como lo que más interesa a la OACI son los documentos de viaje, se añade una nueva serie de pruebas de durabilidad, en especial para los pasaportes electrónicos, al Documento 9303 Informes Técnicos (protocolo RF y norma de pruebas de aplicación para pasaportes electrónicos).

Una vez concluidas las pruebas, el desarrollador del documento recibe el primer proyecto de las especificaciones del documento, que constituye una información importante para la producción final a gran escala del documento.

■ 5.6 Preparación de la producción a gran escala

Antes incluso de que esté finalizado y aprobado el diseño gráfico, comienzan los preparativos para la producción en serie. En función de la naturaleza del proyecto, intervendrán en el mismo otras disciplinas internas del proveedor.

En la primera etapa, esos preparativos pueden suponer la redacción de las especificaciones finales de los materiales y equipos, la celebración de los contratos con los proveedores, la emisión de los pedidos de equipos y materiales, la aplicación de medidas para garantizar la capacidad de producción necesaria, y la redacción de los objetivos de control y de calidad.

En la segunda etapa, hay que tomar medidas para alojar los nuevos equipos y técnicas, y entretanto elaborar los planes de producción, pruebas y aceptación. Durante esta etapa, también hay que supervisar el avance y la calidad de los equipos incorporados, y se deben empezar a suministrar y probar los materiales para comprobar que cumplen las especificaciones. También se ensayan todos los nuevos métodos de

producción necesarios, tras lo cual pueden ser aprobados y puestos en práctica.

Esta etapa requiere una interacción intensa entre los desarrolladores del proyecto, que son los encargados de desarrollar el nuevo documento, y los procesos de producción, que implican a todas las disciplinas necesarias.

La tercera etapa se centra en la selección y capacitación de personal, así como en la implantación de nuevos conocimientos y aptitudes en la organización del proveedor. Esta etapa normalmente entraña programas intensivos de pruebas de equipos, materiales y procedimientos, que desembocan en una prueba de aceptación general por parte de la entidad promotora, en la que se evalúa el funcionamiento y la calidad de todos los subprocesos.

En la preparación de la producción a gran escala, es importante que la entidad promotora y el productor alcancen un acuerdo claro sobre la calidad del producto. Por lo que se refiere al producto impreso, la entidad promotora y el diseñador gráfico se tienen que poner de acuerdo sobre el resultado final de cada hoja impresa producida en serie. Hay que repetir este proceso para cada una de las características pertinentes del producto definitivo. Se suele tratar de características estéticas respecto de las cuales no existen normas internacionales.

El productor tiene la responsabilidad de presentar muestras que sean representativas de toda la producción, es decir, muestras fabricadas en buenas condiciones técnicas de producción y que, por consiguiente, se puedan repetir en las producciones futuras, que se pueden extender durante varios años. El productor tiene que velar por que las aprobaciones que acaban de mencionarse se documenten correctamente para su futura impresión.

■ 5.7 Garantía de calidad

El binomio garantía y calidad es bien conocido por la mayor parte de los directores de proyecto. ¿Qué interpretación personal le podrían dar en el ámbito de los documentos de seguridad? El párrafo siguiente describe una situación ficticia que, sin embargo, ilustra la necesidad de la garantía y calidad.

Imagine un edificio altamente protegido en algún país. Es el fin de semana anterior al comienzo de la expedición de un nuevo documento de viaje. Debido a un calendario muy apretado, durante los dos últimos días se han hecho grandes esfuerzos de ajuste fino de las máquinas para conseguir un nivel de calidad aceptable en la división de personalización. A última hora de la tarde del viernes, hay un corte de corriente eléctrica en todo el edificio. El generador de emergencia se pone inmediatamente en funcionamiento, pero se pierde la configuración del ajuste de las máquinas de personalización. El último operario de servicio busca las copias de seguridad para restaurar los últimos ajustes. Desafortunadamente, el técnico de soporte responsable de hacer las copias de seguridad está de baja desde el lunes, y los soportes magnéticos que hay encima de su mesa no están etiquetados en el orden debido. El supervisor acaba de montarse en el tren, y el teléfono móvil del director de producción está fuera de cobertura.

En lugar de sufrir un ataque de pánico, el operador pide al guardia de seguridad que se reúna con él frente a la caja fuerte. Juntos abren la caja, donde se guardan las copias de seguridad correctas y la documentación conexa. Entretanto, se han puesto en marcha las máquinas y el operador carga los últimos ajustes realizados ese día. Por fortuna, el supervisor había hecho la copia de seguridad habitual justo antes de marcharse...

¿Cómo puede asegurar una organización que una situación determinada se maneje conforme a los acuerdos suscritos con el cliente? ¿Cómo puede el cliente comprobar que todo está en orden para obtener el producto previsto con el nivel de calidad acordado?

Todo depende de la documentación y la comunicación. La garantía de calidad requiere que las personas que intervienen en un proceso de calidad conozcan las respuestas a las preguntas "quién, qué, dónde, cómo, cuándo, por qué" si se encuentran ante una situación (extra) ordinaria. Eso significa que es necesario contar con una descripción detallada del producto y del proceso de producción, es decir que esa información tiene que estar a disposición de las personas que la necesitan; que los ajustes queden registrados y que se haya implantado procedimientos operativos en la organización.

5.7.1 Especificaciones del producto

Como hemos visto en los Capítulos anteriores, un documento seguro es el resultado de un proceso a través del cual diversos componentes semiacabados conforman el producto final. La empresa que reúne los componentes para fabricar el producto final aportando sus propios conocimientos especializados desempeña un papel de coordinación fundamental en el desarrollo y suministro de los componentes, con respecto al aspecto, las especificaciones y los servicios prestados. Naturalmente, la entidad promotora está directamente involucrada en todo esto.

La producción de documentos seguros exige que se documenten las especificaciones de calidad y de los componentes. Para cada aspecto que describe el componente, así como el producto final, se definen valores nominales y tolerancias, es decir, las especificaciones del producto. El productor redacta las especificaciones del producto en cuanto concluye la etapa de desarrollo. A continuación, el productor alcanza acuerdos con los proveedores con relación a las especificaciones y las normas de calidad de sus productos.

5.7.2 Inspección por atributos en un marco de fabricación

El concepto de "*Meten es weten*", famoso dicho holandés, se podría traducir como "se puede controlar lo que se puede medir".

Además del pertinente control del proceso de producción, a lo largo de todo el proceso de fabricación se llevan a cabo varios controles con

objeto de inspeccionar cualitativa y cuantitativamente las características de los productos y comprobar que cumplen las especificaciones. El control de calidad se lleva a cabo en tres etapas del proceso:

1. Cuando se compran las materias primas, para comprobar su conformidad con las especificaciones.
2. En la etapa de producción: se controlan las características de los productos semiacabados para limitar los rechazos.
3. Al final del proceso de fabricación: cuando se comprueban los productos finales antes de su despacho al cliente.

Es necesario alcanzar acuerdos relativos a la calidad de cada aspecto de cada uno de los componentes independientes, para garantizar una calidad constante en cada componente. Sin embargo, por lo general, un cliente de documentos de seguridad está menos interesado en las características y especificaciones de un componente que en la calidad del producto acabado, que es el resultado de la calidad acumulada de los componentes independientes. El control de calidad del producto final forma parte integrante de todo el sistema de calidad del productor, y la determinación de las propiedades de los materiales y procesos constituye una parte importante de dicho sistema.

El operador de la maquinaria de producción lleva a cabo controles de calidad durante el proceso de producción, con objeto de ajustar el proceso en cuanto aparece la primera desviación. Para algunos productos semiacabados, una persona del laboratorio de pruebas interno puede comprobar algunas características que requieran mayores conocimientos técnicos o herramientas especiales. Si los atributos requieren comprobaciones visuales, el productor puede optar por crear modelos que representen los valores nominales y modelos de las tolerancias máximas y mínimas.

La ISO ha elaborado todo un conjunto de métodos de inspección diferentes. Los documentos de seguridad no son un simple producto de consumo, dado que se elaboran a medida. Por consiguiente, el programa de inspección más adecuado es el plan de muestreo llamado inspección por atributos.

Este tipo de plan está concebido fundamentalmente para su utilización sobre una serie continua de lotes o partidas. La inspección es el proceso de medir, examinar, probar o cotejar por otra vía la muestra del producto con relación a los requisitos aplicables a éste. Un "plan de muestreo de aceptación de lote" consiste en un programa de muestreo y una serie de reglas para tomar decisiones. La decisión, basada en el recuento del número de Artículos defectuosos detectados en una muestra, puede ser la aceptación del lote, el rechazo del lote, o incluso, para programas de muestreo múltiple o secuencial, la toma de otra muestra y luego la repetición del proceso de decisión. En la inspección por atributos, la unidad de producto se clasifica simplemente como conforme o no conforme, o se cuenta el número de no conformidades de la muestra con respecto a un requisito determinado o a una serie de requisitos.

El nivel de calidad aceptable es el porcentaje de defectos que constituye el requisito básico de calidad del producto suministrado. El productor querrá diseñar un plan de muestreo concebido de tal forma que exista una alta probabilidad de aceptación de un lote que tenga un nivel de defectos inferior o igual al nivel de calidad aceptable.

La norma ISO 2859 establece el marco de los procedimientos de inspección por atributos.

5.7.3 Calidad del programa computadorizado

Al igual que el documento material, que describe el cliente, diseña el productor, y revisan y prueban ambos, el desarrollo de los programas computadorizados requiere etapas similares. La parte más difícil de explicar en el ámbito de este libro es sin duda la etapa de prueba, que es una métrica de capital importancia en la calidad del programa computadorizado, según la norma ISO 9126.

En la prueba de los programas computadorizados se comprueba principalmente que el código hace lo que se espera que haga, conforme a las especificaciones y sin fallos. La preparación de un protocolo de prueba exige una buena comprensión del objeto sometido a prueba. Esto significa que el diseñador supervisa las funciones del programa

computadorizado que le permitirán definir un número significativo de casos de prueba. La labor del verificador consiste en llevar a cabo una serie de acciones predefinidas para cada caso de prueba, anotar el resultado y compararlo con el resultado esperado. Si obtiene resultados inesperados, probablemente el verificador consulte al técnico de programa computadorizadocuál es la interpretación correcta. La actividad de prueba puede obedecer a criterios de aceptación o de salida, que permiten al verificador llegar a un punto en el que se cumplan.

5.7.4 Calidad de la personalización

De acuerdo con el principio de fiabilidad, habría que supervisar constantemente la calidad de la personalización, tanto si la lleva a cabo una entidad pública como un proveedor.

Los elementos más decisivos de los documentos de identidad y de viaje personalizados son los relacionados con la persona: la firma, el retrato y demás información biométrica (por ejemplo, huellas dactilares, iris). En la práctica, estos son los elementos utilizados para comprobar la identidad del titular del documento. Por consiguiente, tienen que ser lo suficientemente reconocibles como para poder ser utilizados con ese fin. Además, es fundamental que esos elementos cumplan las normas y acuerdos internacionales.

Con independencia del proceso de adquisición de datos, hay que comprobar al menos tres aspectos de la información variable en las etapas de introducción y de salida: que sea exacta, que esté completa, y que cumpla las especificaciones formales (por ejemplo la posición de la información variable).

Así pues, en el entorno de personalización también se establecen procedimientos operativos. El personal de personalización recibe capacitación en materia de evaluación de la calidad, y tiene acceso a normas de calidad definidas y a instrumentos de apoyo.

Referencias

ACPA
2006 *Australian Payment Clearing Association, Payment Fraud Statistics, Methodology paper, Sydney.*

Billmeyer F. W.
1984 *Textbook of Polymer Science, 3rd Edition, John Wiley & Sons Inc*., Nueva York.

Canon
2006 http://www.canon.com/technology/electrophotography/index.html

Fahrmeir A.
2001 "*Government and Forgers: Passports in Nineteenth-Century Europe*", *Documenting Individual Identit*y, Caplan J. y Torpey J. eds., *Princeton University Press, Princeton*.

Fidis
2006 *Budapest Declaration on Machine Readable Documents*, http://www.fidis.net/press-events/press-releases/budapest-declaration/, Bruselas.

Hospel W. G. J. M.
1998 *Application of laser technology to introduce security features on security documents in order to reduce counterfeitin*g, Proc. *Conference on Optical Security and Counterfeit Deterrence Techniques* II, SPIE vol. 3314:254-259, San José.

OACI
2004 Informe técnico V 2.0 Empleo de biometría en los documentos de viaje de lectura mecánica, aprobado por el TAG 15 el 21/5/2004.

ICMA
2006 http://www.icma.com/info/Polycarbonate5605.htm, *International Card Manufacturers Association, Princeton Junction.*

Kodak
2006 http://www.kodak.com/country/US/en/digital/dlc/book3/chapter1/digFundOutput6.shtml

Ponds S. F.
2002 *Inkjet Technology and Product Development Strategie*s, *Torrey Pines Research, Carlsbad*.

Straus S.
2006 http://www.polymernotes.org, Kranj, Eslovenia

van den Berg J. y Augustinus A.
2000 "*New optical security features in plastic documents", Proc. Conference on Optical Security and Counterfeit Deterrence Techniques* III, San José, *SPIE* vol. 3973:167-175, San José.

Van den Berg J.
2004 *testing Three types of e-passports. Keesing Journal of Documents & Identity, a magazine about developments in the security industry*. Número 8, 2004.

Wikipedia
2006 http://en.wikipedia.org/wiki/Polymer_banknote

CAPÍTULO 6

LA IDENTIDAD Y SU VALOR

> "Aquí señalaría que buena parte de lo que un tribunal rechaza como prueba constituye la mayor evidencia para el intelecto"
> *Edgar Allan Poe, El misterio de Marie Roget (1842)*

6.1 Introducción

El estudio de las huellas dactilares como medio de identificación positiva por científicos tan destacados como Sir William Herschel, el Dr. Henry Faulds, Sir Francis Galton, Sir Edward Richard Henry o el Dr. Edmond Locard fue el punto de partida de la ciencia de la individualización, como la llaman algunos criminalistas, o de la ciencia forense, como la llaman otros (Kirk, 1963).

La primera parte de este Capítulo aborda el concepto de identidad y su aplicación a la ciencia forense. El contenido de esa base teórica es un breve resumen del único trabajo de investigación destacado realizado sobre este tema en concreto, a saber, la brillante pero subestimada tesis doctoral del Dr. Quon Yin Kwan titulada "*Inference of identity of source*" (Kwan, 1977). La segunda parte ilustra la confusión asociada a la noción de identidad en la ciencia forense. La tercera parte contiene una descripción del proceso de individualización forense basado en el método hipotético-deductivo, y la última parte propone un marco para el diseño de un sistema informático de individualización biométrica forense.

Nota editorial: Este capítulo fue publicado por Didier Meuwly en Science and Justice en el 2006 (vol. 46 n°4).

■ 6.2 La identidad

6.2.1 Definición

"En la ciencia forense y el derecho, la identidad es el conjunto de características a través de las cuales un ser humano define su propia personalidad y se distingue de todos los demás. En este contexto, la determinación de la identidad de un individuo constituye la labor forense denominada identificación. Un ser humano puede ser similar a otros, o a otra persona, hasta el punto de inducir errores; pero sólo puede ser idéntico a una persona, es decir, a sí mismo. El reto de la identificación reside en la concienzuda discriminación de los elementos de similitud de los elementos de la verdadera identidad".[1] (Locard, 1909)

6.2.2 Ambigüedad

El término "identidad" tiene un carácter dual, y esa dualidad engendra ambigüedad. Cuando se utiliza el concepto de fuente, haciendo referencia a un objeto de interés, para designar una clase de entidades individuales en las que podría tener su origen el objeto en cuestión, dicho concepto se refiere a la identidad cualitativa. Esto se debe al hecho de que una clase se define en función de la identidad de las propiedades de sus miembros. La labor mediante la cual se determina que una clase es la fuente se denomina científicamente "clasificación" o "identificación". Cuando el concepto de fuente se utiliza para designar una entidad individual particular en la cual tiene su origen un objeto, dicho concepto se refiere a la identidad numérica. La denominación científica de la operación mediante la cual se determina que una entidad individual particular es la fuente de un objeto es la "individualización", si bien es frecuente que dicha operación se designe indebidamente como "identificación" en la ciencia forense.

[1] Traducido en el original libremente al inglés de la cita original en francés: "*En police scientifique et en droit, l'identité est l'ensemble des caractères par lesquels un homme définit sa personnalité propre et se distingue de tout autre. Dans ce dernier ordre d'idées, établir l'identité d'un individu est l'opération policière ou médico-légale appelée identification. Un homme peut être semblable à plusieurs autres, ou à un autre, au point d'amener des erreurs ; il n'est jamais identique qu'à un seul, à lui-même. C'est à discriminer avec soin les éléments de ressemblance des éléments d'identité que consiste le problème de l'identification*".

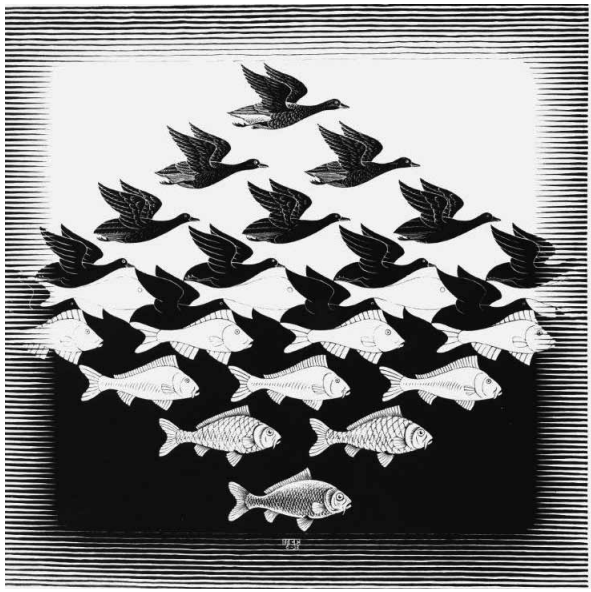


Figura 6-1: M. C. Escher, Cielo y agua I, 1938.
El término “identidad” es dual por naturaleza y esa dualidad induce a la ambigüedad.

En la ciencia forense existe mucha confusión en torno a los términos “identidad”, “identificar” e “identificación”. Así se demuestra claramente en la práctica popular cuando se dice que se “ha identificado al autor de un crimen a partir de sus huellas dactilares”. No se identifica al autor de un crimen, sino que se le individualiza. Lo que demuestran las huellas dactilares es la individualidad (Tuthill, 1994; Doddington, 1985). Kirk (1963) también destaca esa confusión, si bien concluye:

“El verdadero propósito de toda ciencia forense consiste en determinar la individualidad o en acercarse a ella tanto como lo permita el estado actual de avance de la ciencia. La criminología es la ciencia de la individualización. Lo que en última instancia interesa al criminalista no es la similitud entre dos objetos, sino entre sus fuentes respectivas”.
.
Por consiguiente, en la ciencia forense, individualizar a un ser humano a partir de los datos biométricos consiste en última instancia en determinar si un individuo es la fuente del rasgo biométrico analizado.

6.2.3 La identidad en la ciencia forense

Según Kwan, "lo que se entiende por identidad de la fuente depende de a qué se refiera la fuente. Si la fuente hace referencia a la clase, identidad es lo mismo que identidad cualitativa, y si la fuente hace referencia a un individuo, la identidad de la fuente es equivalente a la identidad numérica. Esta distinción entre los dos tipos de identidad es coherente con las formas de identidad clásicas diferenciadas por los filósofos de todos los tiempos. La justificación del enfoque desde una perspectiva filosófica es que de ese modo se llega a conocer el problema fundamental de la identidad de la fuente" (Kwan, 1977).

6.2.4 Diferenciación entre identidad numérica e identidad cualitativa

La identidad cualitativa se establece cuando una serie de propiedades concuerda en dos objetos. La identidad numérica se demuestra determinando la continuidad en el tiempo. Un ejemplo bien conocido de la identidad numérica en la ciencia forense es la cadena de la prueba, o cadena de custodia. Para mantenerse, la cadena de la prueba exige una demostración de que el Artículo en cuestión es la misma entidad individual desde el momento de su recogida en la escena del crimen hasta el momento de su presentación al tribunal. Como la identidad cualitativa no se determina mediante este criterio de continuidad, es relativa. La relatividad de la identidad cualitativa recae en el observador, y en especial con respecto a la selección de propiedades que éste elige para caracterizar los objetos (Kwan, 1977).

La principal característica diferenciadora entre la identidad numérica y la identidad cualitativa es el tiempo. El tiempo remite al absurdo la identidad de los objetos, puesto que dos objetos no pueden ser un mismo objeto simultáneamente. La identidad de la fuente es una relación que implica el tiempo, debido a la necesidad de demostrar la continuidad en el tiempo de los objetos procedentes de una misma fuente. La identidad cualitativa, por su parte, es independiente del tiempo. El tiempo implica que la identidad numérica es compatible con el cambio, mientras que la identidad cualitativa no lo es.

"Una cosa sólo puede ser idéntica a sí misma, y nunca a ningún otro objeto, pues los objetos del universo son únicos. Si esto no fuera cierto, no sería posible la identificación en el sentido utilizado por el criminalista" (Kirk, 1963). Para convencerse de que la identidad numérica es compatible con el cambio, tome su documento de identidad de hace diez años, compare su cara con la foto de la cédula de identidad incluida en ese documento de identidad, y observe los cambios. Eso demuestra que dos objetos con cualidades distintas, existentes en distintos momentos, pueden ser numéricamente idénticos. Esta observación ilustra que la identidad numérica no conlleva la identidad cualitativa y, viceversa, que la identidad cualitativa no conlleva la identidad numérica. Con ello se demuestra la ausencia de una relación lógica entre identidad numérica e identidad cualitativa.

■ 6.3 Confusión entre identidad numérica e identidad cualitativa en la ciencia forense

El examen de la relación entre identidad cualitativa e identidad numérica brinda perspectivas diferentes sobre la identidad. Aunque en su obra Leibniz nunca enunció explícitamente una ley que relacione identidad cualitativa e identidad numérica, dos interpretaciones distintas de su posición sobre la identidad han creado una confusión considerable. La posición de Leibniz sobre la identidad se expresa en dos máximas formales: la ley de los idénticos y la ley de la identidad de los indistinguibles. La primera afirma que cuando dos cosas son numéricamente idénticas simultáneamente, toda característica presente en la una también está presente en la otra.

Esta interpretación no plantea problema, pues, según Wittgenstein, se trata simplemente de la misma cosa repetida dos veces, pero en mundos distintos (Kwan, 1977). Este último autor, por su parte, se limita a equiparar la identidad cualitativa con la identidad numérica, lo cual no constituye una relación válida, como acabamos de explicar. Sin embargo, pese a la cuestionable validez de esta segunda interpretación, se ha convertido en un principio general de la ciencia forense.

6.3.1 Principio general de la singularidad

A. Dogma…

La idea de que se puede deducir la identidad de la fuente basándose en la identidad cualitativa y en la suposición de la singularidad de la fuente sigue contando con un amplio respaldo entre la comunidad forense (Tuthill, 1994). En la ciencia forense, la mayoría de las veces se percibe el proceso de individualización como un proceso de riguroso razonamiento deductivo (Taroni, 1997): como un silogismo compuesto por una premisa mayor, una premisa menor y una conclusión[2].

La premisa mayor es el principio de la singularidad aplicado a las propiedades de una fuente y a las propiedades del objeto generado por dicha fuente; la premisa menor es la observación de la correspondencia de las propiedades observadas entre la fuente y el rastro, en tanto que la conclusión es que la fuente y el rastro tienen un origen común debido a la correspondencia entre las propiedades observadas.

B. … pero con deficiencias

Sin embargo, el principio general de la singularidad asumido en la ciencia forense se debe calificar de dogma, puesto que "este principio de identificación forense" se basa en un razonamiento inductivo. Se basa en una línea de razonamiento que pasa de las declaraciones particulares (basadas en la observación o la experiencia) a las teorías o leyes universales. Tanto Locard (1924) como Eco (1982) son conscientes de esta mala utilización del razonamiento inductivo en la ciencia forense, cuando invocan la octava regla del silogismo según Aristóteles: no se puede proceder a una deducción a partir de dos premisas menores.

Esta exposición lógica fue desarrollada inicialmente por *Sextus Empiricus* (150-230 d.C.), y Hume adaptó esta crítica de la aplicación de la inducción a la noción de causalidad. Por consiguiente, no se

[2] Siguiendo la primera regla del silogismo, según Aristóteles, *"Terminus esto triplex: medius, majorque, minorque*", un silogismo, para ser válido, debe componerse de un principio general, denominado premisa mayor, de una observación particular, denominada premisa menor, y de la deducción, denominada término medio o conclusión.

puede considerar que la inducción sea un razonamiento riguroso para la individualización en la ciencia forense, porque lo que es cierto en lo particular no lo es necesariamente en lo general. El uso indebido de la inducción crea la ilusión de que la ciencia corrobora conclusiones categóricas de identificación o exclusión (Evett, 1996).

C. El criterio de la falsabilidad empírica

Popper utiliza la posición de Hume, pero sostiene que es imposible la verificación completa de cualquier aseveración científica; por consiguiente, tampoco es posible la verificación completa del principio general de la singularidad aplicado a la ciencia forense. Popper refuta el criterio de verificabilidad científica, y en su lugar propone el criterio de falsabilidad empírica como criterio delimitador.

El proceso de razonamiento de Popper se basa en una consideración lógica fundamental: es imposible demostrar el enunciado de un principio general a partir de enunciados particulares, pero en cambio sí es posible demostrar su falsedad. Refutar una hipótesis demostrando su falsedad equivale a demostrar que el enunciado de un principio general es falso porque uno o varios casos lo contradicen: lo que es falso en particular es falso en general. Sin embargo, el fracaso del intento de demostrar la falsedad de la hipótesis de singularidad nunca demostrará que el principio sea cierto, ahora bien, si supera las pruebas, la hipótesis puede alcanzar un grado de corroboración suficiente para permitir su utilización como base de aplicación práctica, descrito por Popper como grado de "verosimilitud".

6.3.2 El principio de la singularidad aplicado a la individualización biométrica

A. Dogma…

Por lo general, tanto en las aplicaciones forenses como comerciales de la biometría se acepta sin discusión la singularidad de las características utilizadas para la individualización biométrica (Doddington, 1985). Además, en la ciencia forense, el principio de la singularidad aceptado para las propiedades de la fuente a menudo se extiende sin cuestionamiento a las propiedades del rastro. Por ejemplo, se supone

la singularidad en el caso de la huella dactilar (fuente) y de la marca de la huella dactilar (rastro), de la cara (fuente) y de la imagen de la cara grabada o en vivo (rastro) así como en el caso de la voz (fuente) y de la grabación sonora del habla (rastro).

B. …pero con deficiencias

El criterio delimitador de la falsabilidad empírica desarrollado por Popper choca en la mayor parte de los casos con la hipótesis de la singularidad de las características utilizadas para la individualización biométrica. La diversa medida en que las diferentes características biométricas pueden cumplir el criterio delimitador de falsabilidad se experimenta tanto en la vida diaria como en la práctica forense, como se demuestra en los ejemplos siguientes.

C. El supuesto de la singularidad de la impresión de las huellas dactilares rodadas completas

Los sistemas automáticos de identificación de huellas dactilares (AFIS, por sus siglas en inglés) se vienen utilizando desde hace 30 años. Se incluyen en las bases de datos de penados y de solicitantes de asilo para detectar a los delincuentes reincidentes e impedir la multiplicidad de peticiones de asilo. En estas dos situaciones, se realiza una impresión de las huellas de los diez dedos del sospechoso o del solicitante de asilo, y se hace una búsqueda de dos de los dedos, por lo general el índice y el corazón de la mano derecha, en el registro de huellas dactilares. Generalmente, en la búsqueda automática no se utilizan los otros ocho dedos, pero cuando el sistema propone un candidato, el examinador de huellas dactilares los puede utilizar para demostrar la falsedad de la supuesta identidad basada en la comparación automática de los dos primeros dedos.

Por lo que sabemos, este procedimiento de individualización basado en diez impresiones a tinta de las huellas dactilares (consideradas fuentes secundarias, siendo las fuentes primarias las verdaderas protuberancias papilares) resulta sumamente difícil de falsificar. Por supuesto, esta consideración sólo tiene en cuenta el resultado del proceso automático, y no el resultado del proceso completo, incluida la interacción humana con

el AFIS, ya que los errores humanos debidos a errores administrativos u otros son intrínsecos de la actividad humana.

Desde nuestro punto de vista, el supuesto de la singularidad de las impresiones de las huellas dactilares formulado inicialmente por Herschel y Galton (Bolt, 1970) alcanza un "grado de verosimilitud" suficiente y, por consiguiente, vuelve válido el supuesto de que la impresión rodada completa de la huella dactilar es una representación del dedo real suficientemente fiable para la individualización humana. Este enunciado es de capital importancia a la hora de elegir las características biométricas pertinentes para la creación de documentos de identidad.

D. El supuesto de la singularidad de la marca de la huella

En cambio, la práctica forense está salpicada por varios casos de individualización errónea de inculpados basada en la comparación de marcas de huellas (rastros) con la impresión a tinta de huellas dactilares realizada por expertos en huellas dactilares. Aparte de la "individualización errónea a través de huellas dactilares en el caso de los atentados con bomba en el tren de Madrid" en el que Brandon Mayfield, abogado musulmán de Oregón, fue erróneamente asociado con huellas encontradas en el lugar del atentado (Stacey, 2004), cabe citar el caso escocés de H. M. Advocate contra Shirley McKie.

En el segundo caso, y por primera vez desde la aprobación de la norma de 16 puntos, se ha impugnado una identificación completa de una marca latente ante un tribunal judicial del Reino Unido, y la impugnación fue estimada por un veredicto unánime (Grieve, 2000). Por consiguiente, desde nuestro punto de vista, el supuesto de la singularidad de la marca de la huella no alcanza un "grado de verosimilitud" suficiente.

E. El supuesto de la singularidad de la cara y la voz humana

También es cuestionable la singularidad de las propiedades de la cara humana, pues no se conoce ni se puede suponer ninguna propiedad idiosincrásica para esta modalidad biométrica. Por lo que se refiere a la voz, aunque sea plausible la hipótesis según la cual no existen dos seres humanos que hablen exactamente igual, hasta la fecha no se ha aportado

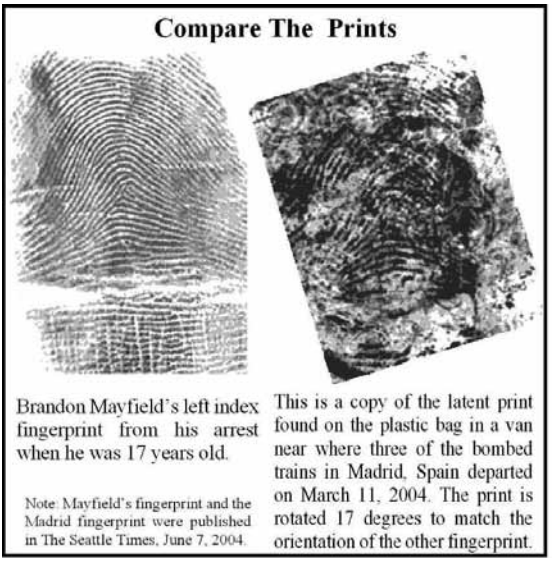


Figura 6-2: Huellas dactilares del caso Brandon Mayfield. La huella dactilar de la izquierda pertenece a Brandon Mayfield, mientras que la de la derecha fue encontrada en el lugar donde se produjeron los atentados de la estación de ferrocarril de Madrid.

ninguna demostración a gran escala de la extensión de la idiosincrasia en una comunidad homogénea de hablantes para avalar esta hipótesis (Nolan, 1991). Por consiguiente, el supuesto de la singularidad no alcanza un "grado de verosimilitud" suficiente para la cara y la voz humanas.

F. El supuesto de la singularidad de las propiedades de los rastros de caras y voces humanas

La consideración que acabamos de hacer también es cierta en el caso de las propiedades de los rastros de caras y voces. La experiencia cotidiana, así como los resultados de la psicología aplicada y de la percepción artificial confirman las limitaciones de la capacidad de individualización biométrica basada en el reconocimiento de la cara, el reconocimiento de la voz o la combinación de ambas por seres humanos y por máquinas (Clifford, 1980; Boves, 1998). Esta situación resulta especialmente pertinente en la ciencia forense, donde normalmente el rastro de la voz y la cara es de calidad limitada, como lo es por ejemplo la calidad del grabado sonoro de una conversación telefónica, de un

grabado de vídeo a través de circuito cerrado de televisión, o de una fotografía de pasaporte.

Esta aseveración no significa que las huellas dactilares, los rastros de caras y los rastros de voces no se puedan utilizar o sean inadecuados para la individualización biométrica en la ciencia forense. Sólo establece claramente los límites de la certidumbre que cabe esperar, dependiendo de la calidad del rastro y de la eficiencia del proceso de individualización biométrica. La falta de constancia en la cara y en la voz, así como en las marcas de las huellas dactilares, pone de relieve la existencia de una variabilidad interna de la fuente, además de la variabilidad existente entre fuentes, que también se debe tener en cuenta en el proceso de individualización forense.

Dado que el proceso de individualización forense no se puede considerar como un proceso deductivo basado en la identidad cualitativa y en el principio general de la singularidad, es necesario considerar otro enfoque para inferir la identidad de la fuente.

6.3.3 Aplicación de esquemas de decisión binaria a la individualización biométrica

Los esquemas de decisión de discriminación y clasificación binaria son considerados igualmente pertinentes para la individualización biométrica forense debido al consenso que existe en la comunidad forense sobre la aplicabilidad de los principios de la identidad cualitativa y la singularidad. Estos esquemas de decisión corresponden al proceso de verificación (discriminación) y al proceso de identificación (clasificación) utilizados en las aplicaciones comerciales de la biometría, de los cuales se espera una decisión binaria pero relativa sobre la identidad de la fuente (Doddington, 1985).

A. Discriminación

La tarea de discriminación utilizada como esquema de decisión para la individualización forense consiste en el proceso de aceptación o rechazo de la hipótesis de que una fuente ha generado el rastro. La decisión de discriminación entre el rastro y la fuente depende de un umbral. La discriminación se interpreta como rechazo, y la no discriminación como

aceptación. Este concepto de identidad no coincide con la definición de la individualización forense; si la probabilidad de coincidencia aleatoria no es nula (corolario del umbral), la conclusión "se ha identificado la fuente" es inadecuada y equívoca (Champod y Meuwly, 2000).

B. Clasificación

La tarea de clasificación utilizada como esquema de decisión para la individualización forense consiste en el proceso de determinación de cuál es la fuente del rastro en un grupo cerrado de fuentes. Sobre un grupo cerrado de fuentes no puede realizarse una clasificación, puesto que la evaluación de la credibilidad de la exhaustividad de las fuentes incluidas en el conjunto no entra en las obligaciones del científico forense. Además, parece injusto revelar únicamente la identidad del mejor candidato, sin aportar la prueba obtenida con respecto a otros, que puede no proceder exclusivamente de la serie cerrada de fuentes comprobadas. Para superar esta deficiencia, la clasificación se debe realizar sobre un grupo abierto de fuentes, si bien ese marco sigue entrañando una decisión de discriminación final basada en un umbral y adolece de los mismos inconvenientes conceptuales que la tarea de discriminación (Champod y Meuwly, 2000).

C. Paradoja en el uso de los esquemas de decisión binaria con fines forenses

Ningún método de discriminación o clasificación es perfecto. Una decisión de discriminación puede adolecer de dos tipos de error: el rechazo indebido (error de tipo I), cuando se descarta la fuente verdadera del rastro, y la aceptación indebida (error de tipo II), cuando se acepta una fuente errónea como fuente del rastro. Una decisión de clasificación sólo puede incurrir en un error de aceptación indebida o error de tipo II.

En el ámbito de las aplicaciones comerciales de la biometría, la evaluación de los métodos de discriminación o clasificación se basa en los costos calculados para uno o ambos tipos de error, en función de la tarea considerada. En la ciencia forense, por otra parte, se da una paradoja en la creencia de que las decisiones pueden y deben ser binarias y libres de error (absolutas) al mismo tiempo.

La inadecuación de los esquemas de decisión binaria para inferir la identidad, y la paradoja relacionada con su uso, constituyen buenos argumentos para buscar otro enfoque respecto de la inferencia de la identidad de la fuente en la ciencia forense. Cuando el concepto de fuente se refiere a una clase de entidades en las que puede tener su origen un objeto, la cuestión de cómo se identifica la fuente no deja de ser una mera cuestión epistemológica sobre cómo se llega a conocer la identidad cualitativa, a saber, a través de un conjunto de características, como se ha explicado anteriormente. Cuando el concepto de fuente significa una entidad individual concreta en la que un objeto tiene su origen, la cuestión de cómo se identifica la fuente constituye un problema mucho más complejo.

La regla general para demostrar la identidad numérica consiste en demostrar la continuidad. Pero esta respuesta es impracticable para el forense, que casi nunca conoce a priori la fuente real, ni tampoco la ha visto. Como nadie puede garantizar la continuidad ininterrumpida entre la fuente y el objeto de interés desde la creación de ese objeto, no hay forma de conocer la identidad numérica de la fuente (Kwan, 1997). Básicamente, la identidad de la fuente permanece inferida en la ciencia forense.

6.3.4 El método hipotético-deductivo

A. Principios

La prueba no está subordinada al concepto de deducción. El método hipotético-deductivo es un enfoque sobre la inferencia de la identidad de la fuente mucho más viable que el método que consiste en la comparación de la identidad cualitativa seguida de una discriminación o una clasificación. Se puede describir como un proceso de formulación y comprobación; es decir, se formula una serie de hipótesis que luego se van comprobando y modificando cíclicamente hasta llegar a una hipótesis modificada irrefutable.

"Cuando se utiliza el método hipotético-deductivo, se empieza por plantear varias hipótesis que podrían explicar un fenómeno que se acaba de observar. Por lo general, las hipótesis se plantean después

de tener en cuenta los conocimientos generales sobre las propiedades de la clase de fenómenos de interés – los conocimientos previos. Sólo entonces se pasa a determinar cuál de las hipótesis de entre el conjunto plausible explica mejor el fenómeno en cuestión.

Las deducciones se realizan a partir de la hipótesis planteada, y sirven de base para proponer experimentos. Es decir, que si se pueden realizar predicciones a partir de esas hipótesis, también se pueden idear experimentos para comprobarlas. Este es el componente más valioso del método hipotético-deductivo. Si una hipótesis no concuerda con el cuerpo de conocimientos previos, o si la experimentación demuestra que sus predicciones son falsas, entonces se descarta. Y así se procede sucesivamente hasta que queda una única hipótesis que explica el fenómeno, cosa que no hace ninguna otra hipótesis alternativa" (Kwan, 1977).

El escritor norteamericano Edgar Allan Poe ya consideraba que el método hipotético-deductivo es un proceso de razonamiento pertinente cuando narró las aventuras del detective Dupin, en su trilogía de cuentos sobre este personaje. Como señala Locard (1924), Poe requería que el detective ideal combinara la imaginación del poeta (para definir la hipótesis) con el método del matemático (para comprobar la hipótesis). Incluso Sherlock Holmes repite que "cuando fallan todas las demás eventualidades, lo que quede debe ser cierto, por improbable que parezca" (Conan Doyle, 1953).

Aunque el proceso analítico descrito más arriba es ante todo un ejercicio de lógica que no guarda relación directa con la realidad, el método hipotético-deductivo exige la validación empírica de la hipótesis resultante (Truzzi, 1983).

La producción de una hipótesis es una condición necesaria pero no suficiente para que de ella parta el razonamiento. Como una hipótesis es intrínsecamente indemostrable, es necesario distinguir la hipótesis alternativa plausible de las hipótesis descabelladas. Ahora se reconoce que es imposible obtener criterios para definir *ex nihilo* la noción de

hipótesis plausible, porque esos criterios dependen en grandísima medida del problema analizado (Marquis, 1999).

Para las cuestiones referentes a la inferencia de la identidad de la fuente de un rastro, es posible definir dos hipótesis alternativas mutuamente excluyentes: la hipótesis inculpatoria (H_p) y la hipótesis exculpatoria (H_d). Una hipótesis se puede considerar plausible cuando el investigador la acepta como posible explicación.

B. Métodos de inferencia estadística

Los métodos de inferencia estadística complementan el método hipotético-deductivo asignando a las predicciones de las hipótesis una ponderación que facilita la selección de la hipótesis que mejor explica la fuente del rastro. No obstante, la estadística no desembocará en un proceso objetivo de identificación absoluta (Meuwly, 2001).

Un supuesto importante que conviene recordar es que cada método cuantitativo elegido para la inferencia de la identidad de la fuente se basa en la premisa de la identidad cualitativa. Significa que los rasgos utilizados para caracterizar un objeto deben ser seleccionados en función de los criterios de distinguibilidad, de la proporción entre la variabilidad interna de la fuente y la variabilidad entre las diversas fuentes, de la estabilidad en el tiempo, de la normalización y de la independencia (Kwan, 1977).

Entre los métodos de inferencia estadística, actualmente se considera que el enfoque de la razón de probabilidad basado en el teorema de Bayes constituye el marco más lógico para la inferencia de la identidad de la fuente en la ciencia forense. Se viene utilizando ya desde comienzos del siglo XX, como se hizo en el caso Dreyfus (Taroni, Champod y Margot, 1998). Publicaciones de los últimos quince años ilustran esta tendencia en la interpretación de muchos tipos de prueba forense (por ejemplo marcas de huellas digitales, ADN, reconocimiento de voz o huella de la oreja) (Champod y Meuwly, 2000; Evett, 1998; Champod y Margot, 1995; Meuwly, 2001; Champod y Evett, 2001).

6.3.5 El método de la razón de probabilidad basado en el teorema de Bayes

A. Definición de la hipótesis

La información sobre los antecedentes (I) del caso y la observación preliminar del rastro constituyen la información necesaria para definir el conjunto de todas las fuentes plausibles del rastro, denominado población potencial. La información sobre los antecedentes también determina qué fuente concreta de la población potencial se presenta como objeto de atención preferente y fuente supuesta del rastro.

La hipótesis inculpatoria H_p es aquella según la cual la fuente supuesta es verdaderamente la fuente del rastro. La hipótesis exculpatoria H_d es aquella según la cual la verdadera fuente del rastro es una fuente alternativa plausible. Un requisito lógico exige que ambas hipótesis sean mutuamente excluyentes, pero no necesariamente exhaustivas.

B. comprobación de la hipótesis

El enfoque de la razón de probabilidad demuestra que la razón de probabilidad de las dos hipótesis concurrentes H_p y H_d determinada *a priori* puede evolucionar hasta convertirse en una razón de probabilidad *a posteriori*, habida cuenta de la información sobre los antecedentes y del resultado de la comparación de la fuente supuesta con el rastro, que se denomina prueba (E). La probabilidad de la prueba se evalúa para el caso de que la hipótesis H_p sea cierta por una parte, y para el caso de que la hipótesis H_d sea cierta por otra parte. La razón entre sendos valores de probabilidad, denominada razón de probabilidad, se define como el valor numérico que permite revisar la razón de probabilidad *a priori* (probabilidades o apuestas previas), basada en la nueva información E, para determinar una razón de probabilidad *a posteriori* (probabilidades posteriores) de las dos hipótesis H_p y H_d.

$$\frac{p(H_p|E,I)}{p(H_d|E,I)} = \frac{p(E|H_p,I)}{p(E|H_d,I)} \times \frac{p(H_p,I)}{p(H_d,I)}$$

a posteriori				*a priori*
razón de probabilidad	=	razón de probabilidad	x	razón de probabilidad
probabilidades posteriores				probabilidades previas

■ 6.4 Herramientas de individualización biométrica en la ciencia forense

Este apartado presenta herramientas concretas de individualización forense a partir de datos biométricos basadas en el método hipotético-deductivo. Dichas herramientas, resumidas en el esquema presentado en la Tabla 6-1, incluyen la definición de las hipótesis alternativas, la selección de las fuentes y bases de datos, el análisis y la comparación de las propiedades biométricas, y la interpretación de la prueba utilizando el método de la razón de probabilidad.

6.4.1 Definición de las hipótesis y selección de las fuentes

El rastro (X) considerado para la individualización biométrica forense puede ser una marca de huella dactilar, una fotografía o una grabación en vídeo de una cara o una grabación sonora del habla. El conjunto de todas las fuentes plausibles del rastro se diseña basándose en la información sobre los antecedentes (I) y en la observación preliminar de dicho rastro. La información sobre los antecedentes también determina cuál de las fuentes plausibles puede ser objeto de atención y seleccionarse como fuente supuesta (Y).

La hipótesis inculpatoria es la hipótesis según la cual la fuente supuesta (Y) es la fuente del rastro (X). En aras de la claridad del esquema, el subconjunto de todas las demás fuentes plausibles se considera como una fuente alternativa genérica. La hipótesis exculpatoria H_d es la hipótesis según la cual una fuente alternativa es la fuente del rastro (X). Ahora bien, en la realidad, la información sobre los antecedentes de las demás fuentes plausibles puede variar, en cuyo caso habrá que considerar una hipótesis exculpatoria particular para cada fuente plausible.

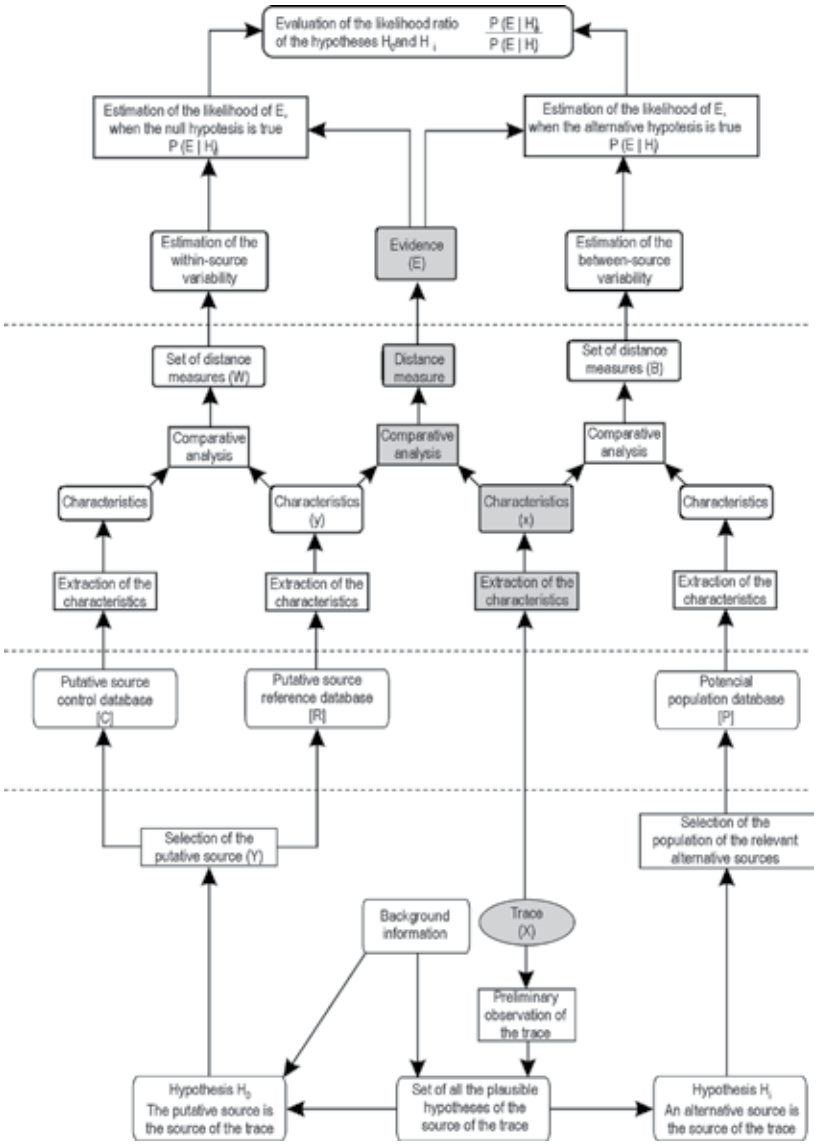


Tabla 6-1: Diagrama del sistema informático propuesto para la individualización biométrica.
(Texto únicamente en inglés)

6.4.2 Selección de las bases de datos

Cuando se aplica a la individualización forense a partir de datos biométricos, el método de la razón de probabilidad requiere datos biométricos para estimar la variabilidad interna de la fuente supuesta y la variabilidad entre fuentes del rastro. Los datos se han estructurado en tres bases de datos: la base de datos de la población potencial (P), la base de datos de referencia de fuentes posibles (R) y la base de datos de control de fuentes posibles (C). A continuación detallamos el contenido y la utilización de cada una de estas bases de datos.

6.4.3 Análisis y comparación

A. Extracción de las características

Nunca se insistirá lo suficiente en la importancia de seleccionar juiciosamente las características. Si las características están mal elegidas, no hay matemáticas en el mundo que puedan salvar un programa de individualización (Bremermann, 1971). Por lo que se refiere a la huella dactilar, la información se conoce y estructura en tres niveles de características: el primer nivel es patrón tipo de la huella dactilar (arco, bucle y anillo de cresta); las minucias o puntos de Galton (terminación de protuberancia, bifurcación e isla) constituyen el segundo nivel; y los poros y bordes de protuberancias constituyen el tercero. Para efectuar el análisis, los sistemas automáticos de identificación de huellas dactilares actuales usan sobre todo la posición y el ángulo de las minucias así como el esqueleto, pero la utilización de otras características, como la probabilidad de configuración de las minucias en la superficie del dedo, contribuiría a desarrollar una evaluación probabilística de las marcas de huellas dactilares basada en la estadística (Champod y Margot, 1995).

En lo tocante a la cara y la voz, el conocimiento de la existencia de características idiosincrásicas tropieza con la dificultad de ofrecer una descripción simbólica de esta información. En esos casos, el proceso de individualización se apoya en el reconocimiento de información que contiene características dependientes de la fuente, pues la información en sí resulta imposible de definir (Thévenaz, 1993).

B. Estimación del valor de la prueba

La prueba es el resultado del análisis comparativo de las características (x) extraídas del rastro X, con las características (y) extraídas de la fuente supuesta Y. En un enfoque informático de la individualización a partir de datos biométricos, el resultado de la comparación entre x e y arroja un valor numérico unidimensional o multidimensional, que estima la "distancia" o el "índice de proximidad" entre ambas; dicha información representa la prueba E.

6.4.4 Interpretación de la prueba mediante la razón de probabilidad

A. Estimación de la variabilidad entre fuentes y cálculo del denominador de la razón de probabilidad (LR)

La base de datos de la población potencial (P) es una base de datos a gran escala utilizada para estimar la variabilidad de las fuentes contenidas en la población potencial. Teóricamente, P está constituido por información que contiene las características de interés exhaustivas de las fuentes alternativas de la población potencial. A efectos de la individualización a partir de datos biométricos, esta base de datos puede consistir en imágenes de impresiones a tinta de huellas dactilares rodadas, fotografías de la cara en dos o tres dimensiones o grabaciones sonoras del habla espontánea de las fuentes alternativas de la población potencial.

Las características correspondientes de las fuentes alternativas pertinentes se extraen y se comparan con las características del rastro. El resultado de este análisis comparativo es un conjunto de medidas de distancia (B) utilizadas para estimar la variabilidad entre fuentes en función del rastro. Esto equivale a calcular la distribución de las medidas de distancia que se pueden obtener al comparar el rastro con las fuentes alternativas de la base de datos de la población potencial. La variabilidad entre fuentes compara la frecuencia relativa de la prueba en la población potencial, dentro del límite de la base de datos P donde se observa, en relación con la población completa. A continuación se utiliza la variabilidad entre fuentes calculada de ese modo para estimar el denominador de la razón de probabilidad $P(E \mid H_d)$.

B. Estimación de la variabilidad interna de la fuente y cálculo del numerador de la razón de probabilidad (LR)

La base de datos de referencia de fuentes supuestas (R) consta de información que teóricamente contiene las características de interés exhaustivas de la fuente supuesta. A efectos de la individualización a partir de datos biométricos, esta base de datos puede consistir en imágenes de impresiones a tinta de huellas dactilares rodadas, fotografías de la cara en dos o tres dimensiones o grabaciones sonoras del habla espontánea. Las características (y) extraídas de la fuente supuesta Y se utilizan para calcular la prueba (E) cuando se comparan con las características del rastro (x).

La base de datos de control de fuentes supuestas (C) consta de información que teóricamente es de la misma calidad que el rastro, pero que tiene su origen en la fuente supuesta. En el caso de la individualización a partir de datos biométricos, se puede tratar de marcas de huellas dactilares de la fuente supuesta, detectadas en la misma superficie que el rastro, de fotos de la cara de la fuente supuesta tomadas en condiciones similares a las del rastro, o de expresiones sonoras del habla de la fuente supuesta grabadas en condiciones similares a las del rastro. Estas pseudo-marcas se utilizan para evaluar la variabilidad interna de la fuente supuesta cuando se procede a comparar las características de las muestras de la base de datos C con las características de la fuente supuesta.

El resultado de este análisis comparativo es un conjunto de medidas de distancia (W) utilizado para estimar la variabilidad interna de la fuente supuesta. Implica el cálculo de la distribución de las medidas de distancia que se puede obtener al comparar la fuente supuesta y un pseudo-rastro del mismo origen. Esta distribución compara la variabilidad interna de la fuente supuesta, dentro del límite de las bases de datos C y R donde se observa, con la variabilidad real de la fuente supuesta. A continuación se utiliza la variabilidad interna de la fuente así calculada para estimar el numerador de la razón de probabilidad $P(E \mid H_p)$.

C. Evaluación de la solidez de la prueba

La evaluación de la razón de probabilidad de las dos hipótesis es el resultado del cálculo de $P(E \mid H_p) / P(E \mid H_d)$. La solidez de la prueba se puede expresar a través de valores numéricos, pero también se puede expresar mediante calificadores lingüísticos, que transmiten la medida en que la prueba E (evidencia) avala la hipótesis H_p frente a la hipótesis H_d, con arreglo a una escala cualitativa de equivalentes verbales correspondientes a valores de razones de probabilidad (Evett, 1998).

■ 6.5 Conclusión

Este Capítulo expone que en la ciencia forense, el concepto de la identidad está relacionado con el concepto de la identidad de la fuente. La determinación de la identidad de la fuente se refiere a un proceso de individualización consistente en determinar si una entidad individual concreta es la fuente de un rastro. Como en la ciencia forense no se puede demostrar la continuidad de la existencia de una fuente y un rastro, la identidad de la fuente es relativa y sólo se puede inferir.

El supuesto de la singularidad, a menudo considerado como un principio fundamental en la ciencia forense, no se verifica en el caso de los rastros, ni en algunas de las fuentes consideradas para la individualización biométrica forense. Aunque esta valoración no significa que las marcas de huellas dactilares, los rastros de caras y los rastros de voces no sean adecuados o utilizables para la individualización biométrica forense, sí que establece claramente su carácter limitado.

La consecuencia lógica es que el proceso de individualización utilizado para la individualización biométrica forense no se puede considerar simplemente como un análisis comparativo de las características de una fuente y de un rastro seguido de una decisión de discriminación o clasificación. En su lugar, el proceso debe organizarse conforme al método hipotético-deductivo, cuyas principales características son la incorporación del conocimiento previo, la exigencia de considerar todas las hipótesis posibles para explicar la fuente de un rastro, y su capacidad de comprobarlas. El esquema propuesto para diseñar un

sistema informático de individualización biométrica forense brinda un posible marco de aplicación del método hipotético-deductivo.

Este Capítulo también hace hincapié en que el uso extensivo de los sistemas automáticos de identificación de huellas dactilares (AFIS) ha demostrado que, hasta ahora, la impresión en tinta de la huella dactilar ha superado la prueba de falsabilidad empírica. En este campo, el principio de la singularidad ha alcanzado un grado de corroboración (verosimilitud) suficiente como para considerar que la impresión en tinta de la huella dactilar constituye una característica biométrica pertinente que puede figurar en los documentos de identidad nuevos.

Referencias

Bolt, R.H., et al.
1970 "*Speaker identification by speech spectrograms: A scientists' view of its reliability for legal purposes*", *Journal of the Acoustical Society of America,* 47(2):597-612.

Boves, L.
1998 "*Commercial applications of speaker verification: overview and critical successfuctors", en RLA2C Workshop: Speaker Recognition and its Commercial and Forensic Applications, Avignon*.

Bremermann, H.J.
1971 "*What Mathematics Can and Cannot Do for Pattern Recognition", en Pattern Recognition in Biological and Technical Systems,* O'Grusser, Ed., Springer-Verlag, Nueva York.

Champod, C. e I. Evett
2001 "*Earmarks as Evidence: A Critical Review*", *Journal of Forensic Science*s, 46(6):1275-1284.

Champod, C. y P.A. Margot
1995 "*Computer Assisted Analysis of Minutiae Occurences on Fingerprints", en International Symposium on Fingerprint Detection and Identification, J. Almog y E. Springer, Editores*, Policía Nacional de Israel, Ne'urim, Israel, 305-318.

Champod, C. y D. Meuwly
2000 "The *inference of identity in forensic speaker recognition"*, *Speech Communicatio*n, 31(2-3):193-203.

Clifford, B.R.
1980 "*Voice identification by human listeners: on earwitness reliability*", *Law and human behaviou*r, 4(4):373 - 394.

Conan Doyle, A.
1953 "*The Sign of Four*", in *The Complete Sherlock Holme*s, *Doubleday & Company*, Nueva York.

Doddington, G.R.
1985 "*Speaker recognition - Identify people by their voices*", Proc. IEEE, 73(11):1651.

Eco, U.
1983 *El nombre de la rosa*. Col. Palabra en el tiempo Nº.. 148, Lumen, 1982.

Evett, I.,
1996 "*Expert Evidence and Forensic Misconceptions of the Nature of Exact Science*", *Science and Justic*e, 36(2):118-122.
1998 "*Toward a uniform framework for reporting opinions in forensic science casework*", *Science & Justic*e, 38(3):198-202.

Grieve, D.,
2000 "*Built By Many Hands*", *Fingerprint Worl*d, 26(100):51-60.

Grieve, M.C. y J. Dunlop
1992 "*A Practical aspect of the Bayesian Interpretation of Fibre Evidence*", *Journal of Forensic Sciences,* 32:169-175.

Kirk, P.L.
1963 "*The Ontogeny of Criminalistics*", *The Journal of Criminal La*w, *Criminology and Police Scienc*e, 54:235-238.

Kwan, Q.Y.
1977 *Inference of Identity of Source, in Department of Forensic Science*, Universidad de California, Berkeley.

Locard, E.
1909 *L'identification des récidivist*es, A. Maloine, París.
1924 *Policiers de roman et policiers de laboratoir*e, Payot, París.

Marquis, P.
1999 "*Sur les Preuves non Déductives en Intelligence Artificielle*", en :(Ed.), en *Le Concept de Preuve à la Lumière de l'Intelligence Artificiell*e, S. J y J. Szczeciniarz, Eds., Presses Universitaires de France, París.

Meuwly, D.
2001 "*Reconnaissance de Locuteurs en Sciences Forensiques: l'Apport d'une Approche Automatique", in Institut de Police Scientifique et Criminologie*, Universidad de Lausana, Lausana.

Nolan, F.
1991 "*Forensic Phonetics*", *Journal of Linguistic*s, 27: 483-493.
Stacey, R.
2004 "A *report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case*," *Journal of Forensic Identificatio*n, 54(6):706–718.

Stacey, R.
2004 "*A report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case*," *Journal of Forensic Identification*, 54(6):706–718.

Stoney, D.A.
1991 "*What Made Us ever Think We Could Individualize Using Statistics*", *Journal of The Forensic Science Societ*y, 31(2):197-199.

Taroni, F.,
1997 "*La recherche et la gestion des liens dans l'investigation criminelle: une étape vers l'exploitation systématique des données de police", in Institut de Police Scientifique et de Criminologie,* Universidad de Lausana, Lausana.

Taroni, F., C. Champod, y P. Margot
1998 "*Forerunners of Bayesianism in early forensic science*", *Jurimetrics Journa*l, 38:183-200.

Thévenaz, P.
1993 "*Résidu de prédiction linéaire et reconnaissance de locuteurs indépendante du texte*", Universidad de Neuchâtel, Suiza.

Thornton, J.I.
1997 "*The DNA Statistical Paradigm vs. Everything Else*", *Journal of Forensic Science*s, 42(4): 758-759.

Truzzi, M.,
1983 "*Sherlock Holmes*", in *The sign of thre*e, *U. Eco and T.A. Sebeok, Eds., Indiana University Press, Bloomington*.

Tuthill, H.,
1994 *Individualization: Principles and Procedures in Criminalistic*s*, Lightning Powder Co, Salem*.

CAPÍTULO 7

EL USO DE LA BIOMETRÍA EN LOS DOCUMENTOS DE VIAJE

7.1 Introducción

El término "biometría" se refiere a la identificación o comprobación de la identidad de individuos vivos de forma automática, utilizando sus características fisiológicas y conductuales (Wayman, 2001; Miller, 1995). La autenticación biométrica es la parte "automática", "en tiempo real", "no forense" del campo más amplio de la identificación humana. Entre los ejemplos de tecnología figuran el reconocimiento por el iris, la cara, la huella dactilar, el reconocimiento de la voz y la geometría de la mano. En la Figura 7-1 se presentan las imágenes de la huella dactilar, la cara, la mano y el iris obtenidas mediante sensores.

Figura 7-1: Imágenes de la huella dactilar, la cara, la mano y el iris obtenidas mediante sensores (Cortesía de Jim Wayman, San José, Estados Unidos de América)

Aunque las fotografías del rostro y las huellas dactilares se utilizan en los documentos de viaje desde hace ya casi un siglo, su intención primordial ha sido la de permitir el reconocimiento del viajero mediante la inspección humana. El concepto de utilización de la biometría en aplicaciones de "punto de servicio" para la comprobación de los datos de identidad se remonta principios de la década de 1960 (Trauring, 1961). Durante la última década, los profesionales de los documentos oficiales han empezado a aplicar este concepto al reconocimiento automático, mecanizado, de los viajeros. Desde los atentados terroristas perpetrados

el 11 de septiembre de 2001 en los Estados Unidos, la atención legislativa y mediática se ha concentrado en mayor medida en las posibilidades de aplicación de la biometría en servicios de inmigración y aeroportuarios (Ley pública de los Estados Unidos, 2002).

Encontramos una de las primeras aplicaciones de la biometría a los documentos de inmigración en la experimentación del sistema basado en la huella dactilar llamado "*Schiphol Travel Pass*" realizada en 1992 en el aeropuerto de Ámsterdam. Aunque el sistema Schiphol original ya no se utiliza, éste sirvió de modelo para el Sistema de servicio acelerado para pasajeros del Servicio de Inmigración y Naturalización de los Estados Unidos (INSPASS, por sus siglas en inglés), que se ha utilizado entre 1993 y 2002. Este sistema también sirvió de modelo a su vez, concretamente, para el proyecto israelí "*Ben Gurion Express Entry*" (Troy, 2001). La tecnología de geometría de la mano utilizada en el INSPASS ha demostrado ser sumamente efectiva desde el punto de vista técnico (Wayman, 2000) a la hora de facilitar los procedimientos de inmigración en los aeropuertos estadounidenses, pero los informes administrativos sobre la eficacia del sistema en su conjunto han sido desiguales, y la financiación del sistema por parte del gobierno no ha sido fiable. La Figura 7-2 muestra el anverso y el reverso de una tarjeta INSPASS.

Figura 7-2: Tarjeta INSPASS
(Cortesía de Jim Wayman, San José, Estados Unidos de América)

El rendimiento de todas las tecnologías biométricas, medido en función de las tasas de procesamiento y precisión, depende en buena medida de las interacciones humanas con los dispositivos. Pese a que muchas veces esas tecnologías han tenido un rendimiento excelente en

laboratorio, su resultado práctico resulta mucho menos predecible y más complicado en entornos concurridos y difíciles de controlar, como son los aeropuertos y los pasos fronterizos. Además de los proyectos de Schiphol e INSPASS, también se han realizado pruebas piloto y pruebas experimentales de sistemas biométricos en aplicaciones de inmigración en el Reino Unido, el Canadá, Hong Kong y Malasia, aunque nunca se ha llegado a publicar en la literatura biométrica los datos sobre el rendimiento de dichos sistemas. Por consiguiente, todavía no se dispone de una visión suficientemente clara del uso de la biometría para el procesamiento automático de pasajeros.

Este Capítulo pretende examinar las propiedades generales de los sistemas biométricos cuando se aplican a los documentos de viaje, explicar cómo funcionan y se ponen a prueba los sistemas biométricos generales, presentar los resultados de pruebas recientes, y exponer algunos detalles sobre el funcionamiento del sistema INSPASS.

■ 7.2 Funciones de los dispositivos de identificación biométrica

Los dispositivos biométricos desempeñan dos funciones distintas:

1. demostrar que eres quien dices ser; y
2. demostrar que no eres quien dices no ser.

En el contexto de los documentos de viaje, la primera función, denominada "identificación positiva", comprueba si el portador es efectivamente el titular correcto del documento, y pretende evitar que un mismo documento tenga varios usuarios. La segunda función o "identificación negativa" comprueba que un solicitante no sea ya titular de un documento, e impide la expedición de varios documentos para el mismo individuo. Dependiendo de su diseño, los sistemas biométricos pueden desempeñar una de estas dos funciones o ambas.

7.2.1 Identificación positiva

En la primera función, utilizamos una "muestra" biométrica (por ejemplo, una huella dactilar) para relacionar al sujeto con un "patrón" almacenado (o "registrado") previamente en el sistema. El usuario del

sistema biométrico realiza una declaración "positiva" de la identidad, a saber, "Soy Fulano, tal como estoy registrado en el sistema", que se comprueba mediante la comparación automática de la muestra presentada con el patrón de "Fulano" que figura previamente en el sistema. A continuación, se puede almacenar el patrón en el documento de identidad, o en una ubicación centralizada a la que se puede acceder electrónicamente desde el punto de utilización del documento. Si los patrones biométricos de la muestra y el modelo se parecen "suficientemente" entre sí, podemos suponer que el portador es la misma persona que la que creó el patrón de registro.

El objeto de un sistema de identificación positiva consiste en evitar la utilización de una misma identidad por varias personas. Si un sistema de identificación positiva no consigue encontrar una coincidencia entre un patrón registrado y una muestra presentada, el resultado será el "rechazo". El resultado también será de rechazo si el sistema biométrico no logra conseguir una muestra – una situación denominada "adquisición fallida". La coincidencia entre la muestra y el patrón dará lugar a la "aceptación". Un impostor que pretendiese engañar al sistema induciendo una "aceptación indebida" tendría que duplicar la muestra biométrica de un usuario registrado.

Para la identificación positiva existen múltiples alternativas a la biometría. A lo largo de la historia, los inspectores humanos han conseguido comprobar las identidades cotejándolas con documentos de identificación.

7.2.2 Identificación negativa

La segunda función posible de un sistema biométrico, denominada "identificación negativa", determina que una persona no es alguien o no está incluida en un grupo de personas que el sistema ya conoce. En ese caso, el usuario realiza la declaración (tal vez de forma implícita) de que no se ha registrado previamente en el sistema. La muestra biométrica que presenta se compara con todas las muestras registradas, que por consiguiente deben estar almacenadas en una base de datos centralizada. Normalmente, el propósito de un sistema de identificación

negativa consiste en impedir la expedición de varios documentos de identidad a una misma persona. La propuesta de utilización de sistemas biométricos para identificar a personas incluidas en "listas de alerta" también constituye una aplicación de la "identificación negativa", donde todos los "usuarios" realizan una declaración implícita (y quizás sin saberlo siquiera) de que no están registrados en la "lista de alerta".

La identificación negativa dirigida a evitar varias inscripciones de un mismo usuario constituye el mayor uso actual de la biometría, y se emplea en los sistemas de expedición de permisos de conducir, prestaciones sociales y seguridad social (en especial en los Estados Unidos). Si un sistema de identificación negativa no consigue encontrar una coincidencia entre la muestra presentada y todos los patrones registrados, el resultado será la "aceptación". Por lo general, también se producirá una aceptación si el sistema no ha conseguido capturar una medida legible. Un sujeto que desee engañar al sistema produciendo una "aceptación indebida" tendrá que hacer que el sistema no consiga encontrar una coincidencia con un patrón registrado previamente, o bien que el sistema fracase en la adquisición de una medición legible. Por consiguiente, la coincidencia entre la muestra y uno de lo patrones da lugar al "rechazo".

En la práctica, una declaración negativa de la identidad sólo puede ser comprobada a través de la biometría. En un sistema con algunos cientos de personas registradas, los inspectores humanos no serían capaces de detectar múltiples registros del mismo individuo, ni de determinar si un individuo figura en una "lista de alerta". Por consiguiente, no existen alternativas, y la participación en el sistema biométrico no puede tener un carácter voluntario.

Los sistemas de identificación positiva exigen la comparación de las muestras presentadas sólo con los modelos almacenados de la persona que declara su identidad. Los sistemas de identificación negativa requieren algún nivel de comparación de la muestra presentada con los modelos almacenados de cada persona inscrita, para demostrar la no inclusión en la base de datos. Como la probabilidad de falsa coincidencia aumenta con el número de comparaciones que haya que llevar a cabo, a efectos

de identificación negativa sólo se pueden utilizar patrones biométricos altamente característicos. Los rasgos de las huellas dactilares y del ojo (iris y retina) son los únicos patrones biométricos que han demostrado su capacidad de identificación negativa con respecto a grandes bases de datos.

7.2.3 Sistemas de doble uso

El INSPASS es un sistema que sólo utiliza la identificación positiva. No cuenta con ninguna medida destinada a impedir la expedición de varios documentos a un mismo viajero. Por otro lado, el sistema de permisos de conducir de California está diseñado para utilizar la impresión de huellas dactilares a efectos de identificación negativa solamente. El patrón de la huella dactilar no está en el documento, no puede accederse fácilmente a éste desde la base de datos, y no se puede utilizar para comprobar la autenticidad del titular del permiso. En cambio, la tarjeta de identificación de los servicios sociales del Estado de Connecticut (Estados Unidos) contiene componentes biométricos tanto "positivos" como "negativos" — identificación negativa realizada en el momento del registro para impedir la emisión de varias identidades a una misma persona, e identificación positiva en las aplicaciones de "punto de servicio" para relacionar al portador con el documento.

La aplicación de la biometría a los documentos de viaje puede englobar tanto la identificación negativa como positiva, dependiendo de los objetivos del sistema. En la Tabla 1 se resumen y comparan las características de los sistemas de identificación positiva y negativa.

POSITIVA	NEGATIVA
Demostrar que soy alguien conocido por el sistema.	Demostrar que no soy alguien conocido por el sistema.
Impedir que haya varios usuarios de un mismo documento de identidad.	Impedir la expedición de varios documentos de identidad a un mismo usuario.
Comparar la muestra presentada con un solo patrón registrado.	Comparar la muestra presentada con todos los patrones registrados.
Una falsa coincidencia da lugar a una "aceptación indebida"	Una "falsa coincidencia" o una "adquisición fallida" da lugar a un "rechazo indebido".
Una "falsa no coincidencia" o una "adquisición fallida" da lugar a un "rechazo indebido".	Una "falsa no coincidencia" o una "adquisición fallida" da lugar a una "aceptación indebida".
Existen métodos de identificación alternativos.	No existen métodos de identificación alternativos.
Puede ser voluntario.	Tiene que ser obligatorio para todos.
Se le puede engañar presentando las medidas biométricas de otra persona.	Se le puede engañar no presentando medidas o presentando medidas alteradas.

Tabla 7-1: Identificación "positiva" y "negativa"

■ 7.3 Limitaciones de la biometría

Sin embargo, aquí conviene ser cauteloso para comprender las limitaciones de lo que se acaba de exponer:

1. La "verdadera" identidad no se pone de manifiesto con ninguna medida biométrica, sino que se debe determinar con la ayuda de documentación externa, que puede ser fiable o no.
2. No todo el mundo puede presentar un patrón biométrico adecuado para el registro.
3. Algunos entornos (y personas) no permiten obtener medidas biométricas repetibles.
4. Como sólo se pueden reconocer las medidas estables, los niños y los jóvenes (quienes siguen en crecimiento) no son buenos candidatos para una identificación biométrica fiable mediante la mayor parte de las tecnologías.
5. Se producen errores de coincidencia, cuya consecuencia es el rechazo de individuos válidos o la aceptación de impostores.

6. Los patrones biométricos no son secretos, sino públicamente observables.
7. El resultado positivo de la comparación positiva entre una medida biométrica y un patrón contenido en un documento no certifica la autenticidad del documento.
8. Los sistemas biométricos, como todas las tecnologías de computación, exigen una inversión considerable en planificación, instalación, mantenimiento y explotación, pero tienen un corto ciclo de vida de asistencia técnica del proveedor.

Ninguna medida biométrica encierra en sí la identidad jurídica del portador. La determinación de dicha identidad en el momento de proceder al registro se debe llevar a cabo con la ayuda de documentación ajena a cualquier sistema biométrico. Dicha documentación puede incluir certificados de nacimiento o de bautismo, documentos oficiales de identificación, cartas de presentación, tarjetas de identificación de empleados, tarjetas de seguro médico y permisos de conducir. En los países que no disponen de un registro civil u otro sistema de inscripción de nacimientos y fallecimientos (como ocurre en los Estados Unidos), esos documentos pueden no ser fiables. De ello se desprende que ninguna medida biométrica permite determinar la nacionalidad, la edad o la situación de inmigración de un usuario. En el momento del registro, la administración del sistema sólo puede confiar en la verdadera identidad, edad, nacionalidad y situación de inmigración del portador en la misma medida en que confía en la documentación externa. Los sistemas biométricos no pueden determinar la validez de la documentación externa. Esa labor incumbe al personal de registro, que tiene que haber recibido una formación especial para la detección de documentos fraudulentos.

No todo el mundo puede presentar medidas biométricas de buena calidad. Cada tecnología tiene una tasa de "registros fallidos" que depende de la población usuaria y del entorno físico donde se realice el registro. En la Figura 7-3 (izquierda), que presenta una huella dactilar de una persona de unos 70 años de edad, se aprecia una falta de contraste en la imagen, habitual en este colectivo de usuarios. A la derecha aparece la huella dactilar de un niño, que no sólo es pequeña, sino además excesivamente húmeda en algunos sitios. Compárense esas imágenes

con la huella dactilar de un estudiante universitario que aparece en la Figura 7-1. Debido a la variabilidad de los individuos, todos los sistemas biométricos deben disponer de procedimientos alternativos que les permitan dar cabida a quienes no se pueden registrar.

Huella dactilar de una persona mayor y huella dactilar de un niño.
(Cortesía de Jim Wayman, San José, Estados Unidos de América)

Pero incluso si una persona muestra una biometría perfectamente clara, un entorno de captura de la imagen adverso puede impedir la captura repetible. Por ejemplo, la captación de señales vocales en entornos ruidosos, o la captura de imágenes de rostros sobre fondos abigarrados, son tareas difíciles. Cada tecnología tiene una tasa de "adquisiciones fallidas" que varía en función de la población y del entorno de aplicación. La Figura 7-4 presenta una imagen facial adquirida sobre un fondo sobrecargado, aunque en las condiciones generales no se garantiza ese resultado. Por consiguiente, todos los sistemas biométricos requieren un "tratamiento de las excepciones" que permita la utilización de medios alternativos de comprobación de la identidad en caso de que no se pueda tomar una medida fiable. Ahora bien, el mecanismo no biométrico de "tratamiento de las excepciones" se puede convertir en un blanco para las violaciones de la seguridad.

Con estos sistemas se producen errores de coincidencia. La coincidencia de las muestras con los patrones sólo determina que los patrones son "suficientemente parecidos" como para suponer que proceden de la misma persona. Se producen errores cuando la imagen biométrica del verdadero titular de un documento ha cambiado significativamente desde el momento del registro, o si un impostor tiene una biometría aproximadamente similar al patrón registrado. Por consiguiente, las "falsas coincidencias" y "falsas disconformidades" son tasas de error antagónicas que se controlan mediante un umbral establecido

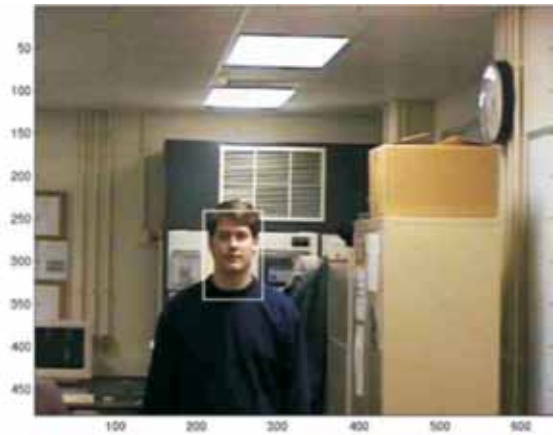


Figura 7-4: Rostro capturado en un fondo abigarrado.
(Cortesía de Jim Wayman, San José, Estados Unidos de América)

por la administración del sistema con el fin de determinar "qué es suficientemente parecido". Cuando esas tasas de error se combinan con la tasa de registros fallidos y de adquisiciones fallidas en el marco de la política del sistema, tal vez permitiendo realizar varios intentos en el momento de la adquisición y la comparación, se pueden estimar las tasas de "aceptación indebida" y de "rechazo indebido". Estas tasas dependen en última instancia de la política de decisión del sistema, así como de la solidez de la tecnología del entorno de aplicación elegido con el colectivo de usuarios específico.

Aunque los patrones biométricos pueden ser públicamente observables, su usurpación requiere normalmente más esfuerzo que la mera observación. Existen métodos bien conocidos de creación de huellas dactilares o de imágenes faciales sucedáneas (van der Putte, 2000; Blackburn et al., 2000; Matsumoto et al., 2002). Ahora bien, las técnicas de introducción de un patrón biométrico usurpado en un sistema de huellas dactilares físicamente seguro requieren algún tipo de prótesis o de modelo físico, y por lo general no están al alcance del viajero con un nivel de habilidad corriente. Se puede evitar la utilización de características biométricas usurpadas mediante una adecuada supervisión del sensor biométrico (tanto en el momento del registro como en el de la comprobación).

Ni siquiera la coincidencia correcta de una muestra biométrica con un patrón registrado incorporado en un documento confirma la validez del documento. El documento puede ser falso en sí, y aún así contener la medida biométrica auténtica del portador. Existen al menos dos maneras de superar este problema para comprobar la autenticidad de la información contenida en el documento: el cifrado y/o el almacenamiento centralizado.

Mediante la aplicación de una "criptografía de clave pública", se puede cifrar el patrón incorporado en el documento utilizando la "clave privada" del organismo expedidor. De momento, la única manera de descifrar el patrón es mediante la "clave pública" asignada a dicho organismo. Si la muestra biométrica del portador coincide con el patrón descifrado mediante la clave pública del organismo expedidor, se puede comprobar la autenticidad de la información. Por consiguiente, el documento se puede vincular convincentemente tanto con el portador como con el expedidor (para mayores detalles sobre la infraestructura de clave pública, ICP, véase el Capítulo 8).

Un segundo planteamiento, que ya se utiliza en el sistema INSPASS, consiste en centralizar el almacenamiento de patrones. El número de pasaporte, tal como se lee en el documento, se transmite al punto de almacenamiento central junto con la muestra recogida. La muestra se compara con el patrón identificado mediante el número de pasaporte. Como la base de datos central es segura, sólo se pueden introducir patrones mediante un proceso de confianza. Por consiguiente, la coincidencia entre la muestra y el patrón permite verificar tanto la identidad del portador como la validez de la información que aparece en el documento (en este caso, el número de documento).

La especificación, compra e instalación de los sistemas biométricos exigen un gran cuidado. Es necesario asegurar una buena capacitación de los operadores y un buen mantenimiento del equipo de computación y de los programas durante toda la vida útil del sistema. Si se estima que el usuario tendrá que hacer frente a tasas de procesamiento importantes, puede resultar necesaria la formación de los usuarios y la personalización de los interfaces de usuario. Si el sistema está conectado a una base de datos centralizada (como deben estarlo

todos los sistemas de identificación negativa), habrá que establecer y mantener la conectividad de la red. Estos requisitos son caros y llevan mucho tiempo. Los sistemas biométricos no son tecnologías de las que uno se pueda olvidar una vez instalados, y es posible que al cabo de tan sólo unos pocos años ya no se disponga de la asistencia del proveedor para los productos instalados. Por ello, la incapacidad de valorar adecuadamente las dificultades inherentes a estos sistemas ha provocado el abandono de muchos proyectos piloto.

■ 7.4 Las tecnologías

Prácticamente parece no existir límite a las partes del cuerpo, características personales y métodos de captación de imágenes sugeridos o utilizados para la identificación biométrica: dedos, manos, pies, caras, ojos, orejas, dientes, venas, voces, firmas, letra, modo de andar y olores. ¿Qué característica es la mejor? Eso depende de una serie de aspectos básicos, que han de ser por lo menos cinco: solidez, carácter distintivo, accesibilidad, aceptabilidad y disponibilidad del patrón biométrico. Solidez significa que la característica es repetible y no está expuesta a grandes cambios. Carácter distintivo supone la existencia de grandes diferencias en el patrón entre la población. Accesibilidad significa que se puede presentar fácilmente a un sensor de captación de imágenes. Aceptabilidad significa que el usuario no percibe que su adquisición resulte invasiva. Disponibilidad significa que cada usuario puede presentar cierto número de medidas independientes.

La Tabla 7-2 presenta las tecnologías probadas en sistemas de identificación positiva y/o negativa públicamente accesibles.

IDENTIFICACIÓN POSITIVA	IDENTIFICACIÓN NEGATIVA
Geometría de la mano	Impresión de huellas digitales
Geometría del dedo	Barrido de la retina
Reconocimiento de la voz	Reconocimiento del iris
Barrido de la retina	
Captación de imagen de la cara	
Impresión de huellas digitales	
Venas de la mano	
Patrones de firma dinámica	
Uso del teclado de la computadora	

Tabla 7-2: Tecnologías que han probado su éxito para la aplicación pretendida

■ 7.5 Cómo funciona el sistema biométrico general

Aunque estos dispositivos se basan en tecnologías muy diversas, hay mucho que decir sobre ellas en general. La Figura 7-5 presenta un sistema genérico de autenticación biométrica, dividido en cinco subsistemas: adquisición de datos, transmisión, procesamiento de la señal, decisión y almacenamiento de los datos. Vamos a examinar uno por uno estos subsistemas.

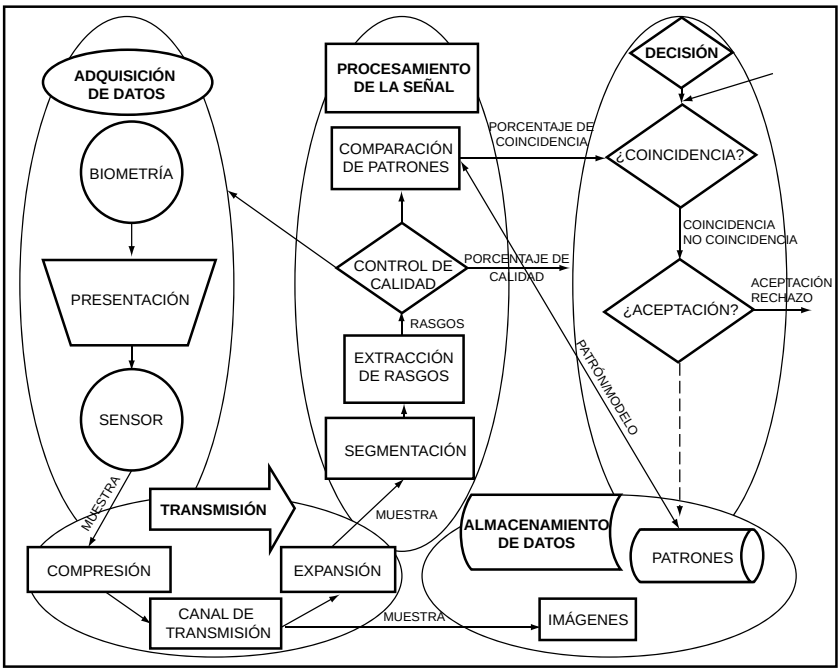


Figura 7-5: Diagrama del sistema biométrico genérico

7.5.1 Adquisición de datos

Los sistemas biométricos comienzan por la medición de una característica conductual o fisiológica. La clave de todos los sistemas es el supuesto subyacente de que la característica biométrica medida es tanto distintiva entre individuos, como repetible en el mismo individuo a lo largo del tiempo. Los problemas de medición y control de estas variables comienzan en el subsistema de adquisición de datos.

Hay que presentar la característica del usuario a un sensor. La presentación de la característica al sensor introduce un componente conductual en cada método biométrico. El resultado producido por el sensor, que es el dato en cuya introducción se basa el sistema, es la confluencia de: 1) la medida biométrica; 2) la forma de presentar la medida; y 3) las características técnicas del sensor. Los cambios sufridos por cualquiera de estos factores inciden negativamente tanto en la repetibilidad como en el carácter distintivo de la medida. Para que los datos biométricos puedan ser compartidos entre distintos sistemas (incluidos los sistemas futuros para la misma aplicación), es necesario normalizar la presentación y las características del sensor para garantizar que los patrones biométricos adquiridos mediante un sistema coincidan con los tomados del mismo individuo por otro sistema. Existen normas internacionales "de facto" para la adquisición de datos del habla, las huellas dactilares y la imagen facial (UIT, 1996; CJIS, 2006; NIST, 2006, y normas ISO). Los sistemas de identificación negativa deben impedir que un usuario fraudulento cambie deliberadamente la biometría o su presentación lo suficiente como para evitar que coincida con registros anteriores.

7.5.2 Transmisión

Algunos sistemas biométricos, aunque no todos, adquieren datos en un punto pero los almacenan y/o procesan en otro. Esos sistemas requieren la transmisión de los datos. Si se transmiten grandes cantidades de datos, puede resultar necesario comprimirlos antes de proceder a su transmisión o almacenamiento con objeto de conservar ancho de banda y espacio de almacenamiento. Dependiendo de la arquitectura del sistema, el subsistema de transmisión se puede situar entre el almacenamiento de datos y el procesamiento de la señal. En esos casos, es necesario expandir los datos comprimidos transmitidos o almacenados para que puedan ser utilizados nuevamente. Por lo general, el proceso de compresión y expansión provoca una pérdida de calidad de la señal restaurada, pérdida que aumenta proporcionalmente a la tasa de compresión. La técnica de compresión utilizada dependerá de la señal biométrica de que se trate. Existen normas de compresión internacionales "*de facto*" para los datos de voz, las huellas dactilares y las imágenes faciales (Cox, 1997; CJIS, 1993; CCITT, 1993). Los

formatos de datos normalizados para la información sobre huellas dactilares e imágenes faciales, así como las especificaciones de formato de datos para los datos biométricos generales se especifican en el sitio Web del NIST (Instituto Nacional de Normas y Tecnologías de los Estados Unidos) y se estipulan asimismo en las normas ISO citadas más arriba.

7.5.3 Procesamiento de la señal

Una vez adquirida y, si fuese necesario, transmitida una característica biométrica, tenemos que prepararla para compararla con otras medidas similares. El papel del subsistema de procesamiento de la señal se puede dividir en tres tareas: extracción de rasgos, control de calidad, y comparación de patrones.

La extracción de rasgos es fascinante. En primer lugar, hay que encontrar el patrón biométrico en la señal más amplia. Por ejemplo, en el reconocimiento del iris, hay que perfilar y extraer la región del iris de la imagen del ojo completo obtenida por el sensor. A continuación, hay que extraer del patrón aquellas características que son diferenciadoras y repetibles, y descartar las que no lo son o son superfluas. Por otra parte, en un sistema de reconocimiento del locutor independiente del texto, por ejemplo, se pueden buscar rasgos, como las relaciones de frecuencia entre vocales, que dependen solamente del hablante y no de la palabra pronunciada. Y además conviene centrarse en los rasgos que no cambian aunque el hablante esté resfriado o no esté hablando directamente al micrófono. Las distintas maneras de abordar estos problemas difíciles pero apasionantes son siempre objeto de protección por patente.

Por lo general, la extracción de rasgos es una forma de compresión irreversible, lo cual significa que no se puede reconstruir la imagen biométrica original a partir de los rasgos extraídos. En algunos sistemas, la transmisión se lleva a cabo después de la extracción de rasgos, con objeto de reducir las necesidades de ancho de banda.

Tras la extracción de rasgos, o quizá incluso antes o durante la misma, se comprobará si la señal recibida desde el subsistema de adquisición

de datos es de buena calidad. Si los rasgos "no tienen sentido" o son insuficientes en cualquier sentido, cabe concluir rápidamente que la señal recibida era defectuosa y se puede solicitar una nueva muestra al subsistema de adquisición de datos mientras el usuario se encuentra todavía ante el sensor.

La incorporación de este proceso de "control de calidad" ha mejorado considerablemente el resultado de los sistemas biométricos durante estos últimos años. Por otro lado, algunas personas parecen no poder presentar nunca una señal aceptable al sistema. Si el módulo de control de calidad no permite invalidar una decisión negativa, el resultado será un error de "registro fallido". Aumentar el nivel de calidad exigido para el registro, incrementando con ello la tasa de "registros fallidos", puede constituir una estrategia efectiva para impedir el registro de usuarios con medidas biométricas deficientes. La supresión de esos usuarios puede reducir la tasa de errores operativos.

Esta "muestra" del rasgo, cuyo tamaño ya se ha reducido mucho con respecto a la señal original, se transmite al proceso de comparación de patrones para su comparación con uno o varios patrones identificados y almacenados previamente. El propósito del proceso de comparación de patrones consiste en cotejar la muestra de rasgo presentada con un modelo almacenado, y enviar al subsistema de decisión una medida cuantitativa de la comparación.

Por simplificar, daremos por supuesto que los patrones estrechamente coincidentes guardarán poca "distancia" entre sí. Las distancias rara vez o nunca serán iguales a cero, pues incluso entre la muestra y el patrón procedentes de una misma persona existirá siempre alguna diferencia biométrica, de presentación o relacionada con el sensor o la transmisión.

7.5.4 Decisión

El subsistema de decisión aplica la política del sistema ordenando la búsqueda en la base de datos, determina las "coincidencias" o "disconformidades" basándose en las medidas de distancia recibidas del comparador de patrones, y al final del proceso toma una decisión de "aceptación" o "rechazo" basándose en la política del sistema. Esa

política puede consistir en declarar la coincidencia para cualquier distancia inferior al umbral establecido, y en "aceptar" a un usuario a partir de esa única coincidencia. También puede consistir en declarar una coincidencia para cualquier distancia inferior a un umbral dependiente del usuario, variable en el tiempo, o vinculado a ciertas condiciones ambientales, y exigir la coincidencia de múltiples medidas para tomar una decisión de "aceptación". Podría permitir a todos los usuarios realizar tres intentos para presentar una medida de distancia baja y ser "aceptados" como coincidentes con el patrón propuesto. En ausencia de un patrón propuesto, la política del sistema también puede consistir en ordenar que se busque en la totalidad o sólo en parte de la base de datos y responder con una única coincidencia o con varios "candidatos" a la coincidencia.

Es la dirección quien elige la política de decisión aplicada, que es específica para cada caso en función de los requisitos operativos y de seguridad del sistema. Por lo general, la ventaja de una reducción en el número de falsas disconformidades puede quedar anulada por el incremento en el número de falsas coincidencias, mientras que la reducción de la tasa de rechazos indebidos se puede compensar con el incremento de la tasa de aceptaciones indebidas. La política óptima del sistema a este respecto dependerá de las características estadísticas de las distancias de comparación procedentes del comparador de patrones, así como de las penalizaciones relativas derivadas de las aceptaciones indebidas y de los rechazos indebidos en el sistema[1].

7.5.5 Almacenamiento

El subsistema que queda por considerar es el de almacenamiento. Se pueden utilizar una o varias formas de almacenamiento, dependiendo del sistema biométrico. Los modelos de rasgos patentados por el proveedor[2] se almacenan en una base de datos con objeto de que el

[1] Además, para configurar los umbrales óptimos, se requiere una estimación *a priori* (mejor candidato basado en la experiencia) de la probabilidad de que un usuario sea un impostor. Por consiguiente, el umbral óptimo siempre se fija parcialmente de manera subjetiva.

[2] Debido al requisito de la interoperabilidad de los sistemas de huellas dactilares en los "puntos de servicio" para llevar a cabo la verificación del titular de una tarjeta, la American Association of Motor Vehicle Administrators ha creado una norma de extracción de las minucias de la huella dactilar, AAMVA DL/ID2000, Nota C, disponible en Internet en www.aamva.org/Documents/stdAAMVADLID-Standrd000630.pdf.

comparador de patrones los pueda cotejar con las muestras de rasgos que van llegando. Para los sistemas de identificación positiva, que sólo exigen la comparación de la muestra presentada con los patrones del supuesto sujeto, la base de datos puede estar distribuida en función de los soportes llevados por cada usuario registrado (véanse en el Capítulo 5, sección 5.4.3 más detalles sobre los medios de almacenamiento). La Tabla 7-3 resume los tamaños típicos de los patrones. Dependiendo de la política del sistema, puede que no sea necesaria la existencia de una base de datos central, aunque en ese tipo de aplicación también se puede utilizar una base de datos, centralizada para detectar tarjetas falsificadas o para volver a expedir tarjetas perdidas sin necesidad de adquirir de nuevo el patrón biométrico.

Huella dactilar	200 – 1000 bytes
Geometría de la mano	9 bytes
Geometría del dedo	14 bytes
Cara	100 – 3.500 bytes
Voz	6.000 bytes
Iris	500 bytes

Tabla 7-3: Tamaños típicos de los modelos

Los sistemas de identificación negativa requieren una base de datos centralizada para realizar búsquedas exhaustivas. Dado que el número de patrones registrados en un sistema de identificación puede llegar a ser muy elevado, las necesidades de velocidad del sistema imponen dividir la base de datos en subconjuntos o particiones de menor tamaño, de tal modo que cualquier muestra de rasgos sólo se tenga que comparar con los patrones almacenados en la partición correspondiente. Esta estrategia permite incrementar la velocidad del sistema y reducir el número de falsas coincidencias, si bien a expensas del incremento en la tasa de falsas disconformidades debidas a los errores de partición. Esto significa que las tasas de error del sistema no se mantienen constantes a medida que aumenta el tamaño de la base de datos, y que los sistemas de identificación no crecen de forma lineal. Por ello, las estrategias de partición de las bases de datos suponen una decisión política compleja. Wayman ha propuesto métodos de estimación de las tasas de error para los sistemas de identificación negativa a gran escala (1999).

A veces es necesario que los seres humanos examinen las imágenes biométricas en bruto de los usuarios del sistema, como puede ocurrir, por ejemplo, en aplicaciones forenses o en el arbitraje de falsas coincidencias. Además, si hay que introducir cambios en el sistema o cambiar de proveedor, puede ser necesario volver a extraer los patrones específicos del proveedor a partir de las imágenes en bruto. Como las imágenes biométricas no se pueden reconstruir a partir de los modelos almacenados, algunos sistemas realizan un almacenamiento centralizado de los datos brutos sin procesar, aunque posiblemente en formato comprimido.

■ 7.6 Pruebas y resultados de las pruebas

Las pruebas biométricas financiadas públicamente tienen al menos dos décadas de historia tras de sí. En este plazo de tiempo, se han seguido muchos planteamientos distintos y contradictorios respecto de las pruebas. En un intento por establecer un enfoque "nominal" el grupo de trabajo de biometría del Reino Unido ha elaborado unas prácticas óptimas para someter a prueba los dispositivos biométricos e informar de los resultados (*UK Biometric Working Group*, 2006). Ésta es la norma internacional *de facto*.

El documento de "prácticas óptimas" reconoce tres tipos de prueba: tecnológica, hipotética y operativa (Philips, et al., 2000). La prueba tecnológica se centra en la capacidad del subsistema de procesamiento de la señal de localizar, extraer y comparar imágenes biométricas utilizando una base de datos recopilada previamente. Aunque la prueba tecnológica puede indicar los tiempos de procesamiento del programa computadorizado, no permite medir la tasa de procesamiento de seres humanos por el sistema y, dependiendo del diseño concreto de la prueba en cuestión, es posible que no permita estimar las tasas de registro o adquisición fallidos.

La prueba hipotética adopta una perspectiva más amplia respecto del sistema biométrico, dado que utiliza a seres humanos en un entorno de prueba especialmente creado para imitar la aplicación deseada. Las pruebas hipotéticas permiten medir tanto las tasas de procesamiento

como las de error. Una prueba operativa, por su parte, pretende evaluar el rendimiento a partir de los datos recopilados en el entorno real contemplado. Como las condiciones de adquisición de los datos resultan difíciles de controlar, esta forma de prueba quizá sea la más difícil de realizar. Existen documentos de referencia que intentan evaluar los datos operativos procedentes del programa INSPASS (Wayman, 2000).

La mayor parte de las pruebas realizadas sobre dispositivos biométricos no se divulgan públicamente. Muchos dispositivos biométricos se utilizan como componentes de sistemas de seguridad operativa, de modo que los operadores del sistema son reacios a revelar datos sobre los resultados de sus pruebas operativas. Además, tanto las pruebas tecnológicas como las hipotéticas son sumamente costosas, debido a la necesidad de asegurar el seguimiento y la gestión de toda una plantilla de personas voluntarias a lo largo de varias visitas de adquisición de datos. Los organismos públicos que financian esas pruebas generalmente no revelan sus resultados a las entidades no patrocinadoras. Muchas veces, los acuerdos de confidencialidad impuestos a los proveedores participantes en las pruebas por parte de las entidades que las llevan a cabo prohíben específicamente la divulgación de los resultados. Una excepción es el informe sobre el proyecto piloto biométrico realizado por el Ministerio del Interior y Relaciones del Reino de los Países Bajos en 2005 (también conocido como "ser o no ser"). Es una lástima que el informe sólo esté disponible en holandés (Ministerio del Interior y Relaciones del Reino de los Países Bajos, 2005). En cualquier caso, hay muy pocos productos biométricos que hayan sido sometidos a ensayos rigurosos e independientes del desarrollador o proveedor para determinar su solidez, carácter distintivo, accesibilidad, aceptabilidad y disponibilidad en aplicaciones de la vida real (y no en laboratorio).

7.6.1 Los resultados de las pruebas dependen de la aplicación

Todos los resultados de las pruebas se deben interpretar en el contexto de la aplicación de la prueba, y no se pueden transponer directamente a otras aplicaciones. Las aplicaciones varían de diversas formas, en función de:

- el grado de supervisión aplicado al registro y utilización;
- la formación y familiarización de los usuarios;

- la naturaleza de la relación existente entre el administrador del sistema y el usuario (que incide en la motivación y cooperación del usuario);
- el entorno físico donde se lleva a cabo.

La mayor parte de las pruebas se han realizado en el marco de aplicaciones altamente supervisadas, con voluntarios formados y familiarizados, en condiciones ambientales de laboratorio o de oficina. Esta es la aplicación más adecuada para las políticas de decisión que producen tasas de error reducidas y un alto nivel de aceptabilidad por el usuario. Está claro que las personas que trabajan a diario con un sistema atendido en un entorno interior y sin necesidad de transmisión de datos son las que pueden proporcionar medidas biométricas claras y repetibles. Los voluntarios habituales, que a menudo son empleados (o estudiantes) "incentivados" de la entidad que realiza la prueba, pueden ser los más capaces de percibir los sistemas biométricos como aceptables y no invasivos. Una encuesta reciente sobre la percepción pública de la biometría sacaba a la luz la existencia de un apoyo impresionante a las aplicaciones biométricas destinadas a la observancia de la ley, obtener un pasaporte u otro documento de identidad y atravesar fronteras, mientras que otras aplicaciones ocupaban posiciones inferiores en la lista (Elliot et al., 2007).

Ahora bien, no se puede esperar que el resultado de un dispositivo de acceso físico situado en un paso fronterizo al aire libre, por el que transitan usuarios ocasionales y distraídos, por ejemplo, sea el mismo que el del laboratorio. El comportamiento de esta aplicación sólo se podrá predecir a partir de mediciones realizadas sobre el mismo dispositivo en la misma aplicación. Por tanto, resulta imposible predecir el rendimiento de cualquier dispositivo biométrico en un contexto de control de la inmigración utilizando solamente datos de laboratorio.

7.6.2 Valores de prueba fundamentales

Las "prácticas óptimas para someter a prueba los dispositivos biométricos e informar de los resultados" identifican varios valores de prueba fundamentales: las tasas de registro fallido y de adquisición fallida; las tasas de falsa coincidencia y de falsa disconformidad; y el rendimiento del sistema. Para los sistemas a gran escala, y en especial

los que utilizan huellas dactilares, también se miden y comunican las tasas de error y de eficiencia asociadas a las técnicas de partición de bases de datos.

Como ya se ha señalado, las tasas finales de "aceptación indebida" y "rechazo indebido" del sistema dependerán de las medidas fundamentales y de las políticas de decisión del sistema, como también de los umbrales operativos y el número de intentos autorizado. Al igual que las tasas de "falsa coincidencia" y "falsa disconformidad", esas medidas de error también son antagónicas. Puede que lo que interese en última instancia a la administración del sistema sean las cifras absolutas de falsos rechazos y de aceptaciones indebidas que se producen en un periodo de tiempo determinado, por ejemplo en una hora o en un día. La estimación del número de incidencias dependerá no sólo de las tasas en cuestión, sino también del número de usuarios auténticos e impostores que se presenten durante ese periodo de tiempo, y del número de comparaciones generadas por cada presentación de usuario. Wayman propone un enfoque matemático rudimentario para estimar el número de errores a partir de los valores básicos de prueba (1999, 2000).

7.6.3 Curvas de compensación de los errores de decisión

El método más útil de presentar tanto las tasas de falsa coincidencia/ falsa disconformidad como las de aceptación indebida/rechazo indebido consiste en utilizar la curva de "compensación de errores de decisión (DET, por sus siglas en inglés). Estas curvas ilustran gráficamente cómo se posicionan las tasas de error las unas respecto de las otras en función de los umbrales y de las políticas de decisión. En la Figura 7-6 (Mansfield, et al., 2001) se presenta una curva DET que ilustra la compensación de la incidencia de falsa coincidencia/falsa disconformidad de tecnologías ensayadas en un entorno de tipo oficina meticulosamente controlado. La Figura 7-7 presenta la curva DET que ilustra las tasas de identificación positiva, aceptación indebida / rechazo indebido de las mismas tecnologías, pero con una política que permite tres intentos y considerando las tasas de registro y adquisición fallidas[3].

[3] La figura 7 muestra ocho tecnologías porque los datos obtenidos con el escaneo sólido de huellas dactilares no fue transmitido en línea y concierne un sistema adicional.

Estos resultados, si bien son indicativos de los rendimientos del control de acceso de estos sistemas sobre voluntarios y en un entorno de oficinas, no serían indicativos del rendimiento en la mayor parte de las aplicaciones de paso fronterizo. Tenderíamos a predecir que un entorno más difícil induciría mayores tasas de error con todas las tecnologías.

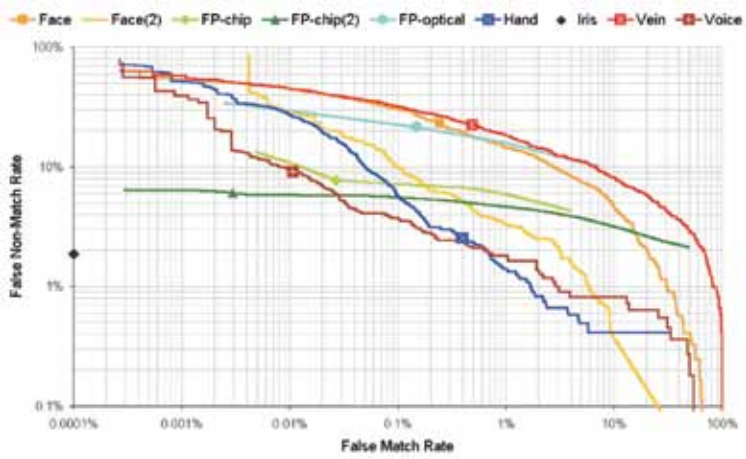


Figura 7-6: Curvas DET de falsa coincidencia/no coincidencia

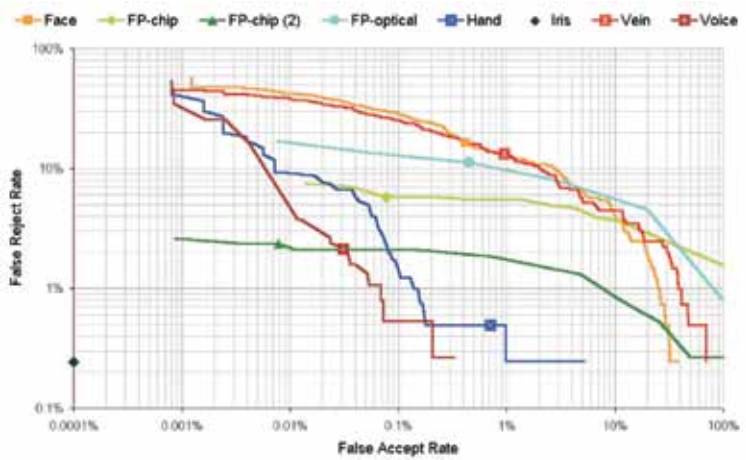


Figura 7-7: Curva DET de aceptación indebida/rechazo indebido según la “política de los tres intentos”

■ 7.7 Un ejemplo de sistema: INSPASS

7.7.1 Antecedentes

La ley federal de Estados Unidos exige que los Servicios de Ciudadanía e Inmigración de los Estados Unidos (*US Citizenship and Immigration Services,* USCIS) inspeccionen a cada persona que entra en el país. Uno de los programas desarrollados por el antiguo Servicio de Inmigración y Naturalización para automatizar el proceso de inspección es el sistema de servicio acelerado para pasajeros del Servicio de Inmigración y Naturalización de los Estados Unidos (INSPASS), que expedía un pase ligado a la geometría de la mano para los "viajeros conocidos". En las "puertas de entrada" situadas en nueve aeropuertos, los viajeros podían presentar ese pase en un terminal interactivo totalmente automatizado en lugar de enseñar su pasaporte a un funcionario de inmigración. El pase estaba vinculado al portador través de una medición de la geometría de la mano. Podían participar en el programa los ciudadanos de los Estados Unidos y de otros 26 países participantes en el "programa de renuncia al visado".

El programa INSPASS contribuía al objetivo del Gobierno estadounidense de mejorar el servicio al cliente reduciendo el tiempo dedicado por los viajeros preinscritos y de bajo riesgo a someterse a las inspecciones. Al eliminar a estos viajeros de bajo riesgo de las colas de inspección normales, se podían asignar los recursos disponibles al procesamiento de otros viajeros. La creación del INSPASS le costó al Servicio de Inmigración y Naturalización más de 18 millones de dólares EE.UU. (US DOJ, 2000).

7.7.2 Registro

Los viajeros frecuentes se podían registrar en las oficinas del INSPASS abiertas en seis de los aeropuertos participantes. Para ello, tenían que presentar un pasaporte válido y demostrar en el proceso de solicitud que no tenían antecedentes penales. Se les tomaba electrónicamente una impresión de las huellas dactilares para facilitar la comprobación de sus antecedentes. A continuación, se enviaba su nombre y número de pasaporte al Sistema Interinstitucional de Inspección de Fronteras

(*Interagency Border Inspection System*, IBIS) para comprobar que el viajero no figuraba en ninguna lista de personas en búsqueda y captura. Se enseñaba al solicitante a utilizar el sistema de geometría de la mano, y luego éste proporcionaba tres muestras de la mano a partir de las cuales se creaba un patrón medio. En el momento del registro se creaba y entregaba al viajero una tarjeta de identificación con fotografía y con indicación del nombre, sexo, nacionalidad, fecha de nacimiento y número de pasaporte, como la que aparece en la Figura 7-2. El proceso de registro completo llevaba unos 30 minutos. En 2000, había unos 60.000 usuarios registrados en el sistema. La tarjeta tenía un año de validez, y para renovarla era necesario repetir todo el proceso de registro. En la actualidad, la emisión y la utilización de la tarjeta INSPASS es totalmente gratuita.

7.7.3 Utilización de la tarjeta

Una vez inscrito, el viajero podía utilizar la tarjeta a su siguiente llegada a los Estados Unidos. A continuación se indica el número de viajeros procesados a través de los terminales del INSPASS durante el periodo comprendido entre diciembre de 1999 y noviembre de 2000:

- Nueva York (JFK) — 45.000 (siete terminales)
- Los Ángeles — 22.000 (cinco terminales)
- Miami — 41.600 (tres terminales)
- Newark — 72.000 (dos terminales)
- Toronto — 48.600 (tres terminales)
- Vancouver — 32.000 (dos terminales)
- San Francisco — 14.000 (dos terminales)
- Dulles — 4.800 (cuatro terminales)
- Detroit — 1.300 (un terminal)

Todos los terminales se encontraban en los puntos de trabajo de los inspectores de inmigración, cuya proximidad disuadía los intentos de alteración del sistema o de vandalismo. De hecho, los inspectores del INS no han detectado nunca ningún intento de vandalismo. El sistema procesaba a un viajero válido en un promedio de 30 segundos, medidos desde el momento de la inserción de la tarjeta en el lector hasta la finalización de la impresión del recibo. En esos 30 segundos,

el sistema leía la tarjeta, recibía la información sobre el vuelo (en caso necesario), validaba la muestra biométrica del usuario comparándola con el patrón registrado, actualizaba el patrón almacenado en la central, e imprimía un recibo INSPASS por el que se transmitía a la persona que cruzaba el paso fronterizo una confirmación al IBIS de la conclusión de cada validación positiva. El viajero podía salir por la puerta a los tres segundos de recoger el recibo.

Los titulares de tarjetas INSPASS tenían que llevar el pasaporte mientras utilizaban el sistema, de modo que en caso de "rechazo" por el sistema, los titulares de tarjetas INSPASS tenían la instrucción de dirigirse a la cabeza de la cola de inspección más próxima, donde se sometían a los mismos procedimientos de inmigración aplicados a los viajeros no usuarios del INSPASS. Adicionalmente, los inspectores realizaban comprobaciones aleatorias periódicas de los usuarios del INSPASS con sus pasaportes.

7.7.4 Equipos computadorizados

La Figura 7-8 presenta el terminal del INSPASS que contiene el material siguiente:

- pantalla táctil;
- unidad de geometría de la mano con transformador de corriente alterna (AC);
- convertidor de señal para la unidad de geometría de la mano;
- lector de tarjeta;
- interfaz puerta con puerta (específico para cada emplazamiento);
- transformador de señal con transformador de corriente AC;
- impresora de recibos;
- impresora de alarmas;
- servidor de impresión JetDirect;
- PC de sobremesa con teclado y ratón;
- fuente de alimentación continua;
- tarjetas adaptadoras;
- tarjeta de interfaz Red LAN;
- concentrador Ethernet de cuatro puertos;
- cables de interfaz entre todos los dispositivos y componentes;
- estructura del terminal.

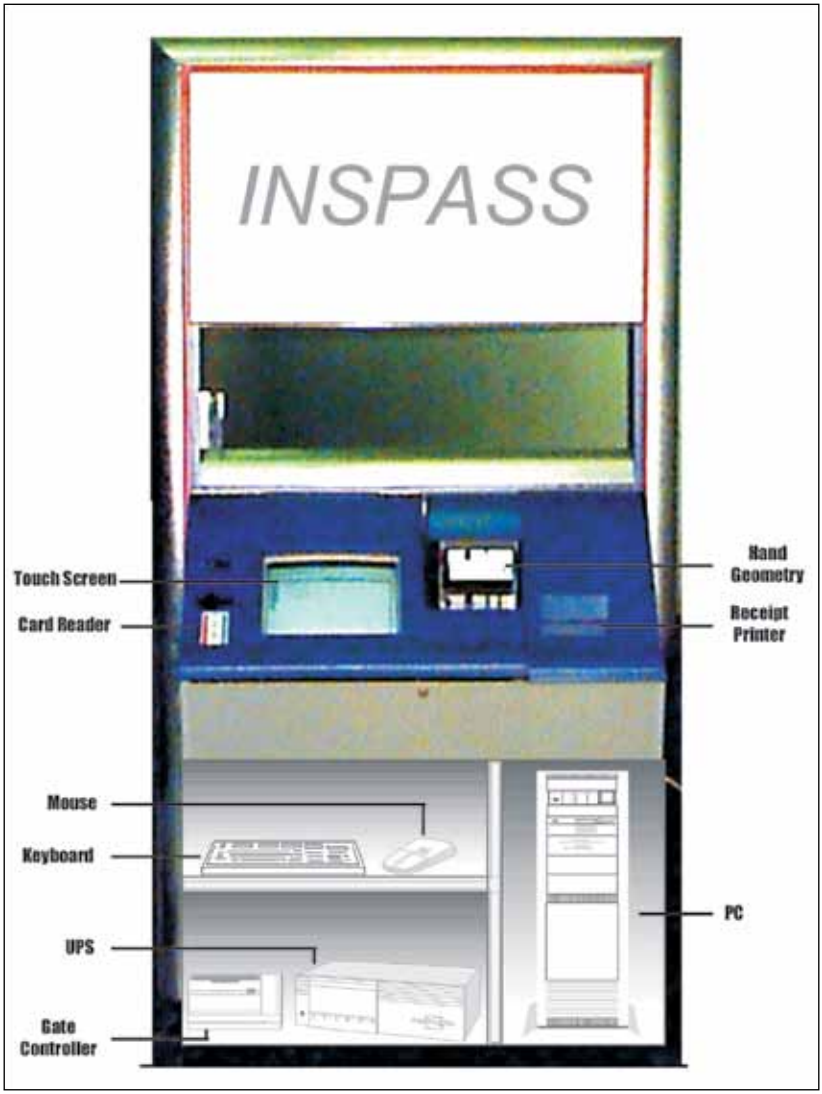


Figura 7-8: Terminal INSPASS con todos sus elementos.
(Cortesía de Jim Wayman, San José, Estados Unidos de América)

El material de una configuración típica de aeropuerto, con cuatro terminales de comprobación y un mostrador de registro, tiene un costo estimado de unos 250.000 dólares EE.UU. (Hornaday, 2001).

7.7.5 Programas computadorizados

Para el INSPASS se utilizaba el programa computadorizado siguiente:

- MS Windows para trabajo en grupo 3.11
- MS Access 2.0
- *Novell NetWare Client* 32 para Windows Versión 1.22
- *MicroTouch TouchWare Versión* 3.4
- *Dynacom/Elite Versión 3.52 DigiBoard Intelligent Board Driver para MS Windows* 3.11 Versión 1.4.3
- *Imaging Automation EyeRead Versión* 1.93
- *McAfee VShield* (version más reciente)
- *MS Open Data Base Drivers* 2.0 (16-bit)

La Figura 7-9 ilustra el diagrama de los programas computadorizados de la versión actual de INSPASS.

Un solo terminal del INSPASS podía procesar 15.000 usuarios al mes, conservando todos los datos en una base de datos local durante un periodo de tiempo indefinido. Esto permitía la producción de informes históricos. Se conservaban los datos siguientes sobre cada usuario registrado del sistema: identificación del usuario (ID), apellido, nombre, fecha de nacimiento, contraseña, fecha y hora de la última actualización, y patrones de geometría de la mano. El sistema almacenaba los datos siguientes sobre las transacciones de validación completadas: ID del usuario, clase de visado, código del país de nacionalidad, identificador del componente de validación, intentos de lectura de la tarjeta, fallos de lectura de la tarjeta, intentos de lectura de la geometría de la mano, fallos de lectura de la geometría de la mano, puntuaciones de la lectura de la geometría de la mano, correcto/fallido, motivo del fallo, fuente de información del vuelo, hora de comienzo de la transacción, hora de finalización de la transacción, hora de consulta al IBIS, tiempo de respuesta del IBIS, historial de tiempos de respuesta del IBIS, y número de mensaje.

Como el INSPASS es un sistema de tratamiento automático de los datos que procesa y almacena datos sensibles pero no reservados sobre los individuos, el acceso a su base de datos en los Estados Unidos estaba regulado por la *Privacy Act* de 1974 (US DOJ, 2006) y requería protección contra la divulgación y alteración. El acceso administrativo a las bases de datos de los terminales se controlaba a través del sistema de tarjeta y de geometría de la mano del terminal, y a tal efecto se emitía una tarjeta especial a los administradores del sistema.

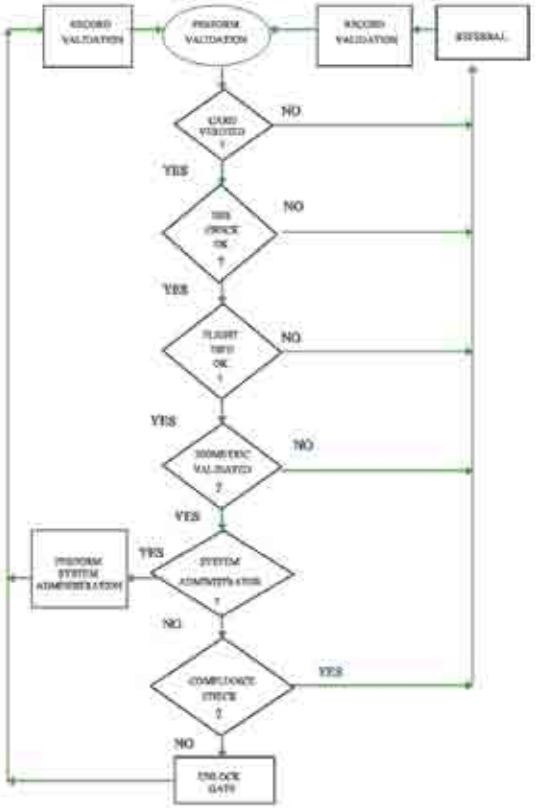


Figura 7-9: Diagrama de software de INSPASS.
Versión original de INSPASS

Referencias

Blackburn D., M. Bone, y P. J. Phillips
2001 "*Facial Recognition Vendor Test 2000 Evaluation Report*", www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.html, febrero de 2001.

CCITT
1993 "Tecnología de la información - Compresión digital y codificación de imágenes fijas de tonos continuos –Requisitos y directrices", CCITT Recomendación T.81, ISO/IEC – 10918; www.w3.org/Graphics/JPEG/itu-t81.pdf

Criminal Justice Information Services
2006 CJIS-RS-0010 (V4), *Appendix G Interim Iafis Image Quality Specifications For Scanners*, www.engr.sjsu.edu/biometrics.

Cox, R.
1997 "*Three New Speech Coders from the ITU Cover a Range of Applications*," *IEEE Communications Magazine: Special issue on Standardization and Characterization of G.729*, 35(9): 40-47, septiembre.

Departamento de Justicia de los Estados Unidos
2001 "*Management Challenges in the Department Of Justice ", US Department of Justice – Office of the Investigator General*, http://www.usdoj.gov/oig/, *1 December*. Véase también *OIG Reports #00-07* (marzo de 2000) y #95-08 (marzo de 1995)
2006 5 U.S.C. § 552A, www.usdoj.gov/04foia/privstat.htm

Elliot S. J., Massie S. A., Sutton M. J.
2007 "*The perception of Biometric Technology: A Survey*", *Proceedings of IEEE Workshop on Automatic Identification Advances Technologie*s, Alghero.

Hornaday, B.W.
2001 "*Automated ID devices are taking off at airports*", *Dallas-Fort Worth Star-Telegram, Northeast Edition*, 20 de junio.

ISO
2005 ISO/IEC 19794-4:2005 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 4: datos de imagen de huella digital.
ISO/IEC 19794-5:2005 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 5: datos de imagen facial.
ISO/IEC 19794-5:2005/Amd 1:2007 Condiciones para tomar fotografías para datos de imagen facial.

ISO/IEC 19794-6:2005 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 6: datos de imagen del iris.
ISO/IEC 19794-2:2005 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 2: datos de minucias de huella digital.

2006 ISO/IEC 19784-1:2006 Tecnología de información – Programación de interfaz aplicaciones biométricas — Parte 1: Especificación BioAPI.
ISO/IEC 19794-1:2006 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 1: Estructura.
ISO/IEC 19794-3:2006 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 3: Datos espectrales del patrón del dedo.
ISO/IEC 19794-8:2006 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 8: Esquema de datos del patrón del dedo.

2007 ISO/IEC 19794-7:2007 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 7: Datos de series temporales de la firma.
ISO/IEC 19794-9:2007 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 9: Datos de imágenes vasculares.
ISO/IEC 19794-10:2007 Tecnología de la información— Formato de intercambio de datos biométricos — Parte 10: Datos de la silueta de la geometría de la mano.

Ley pública de los Estados Unidos – Biblioteca de Derecho del Congreso
2002 "*Enhanced Border Security and Visa Entry Reform Act of 2002*" (*United States Public Law*.107-173), http://www.loc.gov/law/guide/uscode.html

Lucini, D.E.
2000 "*Minutes of the May 10, 2000 INS User Fee Advisory Committee Meeting*", *Airports Council International* – North America, http://216.205.117.217/new_website/depts/tech_envir_affairs/fi_services/MAY00_Meeting_Report_del.pdf, 26 de mayo.

Mansfield, A., G. Kelly, D. Chandler, y J. Kane.
2001 "*Biometric Product Testing Final Report*", *National Physical Laboratory*, Londres, 19 de marzo de 2001, www.cesg.gov.uk/technology/biometrics

Matsumoto T., Matsumoto H, Yamada K., Hoshino S.,
2002 *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*, *Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE* Vol. 4677.

Miller, B.
1995 "*Introduction to Identification Technologies*", *PIN Industry Sourcebook*, Miller and Warfel.

Ministerio del Interior y Relaciones del Reino de los Países Bajos
2005 "*Evaluatierapport Biometrieproef 2b or not 2b*", La Haya, http://www.minbzk.nl/ onderwerpen/persoonsgegevens-en/reisdocumenten/publicaties/54771/evaluatierapport.

National Institute of Standards and Technology (NIST)
2006 "*Data Format for the Interchange of Fingerprint, Facial, Scar, Mark and Tattoo (SMT) Information*," ANSI/NIST-ITL-1-2000, NIST Special Publication 500-245, www.itl.nist.gov/iad/894.03/fing/fing.html

2006 "*CBEFF: Common Biometric Exchange File Format*", NIST Technical Report 6529, www.itl.nist.gov/div895/isis/cbeff/CBEFF010301web.PDF, 3 de enero.

2006 "*Best Practice Recommendations for Capturing Mugshots and Facial Images*", Versión 2, www.itl.nist.gov/iad/894.03/face/bpr_mug3.html

Oficina Federal de Investigaciones
1993 "*Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification*", *Criminal Justice Information Services, Federal Bureau of Investigation*, IAFIS-IC-0110v2, 16 de febrero.

Philips, P. J., A. Martin, C. L. Wilson, y M. Przybocki
2000 "*An Introduction to Evaluating Biometric Systems. IEEE Computer*, 33(2):56-63, febrero de 2000, www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.html

Trauring, M.
1961 "*On the automatic comparison of finger ridge patterns for personal-identity verification", Hughes Research Laboratory Report* #190, marzo de 1961, copias disponibles en el *Biometric Test Center, San José State University*.

Troy, D.
2001 "*Lessons Learned from Biometric Immigration Projects*", *Biometrics 2001 Delegate Manual de la Elsevier Advanced Technology Conference*, Londres, 28-30 de noviembre.

Unión Internacional de las Telecomunicaciones
1988 Recomendaciones UIT-T G.711, "Modulación por impulsos codificados (MIC) de frecuencias vocales".
1996 G.712 "Características de la calidad de transmisión de los canales de modulación por impulsos codificados."

United Kingdom Biometric Working Group
2006 "*Best Practices in Testing and Reporting Biometric Device Performance*", versión 2.01, www.cesg.gov.uk/technology/biometrics

Van der Putte, T., y J. Keuning
2000 "*Biometrical Fingerprint Recognition: Don't let your fingers get burned", proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, Kluwer Academic Publishers*, 289-303, Londres.

Warren, J.
2001 "*Entering a twilight zone at the INS*", *Chicago Tribune*, 26 de agosto.

Wayman, J.L.
1999 "*Error Rate Equations for the General Biometric System*", *IEEE Robotics and Automatio*n, 6(1):35-48, marzo, www.engr.sjsu.edu/biometrics/nbtccw.pdf

2000 "*Evaluation INSPASS Hand Geometry Data*", in *National Biometric Test Center Collected Works: 1997-2000, San Jose State University*, disponible en Internet en www.engr.sjsu.edu/biometrics/nbtccw.pdf

2000 "*Technical Testing and Evaluation of Biometric Identification Devices*", *Biometrics: Personal Security in Networked Society, A. Jain, et al (eds.), Kluwer Academic Press*, Londres.

2001 "*Fundamentals of biometric authentication technologies*", *Int. Journal of Imaging and Graphic*s, 1(1).

CAPÍTULO 8

EL PROCESO DE IDENTIFICACIÓN DIGITAL

8.1 Introducción a la identificación digital

Este Capítulo trata sobre los principios de la identificación digital. En primer lugar, examina la identificación en general, cómo funciona, los aspectos relativos a la solicitud y expedición y el procedimiento de contratación que conllevan los documentos de identificación digital. En general, no sólo la tecnología es importante, sino también las medidas organizativas y de procedimiento, como son el mantenimiento de la seguridad y la realización de un análisis del riesgo. Estas aplicaciones y la creación de identidades digitales siempre se deben sopesar a la luz de los objetivos y riesgos implicados. Cada vez hay que plantearse dos preguntas importantes: ¿es necesario? y ¿es suficiente?

La identificación digital es muy importante en entornos donde la gente trabaja con equipos digitales o se comunica a través de ellos, por la sencilla razón de que los dispositivos digitales necesitan saber con quién están interactuando. Buen ejemplo de ello es la computadora. Cuando un la computadora está restringido a un único usuario, necesita un medio de saber que el usuario actual está autorizado. Sólo si el usuario registrado tiene una identidad digital y es el único usuario de esa identidad, podrá confirmar la computadora quién está pulsando las teclas.

La identificación digital también es necesaria para autorizar el acceso a datos almacenados en formato digital. Lo mismo ocurre con la comunicación entre seres humanos a través de medios digitales, por ejemplo a través de Internet o por correo electrónico, donde es necesaria la confirmación de la identidad de la persona. ¿Sabe realmente la gente quién está del otro lado de la línea de comunicación? ¿Se puede confiar en que el remitente de un mensaje electrónico sea también su autor?

Ahora bien, no sólo es necesario identificar a las personas. También es importante la identificación de sistemas, puesto que muchas de las tareas realizadas por seres humanos también pueden ser ejecutadas automáticamente por sistemas. Por ello, en los procesos que atañen a la implantación de la identificación digital es preciso introducir una clara distinción entre personas y sistemas.

La identificación digital también desempeña un papel decisivo en los procesos digitales seguros, como los que se aplican a los documentos de identidad seguros de gran calidad. En la actualidad, dichos documentos se personalizan mediante sistemas de alta tecnología que se nutren de datos digitales de personalización. Si esas máquinas no pudiesen comprobar que los datos los ha suministrado una persona legítima, el documento físico no tendría ningún valor.

Para comprender cómo funciona la identificación digital en los casos mencionados *supra*, ante todo hay que comentar varios principios y usos de los documentos físicos, en la medida en que se aplican también a la identidad digital. Los documentos físicos ilustran que la fiabilidad de un documento de identidad depende de la combinación de la seguridad del documento, las políticas, procedimientos y administración de la expedición, la seguridad del proceso de personalización, y el registro y la auditoría de todo el proceso. Esos mismos principios se aplican igualmente a la identificación digital.

8.1.1 Identificación física

Una persona puede demostrar su identidad de muchas maneras distintas. La forma en que lo haga dependerá de lo que tengan convenido las diversas partes interesadas. Una de esas formas consiste en presentar un documento de identidad físico. Esto permite a la parte verificadora determinar la identidad del portador y confirmar si es o no su titular registrado. Normalmente, esto se lleva a cabo mediante una fotografía. Con frecuencia, un documento tiene un periodo de vigencia limitado, que también aparece en el documento junto con el nombre de la autoridad que lo expide. La parte verificadora debe determinar si el documento es auténtico o falso. Ahí es donde los elementos de seguridad desempeñan un papel importante.

Los documentos de identidad a menudo se utilizan para la comprobación rápida y fiable de la identidad de una persona. Ahora bien, esto sólo funciona si las partes interesadas han llegado a un acuerdo sobre el nivel de fiabilidad del documento y sobre otros aspectos relativos a su expedición. Esto se puede conseguir mediante un acuerdo bilateral o multilateral, como ocurre con los documentos de viaje. Normalmente, ese acuerdo se basa en la norma aceptada por todas las partes. Sin ese tipo de acuerdo, los documentos de identidad no tendrían ningún valor, fuera cual fuese su calidad.

Las partes que utilizan los documentos confían en los aspectos detallados en la Tabla 8-1, que están relacionados con la expedición de los documentos de identidad. Éstos brindan un marco de confianza, para que las partes verificadoras puedan depositarla en un documento. Si uno o varios de estos aspectos están ausentes o incompletos, el documento deja de ser fiable.

Aspectos de confidencialidad	**Descripción**
Políticas de expedición	Conjunto de reglas que determinan la confidencialidad, el alcance y las características del documento
Procedimientos de solicitud	Aplican las políticas de expedición al proceso de solicitud, y garantizan la fiabilidad de la identidad del solicitante
Seguridad de la personalización del documento	Garantiza la fiabilidad de los datos de personalización que figuran en el del documento
Sistema de archivo de la situación del documento	Permite comprobar la validez del documento y si éste ha sido revocado o no
Registro de los procesos de solicitud y personalización y de los aspectos de seguridad que rodean a los documentos	Permite realizar auditorías, filtrados e investigaciones de los procesos para eliminar el fraude
Seguridad del documento	Garantiza la autenticidad y la integridad del documento
Auditorías de todo lo anterior	Confirma que las políticas se han aplicado adecuadamente y consolida el nivel de confidencialidad. La retroinformación resultante permite formular recomendaciones de mejora

Tabla 8- 1: Aspectos de confidencialidad relacionados con la identificación digital

8.1.2 Identificación digital

A menudo la necesidad de que una persona demuestre su identidad surge cuando las partes desconocen la verdadera identidad de esa persona. Sólo en las situaciones en las que se reconoce a una persona por su aspecto o por su voz resulta innecesaria la comprobación de la identidad por medio de un documento. No obstante, el mundo digital carece de un método de identificación tan fácilmente discernible. Por ejemplo, cuando se recibe un mensaje electrónico normal, no hay manera de saber quién lo ha escrito o enviado realmente. Podría haber sido cualquiera.

En el mundo digital, la identificación de las personas y los dispositivos se suele llevar a cabo mediante una combinación de los datos de identidad y una clave secreta. Una persona o dispositivo aplica una clave secreta para demostrar que los datos de identidad son realmente suyos. Por ejemplo, un nombre de usuario puede servir de dato de identidad, y una contraseña de clave secreta. El principio subyacente es que sólo el propietario registrado conoce la clave secreta, y sólo él la puede utilizar para validar sus datos de identidad. Este proceso de verificación digital se denomina autenticación. Igual que ocurre con los documentos físicos, el contexto de utilización de la clave debe ser suficientemente seguro como para que no quepa duda de que el usuario es el titular registrado de la clave.

Es preciso establecer una distinción entre autenticaciones frágiles y robustas. En la autenticación frágil, el usuario proporciona manualmente los datos de identidad o, si utiliza un dispositivo, los extrae de un archivo. La forma más corriente consiste en la utilización de nombres de usuario y contraseñas. En la autenticación robusta, se almacena una clave secreta en un soporte seguro, por ejemplo una tarjeta inteligente a prueba de alteraciones. Esa clave secreta sólo se puede utilizar si el usuario introduce un código secreto. La identificación robusta se basa en el principio de que el usuario posee algo (un soporte) y también sabe algo (una contraseña). También se pueden utilizar los rasgos físicos (biometría) para producir la combinación siguiente: el usuario *tiene* algo (soporte) y *es* algo (biometría), completado posiblemente con el *conocimiento de* algo (contraseña).

Este Capítulo sólo se centra en la autenticación robusta, que presupone la utilización de un soporte seguro por parte de personas. Si bien se puede utilizar la misma técnica sin un soporte seguro, la ausencia del mismo reduce el nivel de seguridad.

Para ilustrar la diferencia entre la identificación digital mediante la autenticación robusta y la identificación física, examinaremos cómo se retira dinero en efectivo de un cajero automático y las salvaguardas que entraña la operación. Aunque normalmente una tarjeta bancaria no suele ser una tarjeta inteligente, el mismo proceso se puede aplicar a una tarjeta inteligente. Ese proceso se ilustra en la Figura 8-1.

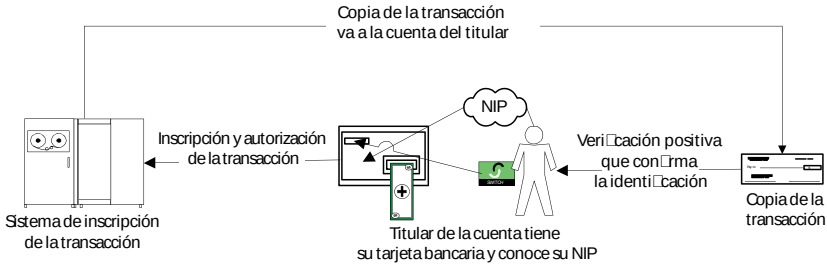


Figura 8-1: El titular de una cuenta bancaria tiene una tarjeta bancaria y conoce su NIP, que le permite retirar dinero de un cajero automático. Se introduce la transacción y se envía un extracto de cuenta al titular. Si éste acepta dicha transacción, se confirma la verificación positiva.

El cajero automático lee todos los datos de identificación de la tarjeta bancaria para que se pueda retirar el efectivo de la cuenta bancaria correspondiente. Sin embargo, en este punto el cajero automático no sabe si quien ha introducido la tarjeta es el propietario registrado u otra persona. Para comprobarlo, la máquina pide una información que sólo conoce el titular de la cuenta, a saber su Número de identificación personal (NIP o PIN, por sus siglas en inglés). Este número de identificación personal es la clave secreta que confirma la identidad del titular de la cuenta. Una vez introducido el NIP correcto, se lleva a cabo una verificación positiva y la máquina expide el importe solicitado.

Si el titular de la cuenta mantiene secreto su número de identificación personal, este mecanismo de autenticación será siempre robusto. Pero si éste se compromete, se guarda en malas condiciones o se comunica a un tercero, cualquier persona que tenga acceso a la tarjeta y al NIP

puede superar una verificación positiva. Por eso ha de incorporarse una comprobación adicional. El cajero automático administra la transacción, y se envía un extracto bancario al titular de la cuenta. Si el titular de la cuenta descubre en su extracto bancario que otra persona ha retirado ilegalmente dinero de su cuenta, puede reclamar el importe, anular la tarjeta y el NIP, y pedir una nueva tarjeta con su correspondiente NIP.

Para que el sistema funcione, el uso de la tarjeta bancaria y del NIP debe estar restringido al titular de la cuenta exclusivamente. Cuando alguien solicita una tarjeta bancaria, el banco debe comprobar que el solicitante y el titular de la cuenta son realmente una misma y única persona. Por ello, hay que enviar al titular la tarjeta bancaria y el NIP por separado, para asegurarse de que no puedan ser interceptados simultáneamente. El NIP va protegido en un sobre sellado para mantenerlo secreto, y su integridad es comprobable, es decir que el sobre no tiene que llegar abierto al destinatario.

Esta breve descripción del proceso de retirada de efectivo de un cajero automático utilizando una tarjeta bancaria demuestra que la identificación digital presenta similitudes con el uso de documentos de identidad físicos. La transacción no consiste únicamente en procedimientos técnicos, sino que también cabe aplicar el conjunto de reglas detallado en la Tabla 8-1.

■ 8.2 Cómo funciona la identificación digital

Hasta aquí, hemos examinado el contexto de aplicación de la identificación digital, pero todavía no hemos dicho nada sobre cómo funciona realmente la identificación digital. El apartado siguiente presenta un breve resumen del funcionamiento de la identificación digital en general y de la Infraestructura de clave pública (ICP, o PKI por sus siglas en inglés) en particular.

8.2.1 La identificación digital en general

La identidad digital se suele basar en la tecnología criptográfica. Alguien tiene un código secreto o una clave secreta que se utiliza para convertir los datos simples en datos cifrados. El proceso se lleva a

cabo de manera que, sin la clave secreta, nadie pueda reproducir los datos simples originales a partir de los datos cifrados. El texto cifrado sólo puede ser generado por el propietario de dicha clave secreta. La identidad se puede verificar comprobando si los datos se han cifrado con la clave secreta asociada a la identidad de una persona en concreto.

8.2.2 Cifrado simétrico

El cifrado simétrico tiene lugar cuando el cifrado y el descifrado se llevan a cabo mediante una única clave, como se puede observar en la Figura 8-2.

Figura 8-2: En el cifrado simétrico una única clave secreta compartida se utiliza para cifrar y descifrar los datos. Tanto la parte del cifrado como la del descifrado pueden utilizar la misma clave y realizar las mismas operaciones.

Cada parte debe tener su propia clave secreta, y sólo debe utilizar esa clave secreta para el cifrado de datos de autenticación. Para aplicar el cifrado simétrico, cada parte debe tener una copia de la clave secreta de la otra parte. Esto significa que en la autenticación, nadie sabe si el remitente es realmente el titular de la clave secreta (Rivest et al., 1978). Además, la gestión de claves es muy complicada. Las claves secretas se deben distribuir de forma segura a todas las partes, y cada parte debe guardar celosamente sus claves para salvaguardar la integridad del sistema. Todo esto hace que el cifrado simétrico no resulte adecuado para la identificación digital. Normalmente, esta técnica sólo se utiliza para mantener el secreto de datos sensibles.

8.2.3 Cifrado asimétrico

También se pueden utilizar dos claves distintas y complementarias: una para el cifrado y otra para el descifrado. No se pueden descifrar datos con la misma clave que se ha utilizado para su cifrado, que requiere la clave complementaria. Esa técnica se denomina cifrado asimétrico (Rivest et al., 1978; Schneier, 1995).

Una de las claves a las que se hace referencia es la clave pública. No es necesario mantener dicha clave en secreto, y puede estar a disposición del público. La otra clave, sin embargo, es la clave secreta, que sólo debe ser revelada a su titular y sólo debe ser utilizada por éste. Para mantener la confidencialidad de la información, una persona utiliza dicha clave secreta para cifrar datos simples mediante la función criptográfica P (véase la Figura 8-3.). Por consiguiente, los datos cifrados sólo se pueden descifrar mediante la función criptográfica complementaria S y la clave secreta. Por lo tanto, el propietario de la clave secreta es el único que puede descifrar los datos. Como la clave pública está a disposición del público, cualquiera que tenga acceso a la clave pública puede utilizarla para enviar datos seguros al propietario de la clave secreta.

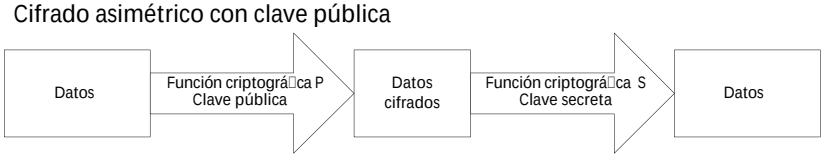


Figura 8-3: Con el cifrado asimétrico, los datos cifrados con la clave pública únicamente pueden ser descifrados con la clave secreta, que sólo conoce el titular de ésta.

El cifrado asimétrico tiene otra particularidad interesante para la identificación. Desde un punto de vista técnico, también se puede utilizar la función criptográfica S junto con la clave secreta para cifrar datos simples (véase la Figura 8-4.). El titular de la clave secreta es la única persona que puede hacerlo. De ese modo, utilizando la función criptográfica P cualquiera que tenga acceso a la clave pública puede utilizar los datos cifrados para descifrar los datos simples originales mediante la aplicación de la clave pública asociada. Por consiguiente, cualquiera que tenga acceso a la clave pública puede descifrar los datos cifrados con la clave secreta.

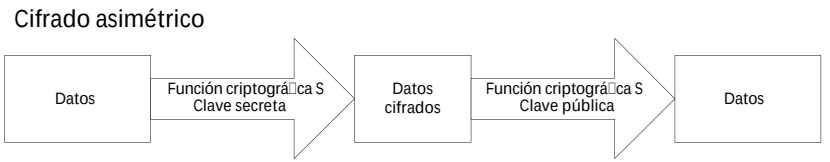


Figura 8-4: Con el cifrado asimétrico, los datos que han sido cifrados con la clave secreta, que sólo conoce el titular, únicamente pueden ser descifrados con la clave pública.

Así, la autenticación resulta fácil. Cualquiera que desee autenticarse tiene que cifrar con su clave secreta una serie de datos conocidos por la parte verificadora. Entonces se puede comprobar la identidad declarada mediante la descodificación de los datos cifrados, que se lleva a cabo aplicando la clave pública correspondiente a la identidad de la persona que solicita la autenticación. Si tiene éxito, la persona es autenticada positivamente.

También se puede crear un código único del mensaje que vaya a enviarse, que es una representación exacta de dicho mensaje. Este código, también llamado resumen del mensaje, se crea de tal manera que a partir de un mismo resumen del mensaje es imposible extraer un mensaje de significado distinto del mensaje original. Si los datos del mensaje se alteran de algún modo, el resumen del mensaje cambia completamente. Se cifra mediante una clave secreta, de manera que el destinatario pueda descifrarlo y cotejarlo con el mensaje recibido. Si son iguales, el destinatario sabe con seguridad quién es el remitente (siempre que tenga acceso a la clave secreta) y que el mensaje está intacto. Esta técnica se describe en la Figura 8-3, y se utiliza para firmar digitalmente documentos con objeto de garantizar la integridad el documento (Schneier, 1995; ISO, 2001).

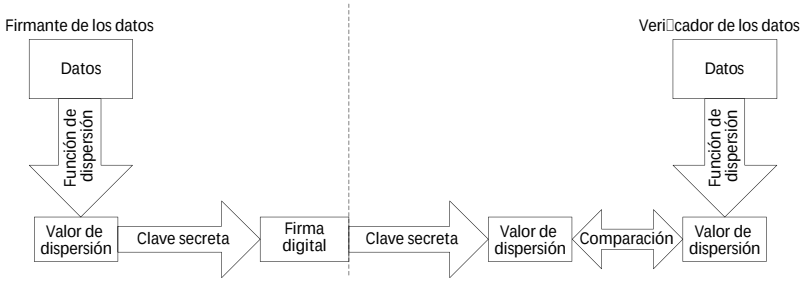


Figura 8-5: Proceso de generación de una firma digital

Tal como se ilustra en la Figura 8-5, la firma digital se puede conseguir en dos etapas. En primer lugar, se somete a los datos a una función de dispersión para generar un código único para los datos, mediante la que incluso la más ligera modificación de los datos – basta un bit para ello – puede dar lugar a un código completamente distinto. La función de dispersión se descifra mediante la clave secreta de la parte signataria. La

firma se comprueba descifrando la firma digital con la clave pública de la parte signataria. Eso garantiza que la parte signataria sea la persona que declara ser. Se procede a sondear los datos, y si son idénticos a los datos firmados, dan el mismo resultado que los datos descifrados.

Si un remitente cifra un mensaje o datos con la clave pública del destinatario, sólo el destinatario, es decir, el titular de la clave secreta correspondiente, puede abrir el mensaje en cuestión. Esta técnica se utiliza para garantizar la confidencialidad.

Si el propietario de una clave secreta he generado dicha clave sin ayuda externa, él es el único que conoce dicha clave. Si el propietario de esa clave firma digitalmente un documento, mensaje o transacción, le resulta prácticamente imposible negar que lo haya hecho. Con ello, se consigue un sistema que garantiza un no repudio completo e independiente.

Existen diversas funciones matemáticas que pueden aplicarse igualmente al cifrado asimétrico. También puede modificarse el tamaño de la clave. La norma general es que cuanto más larga es la clave, mayor es la seguridad, pero también es mayor el tiempo de procesamiento. Por consiguiente, una clave más larga conlleva una espera más larga. Para seleccionar el tamaño de la función matemática y de la clave que la acompaña conviene consultar a un experto. Las funciones matemáticas pueden dejar de ser utilizables debido al desarrollo de funciones mejoradas o a la sustitución de la tecnología. Por lo que se refiere al tamaño de la clave, tiene que ser suficientemente larga como para que no se pueda adivinar o predecir. Normalmente, la fuerza de una clave disminuye con el paso del tiempo, porque el equipo de computación más reciente facilita el pirateo de una clave.

8.2.4 La infraestructura de clave pública

Quedan dos preguntas por responder: ¿Cómo se puede reconocer la autenticidad de las claves públicas, y cómo sabemos quién es el titular de la clave privada?

La respuesta a ambas es un certificado o un documento de identidad digital. Éste contiene información sobre el titular, como su nombre, su fecha de nacimiento o su número de identidad. Además, la clave pública del titular también contiene información sobre la vigencia, el nivel de confidencialidad del certificado y el nombre de la entidad emisora. Existen diversos formatos de certificado, pero la norma más corriente para la ICP es el formato de certificado X.509 (ISO, 2001; Housely et al.; 2002).

Estos certificados constituyen el corazón de la infraestructura que presta servicios basados en el cifrado asimétrico, conocida como infraestructura de clave pública (ICP). El certificado lleva la firma digital de la Autoridad Certificadora (AC). Los usuarios de la infraestructura de clave pública (ICP) conocen y confían en la Autoridad Certificadora y en su certificado. Mediante un certificado de la Autoridad Certificadora se pueden autenticar también otros certificados emitidos por la propia Autoridad Certificadora.

Según las especificaciones de la Unión Europea en materia de pasaportes, cada Estado miembro debe establecer una única *AC signataria del país* que actúe como punto de confianza nacional para todos los Estados receptores y al menos un *Signatario de Documentos* que emita pasaportes. Con respecto a los detalles sobre la ICP, este documento hace referencia a un informe técnico del Grupo de Trabajo sobre Nuevas Tecnologías de la OACI (OACI, 2004), recientemente integrado en el Documento 9303 de la OACI (OACI, 2006).

La arquitectura de la infraestructura de clave pública se basa en la tecnología de cifrado asimétrico, que por sí misma no garantiza una seguridad global. Como ocurre con los documentos físicos, el proceso de obtención de un documento y los procedimientos administrativos asociados también desempeñan un papel muy importante por lo que respecta a la seguridad. Por ejemplo, si la tecnología proporciona una seguridad adecuada pero el procedimiento tolera el uso de una falsa identidad, evidentemente el sistema no es adecuado para la comprobación de la identidad. Esto mismo es aplicable a la Autoridad Certificadora. Si ésta es incapaz de garantizar que un individuo es el

único poseedor de la clave secreta de la Autoridad Certificadora para firmar certificados, entonces existe incertidumbre sobre si el certificado fue realmente emitido por la Autoridad Certificadora, habida cuenta de que otra persona podría haber utilizado una copia de la clave de la Autoridad Certificadora.

En una infraestructura de clave pública, una Autoridad de Registro (AR) tramita la solicitud y la comprobación de la identidad de un solicitante, siguiendo un proceso idéntico al observado para la obtención de un documento de identidad físico. La calidad y la gestión de los procedimientos determinan la confianza que se puede depositar en el valor de la identificación por medio de un certificado digital. Dado que los certificados se pueden revocar, la Autoridad Certificadora tiene que mantener y publicar también una lista de todos los certificados revocados. Esa lista se puede consultar de tres maneras distintas: a través de una lista de revocación de certificados (CRL, por sus siglas en inglés), de un protocolo en línea de la situación del certificado (OCSP) y de un protocolo en línea para la norma Internet XML (XKMS).

La entidad expedidora, es decir la Autoridad Certificadora (AC) de una infraestructura de clave pública (ICP), publica un documento que establece las directrices y medidas relativas a la seguridad. Ese documento establece el valor de confidencialidad conjunto de los certificados en el marco de la ICP. Se podría comparar con los aspectos detallados en la Tabla 8-1 relativa a los documentos de identidad en el mundo físico. Ese documento suele constar de dos partes:

i. La política de certificación (PC), que es una "colección definida de directrices que determinan la aplicabilidad de una certificación dentro de cierta comunidad y/o con necesidades comunes en materia de seguridad" (ISO, 2001); y
ii. la declaración de prácticas de certificación (DPC), que es una "explicación de las medidas y procedimientos utilizados por una Autoridad Certificadora para emitir las certificaciones' (*American Bar Association*, 1997).

Se suele hacer referencia a estas dos partes como la PC y la DPC de la AC. Internet RFC 2527 brinda un marco a los redactores de documentos

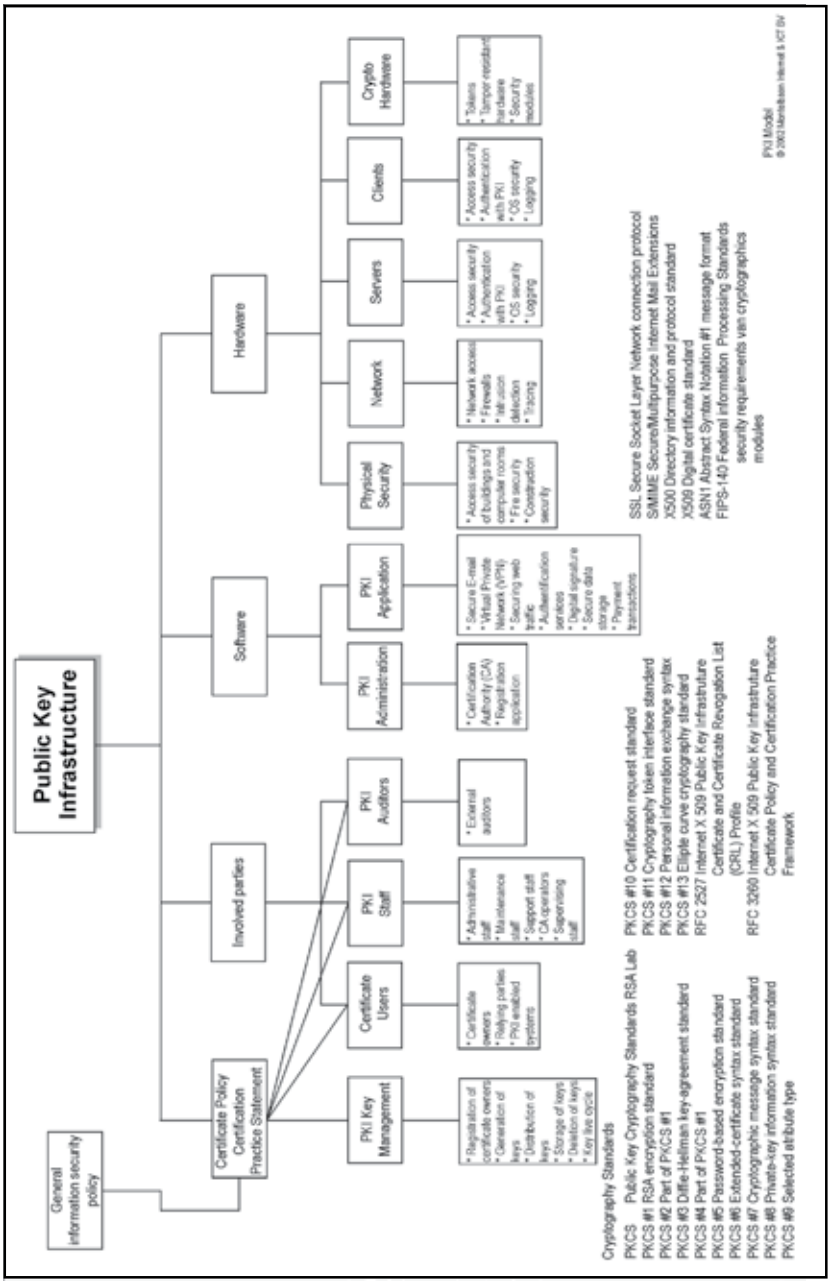


Figura 8-6: Estructura de una ICP
Modelo original de PKI (ICP)

de PC y DPC. La PC y la DPC son complementarias, y garantizan un nivel eficiente de seguridad de la certificación.

El marco global de una infraestructura de clave pública se ilustra en la Figura 8-6, que indica cuáles son los elementos importantes de una ICP. Para crear una ICP, lo mejor es empezar por la PC/DPC. Para proceder a ello, se debe disponer de la política de seguridad general, con objeto de garantizar que la ICP brinde un nivel de seguridad adecuado en función del entorno de aplicación. Por ejemplo, en el proceso de solicitud de documentos de viaje, la ICP tiene que garantizar que los datos de personalización sean tan seguros como el resto del proceso de personalización.

Como se ha demostrado en el modelo, la PC/DPC impone reglas, obligaciones y procedimientos a los usuarios. Los auditores de ICP desempeñan un papel importante en las comprobaciones periódicas de la ICP. Garantizan que lo que sucede en la práctica real se adecua a la PC/DPC, y elaboran propuestas de mejoras.

Los programas computadorizados del usuario deben ser adecuados para una ICP. Ahora bien, esto no significa automáticamente que el programa computadorizado sea seguro. Si la lógica de procesos del programa computadorizado no es segura, la ICP no podrá remediarlo. El diseño y la implantación de la ICP en la solicitud deben ser objeto de un atento escrutinio y de pruebas extensivas.

La Figura 8-6 presenta la estructura de una ICP. Existen cuatro componentes fundamentales: la PC/DPC, los usuarios implicados, el programa computadorizado y el equipo computadorizado. La PC/DPC debe ser acorde con la política de seguridad general. Impone reglas, obligaciones y procedimientos a los usuarios. El programa computadorizado hace posible la utilización de la ICP. El equipo de computación también es importante, porque está directamente expuesto a las amenazas a la ICP.

8.2.5 Autenticidad de las certificaciones

La firma digital de la Autoridad Certificadora garantiza la autenticidad de las certificaciones. El único elemento secreto de las mismas es la

clave secreta de la Autoridad Certificadora, a diferencia de la función de dispersión y demás funciones criptográficas que están a disposición pública. La clave secreta debe ser lo suficientemente larga como para impedir que se adivine. Esto significa que la tecnología de ICP es del dominio público. El hecho de que todas las funciones matemáticas de la ICP sean del dominio público es lo que confiere a ésta su carácter seguro, puesto que no existe ningún factor de seguridad expuesto a posibles violaciones, con excepción de la clave secreta. Pero si se rompe el secreto de la clave, sólo queda comprometida una única certificación, y el sistema sigue siendo seguro. En las certificaciones digitales, ningún elemento de seguridad está basado en el secreto ni se cuenta con la "seguridad por opacidad". Esto significa que la seguridad no se garantiza mediante algoritmos matemáticos secretos.

8.2.6 Utilización de una infraestructura de clave pública para la identificación digital

Existen muchas maneras de utilizar las certificaciones de una ICP como documentos de identificación digital, como por ejemplo para proteger el acceso a un edificio, una computadora, agendas digitales de bolsillo, teléfonos móviles, una red, bases de datos, etc. Existe una diferencia fundamental con respecto al mundo físico, y es que en ocasiones las personas se identifican digitalmente a través de un dispositivo digital, en lugar de identificarse en persona ante otras personas. Este apartado comenta varios aspectos característicos de la aplicación de la identificación digital.

En general, las certificaciones de una ICP están destinadas a la identificación del titular. Tras la autenticación, un proceso de autorización brinda acceso al sistema al titular de la certificación. Las certificaciones se pueden aplicar de diversas maneras al proceso de autenticación y autorización.

Una posibilidad es que la certificación sólo contenga los datos de identidad del propietario. En ese caso, la certificación se utiliza a efectos de autenticación en un sistema, y un proceso de autorización del sistema permite al usuario el acceso para el cual está autorizado. El usuario también puede utilizar esa misma certificación para autenticarse

en diversos sistemas mediante la misma certificación, y en ese contexto los derechos que se le reconozcan en cada sistema estarán vinculados a la identidad comprobada en el proceso de autorización. Esta aplicación permite el registro de todas las acciones del usuario a través de su identidad.

Una segunda opción consiste en que la certificación contenga datos sobre la función de un usuario, lo cual permite que la certificación vincule autorización y autenticación. No es necesario un proceso independiente de autorización para el sistema, puesto que en este caso no se reconoce al usuario a través de su identidad personal, sino como a alguien que desempeña una función determinada, y es la función la que está directamente vinculada a la autorización. Una de las ventajas de este enfoque reside en que pueden usar las certificaciones varias personas que desempeñen la misma función. Otra de ellas es que los nuevos usuarios del sistema pueden reutilizar las certificaciones de otros usuarios. Ahora bien, esta aplicación no es adecuada cuando se responsabiliza a los usuarios de sus acciones en el sistema. Otro aspecto que hay que tener en cuenta es que la certificación no podrá ser utilizada fácilmente en otros sistemas.

Una tercera posibilidad es que además de datos sobre la función del titular, la certificación contenga datos sobre su identidad. En ese caso, las certificaciones se podrán utilizar para los dos mecanismos reseñados más arriba. Esto puede resultar útil si en los sistemas las funciones están reservadas a personas específicas autorizadas, pero dicha autorización se expide fuera del sistema. Por ejemplo, si una organización que no tiene acceso a un a sistema autoriza a miembros de su plantilla a realizar determinadas acciones, entonces la autorización se podrá comprobar por esa vía. La solicitud de autorización se remite a la organización que otorga la autorización. Esa autorización se transmite a la Autoridad Certificadora, y ésta emite el certificado especial. De ese modo, la organización que expide la autorización tiene un control remoto sobre el sistema.

8.2.7 Autorización, firma digital y cifrado de los datos

Otro punto importante es que una certificación se puede utilizar no sólo a efectos de autenticación, sino también para firmas digitales y para cifrar datos exclusivos. Desde el punto de vista técnico, es posible realizar esas tres acciones usando una única certificación. Sin embargo, los requisitos de estas tres acciones pueden variar considerablemente. Es importante decidir si se emite una única certificación para las tres acciones, o varias certificaciones digitales para las diversas acciones. Si una certificación es adecuada para el cifrado de datos exclusivos, probablemente la clave secreta de cifrado requiera un mecanismo de custodia por un tercero. Se puede utilizar para descifrar datos codificados en caso de que se pierda la clave secreta. En cambio, no es necesario para las certificaciones utilizadas a efectos de autenticación o de firmas digitales, porque en esos casos sólo es necesaria la clave pública para descifrarlas. Es más, para la autenticación y las firmas digitales, sería incluso indeseable un mecanismo de custodia por terceros, pues significaría que una clave secreta podría ser conocida por un tercero, o que alguien podría tener acceso a ella sin que nadie lo advirtiera. Ese tipo de clave secreta se debe generar a partir de una tarjeta inteligente para las aplicaciones de gran calidad, y hay que descartar que la clave secreta se pueda leer a partir de la tarjeta inteligente. Eso garantiza que sólo el microprocesador de la tarjeta inteligente podrá utilizar la clave secreta, pero significa que las funciones de cifrado a efectos de autenticación y de firmas digitales también deberán ser ejecutadas por la tarjeta inteligente.

La autenticación y las firmas digitales pueden imponer también diversas exigencias en cuanto a los procedimientos utilizados. Por ejemplo, las directivas de la UE relativas a las certificaciones de firmas digitales requieren que la parte emisora acepte una responsabilidad limitada (UE, 1999).

Hay que considerar asimismo si es necesaria una certificación de firma digital cuando se emite una certificación de autenticación. Un ejemplo de protocolo que usa un solo certificado para la autenticación y el cifrado de datos es el protocolo de conexión segura SSL (*Secure*

Socket Layer) (*Freier* et al., 1996). Ese protocolo utiliza un certificado de autenticación para el cifrado de datos que no crea problemas de recuperación porque los datos sólo están codificados durante el envío y no se requiere su almacenamiento. Como el cifrado sólo se utiliza para la transmisión de datos, no es necesaria la custodia de la clave por un tercero. Eso garantiza que no se pueda producir un acceso indiscreto a los datos y que ninguna otra parte tenga acceso a la clave secreta.

8.2.8 Licitación de una infraestructura de clave pública

Cuando se saca a concurso un sistema o servicio de ICP, y tanto si está llamado a formar parte de un sistema más amplio como si no, se plantean varias cuestiones importantes.

La licitación debe incluir una lista clara de requisitos, que especifiquen el nivel de seguridad que se pretende implantar. Eso permite a la parte contratante evaluar eficazmente las ofertas, y de ese modo también se puede cotejar fácilmente con la lista cualquier cambio efectuado durante la implantación.

En el caso de una ICP, la licitación debe incluir los términos detallados en la Tabla 8-2.

Política de seguridad	Determina el nivel de seguridad requerido
Análisis de riesgos	Determina los riesgos para la seguridad y el nivel de contramedidas necesario
Política de certificación	Define el nivel de confidencialidad de la ICP
Arquitectura general y procedimientos	Indica los requisitos funcionales del sistema operativo
Especificaciones técnicas	Indica los requisitos técnicos que debe cumplir el sistema
Criterios de aceptación	Define qué criterios debe cumplir el sistema para ser aceptado

Tabla 8- 2: Aspectos que han de contemplarse al sacar a concurso público una ICP

Lo anterior se basa en el supuesto de que los usuarios del sistema y de la computadora utilicen la ICP a efectos de autenticación robusta y de firmas digitales, posiblemente en combinación con el secreto. Incluso en el caso de Tecnología de Información que no utilice una ICP, las entradas de la Tabla 8-2 siguen siendo aplicables a los concursos públicos, excepto la política de certificación.

■ 8.3 Política de seguridad

Ha de elaborarse una política de seguridad general aplicable a todas las partes del sistema o servicio licitado. Dicha política se debe incluir en las condiciones de licitación, con objeto de sentar una línea de partida para la seguridad general y para la seguridad informática en particular. El *Código de buenas prácticas para la gestión de la seguridad de la información* (ISO, 2005) contiene un manual al respecto.

8.3.1 Análisis de riesgos

Como se ha explicado anteriormente, no sólo tienen que ser seguros el servicio de ICP o de certificación digital, sino toda la cadena del proceso. Se trata de alcanzar el equilibrio adecuado entre las Tecnología de Información, los procedimientos, las personas, la organización y los demás sistemas.

Para conseguir el nivel de seguridad deseado, hay que llevar a cabo un análisis de riesgos. Dicho análisis debe describir la interdependencia de la seguridad de los procedimientos, la organización, las personas, los sistemas y las revisiones y auditorías. Se debe combinar con un análisis de la vulnerabilidad de dichos componentes entre sí. El principio básico es que la seguridad del sistema es una cadena, y todos los eslabones de la cadena deben ser igual de resistentes. El análisis de riesgos se utiliza para describir las relaciones de seguridad entre los diversos eslabones, y para definir las medidas necesarias para alcanzar el nivel de seguridad deseado (BSI, 2004; ISO 2005).

La inclusión de un análisis de riesgos ofrece a los proveedores una idea de las medidas que hay que tomar para gestionar los riesgos.

8.3.2 Política de certificación

Este documento describe la política de emisión de certificaciones digitales. Una guía útil para ese documento es Internet RFC 2527 (Chokhani y Ford, 1999). La política de certificación estipula los requisitos que debe cumplir la ICP, que en realidad son equivalentes a los que debe ofrecer el licitador. Aunque una ICP forme parte de un sistema más amplio, sigue siendo

importante incluir este documento en el pliego de condiciones de la licitación.

8.3.3 Arquitectura y procedimientos operativos

En el pliego de condiciones del concurso también habrá que incluir la arquitectura del sistema. Es aconsejable incluir asimismo en el pliego del concurso modelos de datos para los interfaces y mensajes. Esto es especialmente importante cuando se intercambian datos de intercambio entre diversas bases de datos.

Hay que incluir los procedimientos operativos de modo que el licitador sepa qué funcionalidad debe proporcionar.

8.3.4 Especificaciones técnicas

También hay que incluir las especificaciones técnicas para aclarar cuáles son los requisitos de seguridad específicos. Éstos deben ser punteros, para permitir seguir el ritmo acelerado de la evolución de las condiciones de seguridad en el universo digital. También es necesario definir e implantar un mecanismo que permita alterar, mejorar y actualizar los componentes de seguridad. Dicho mecanismo debe incluir los aspectos enumerados en la Tabla 8-2.

8.3.5 Criterios de aceptación

Los criterios de aceptación deben incluir los requisitos de seguridad descritos en la política de seguridad, el análisis de riesgos y las especificaciones técnicas. Si los criterios de aceptación sólo contienen las especificaciones técnicas, se corre el riesgo de que el resultado final se desvíe de los requisitos estipulados en la política de seguridad y en el análisis de riesgos.

Referencias

American Bar Association
1997 *Digital Signature Guidelines*

Bundesamt für Sicherheit in der Informationstechnik
2004 *IT-Grundschutz Manual: Catalogues of safeguard*s, Bonn, Alemania

Chokhani S. y W. Ford
1999 RFC 2527; *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

Freier A.O., P. Karlton y P.C. Kocher
1996 *The SSL Protocol* Versión 3.0, *Transport Layer Security Working Group* 18 de noviembre de 1996, Proyecto-Internet, http://wp.netscape.com/eng/ssl3/ssl-toc.html.

Housley R., W. Polk, W. Ford, y D. Solo
2002 *RFC 3280; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

ISO
2001 *ISO/IEC 9594-8:2001; Information technology – Open systems Interconnection – The directory: Public-key and attribute certificate framework*s, Ginebra.
2005 *ISO/IEC 17799: 2005, Tecnología de la información – Código de buenas prácticas para la gestión de la seguridad de la información*, Ginebra.

OACI, NTWG
2004 *PKI for Machine Readable Travel Documents Offering ICC, Read-Only Acces*s, Informe técnico, versión 1.1
2006 Documento 9303 – Parte 1 Pasaportes de lectura mecánica, Volumen 2 *Specifications for electronically enabled passports with biometric identification capabilities,* Montreal, Canadá

Rivest R.L., A. Shamir and L.M. Adleman
1978 "*Method for Obtaining Digital Signatures and Public-Key Cryptosystems*", *Communications of the ACM*, 21(2): 120-126.

Schneier B.
1995 *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2ª edición, John Wiley & Sons, Nueva York.

Unión Europea

1999 *Marco comunitario para la firma electrónica*, Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999.

2006 *Biometric deployment of EU passports: EU passport specification*, documento de trabajo.

CAPÍTULO 9

INFORMACIÓN, COOPERACIÓN Y FORMACIÓN

9.1 Fuentes de información

Este Capítulo ofrece diversas fuentes de información sobre el desarrollo de documentos seguros, incluida una selección de entidades, empresas y sitios Web dedicados específicamente a los documentos seguros. La ubicación geográfica, el segmento del mercado y los medios financieros tienen un gran peso en la selección de proveedores, de modo que la información siguiente se debe utilizar como mera referencia para el estudio ulterior.

9.1.1 Información sobre los documentos de instituciones internacionales y organismos públicos

La Organización de Aviación Civil Internacional (OACI) tiene un sitio Web dedicado enteramente a los documentos de lectura mecánica. Permite conocer el Documento 9303 de la OACI y diversos documentos técnicos que sirven de base para el desarrollo de documentos de viaje (véase la información detallada en la sección 2.6.2).

El sitio Web de la Unión Europea contiene información sobre la legislación europea relativa a los documentos de identidad y de viaje (véase la información detallada en la sección 2.6.5).

El Banco Central Europeo (BCE) tiene un sitio web que ofrece información sobre los nuevos billetes de Euro, desde su diseño hasta su distribución.

El *Counterfeit Intelligence Bureau* (CIB) lleva el Registro de Imágenes Holográficas de la IHMA. Creada en 1985 por la Cámara de Comercio

Internacional, esta organización representa y funciona como punto de convergencia de la industria contra el problemoo baa creciente de la falsificación. Para mayor información, puede visitarse http://www.iccwbo.org/index_ccs.asp.

Además, varios países ofrecen información técnica en línea sobre los documentos de viaje e identidad emitidos por sus autoridades competentes. Ese es el caso de Estonia, Lituania, los Países Bajos, el Pakistán, el Canadá y Suiza. Otros países ofrecen información jurídico (en su mayor parte en el idioma del país): por ejemplo, Italia, España y la India.

Además, Italia tiene un sitio de acceso público en Internet para comprobar los números de cheque en la base de datos de "documentos en blanco robados", así como los números de matrícula y de bastidor de vehículos robados. La República Checa tiene un sitio Web donde se pueden buscar documentos de identidad inválidos.

La Tabla 9-1 presenta un resumen de los sitios Web de instituciones internacionales y organismos públicos.

Canadá	www.ppt.gc.ca/passports/book_e.asp
República Checa	www.mvcr.cz/english.html
Banco Central Europeo	www.euro.ecb.int
Unión Europea	http://europa.eu.int./index_es.htm
Estonia	www.mig.ee/eng
OACI	www.icao.int/mrtd/home/index.cfm
India	www.passport.nic.en
Italia	http://coordinamento.mininterno.it/servpub/ver2/principale.htmwww.poliziadistato.it/
Lituania	www.dokumentai.lt
Países Bajos	www.identidaddocuments.nl
Pakistán	www.nadra.gov.pk
España	www.mir.es
Suiza	www.fedpol.ch/e/themen/index.htm

Tabla 9- 1: Instituciones internacionales y organismos públicos

9.1.2 Información comercial sobre documentos

En Internet hay mucha información disponible sobre productores y productos. Nuestra "visita virtual de los sitios Web" (véase la Tabla 9-2 más abajo) empieza por las empresas que fabrican documentos seguros o los integradores de sistemas. Recuerde que la selección del productor depende del documento seguro que se desea desarrollar, así como de los requisitos técnicos y los medios financieros, etc., como ya hemos mencionado.

La Tabla enumera asimismo las empresas que suministran componentes para documentos seguros como tintas, papel, dispositivos ópticamente variables, láminas protectoras, etc.

La información sobre los elementos de seguridad de los documentos también se puede comprar. *Keesing Reference Systems*, una empresa especializada en documentación de referencia, ofrece una base de datos que contiene imágenes y las descripciones correspondientes de documentos de identidad y billetes de banco auténticos y también de billetes falsos.

Por último, se incluye una lista de empresas especializadas en equipos de personalización.

Fabricantes	www.abncompany.com
	www.allaminyomda.com
	www.bundesdruckerei.de
	www.cbnco.com
	www.delarue.com
	www.fnmt.es
	www.gi-de.com (Gieseke+Devrient)
	www.goznak.ru
	www.imprimerienationale.fr
	www.incm.pt
	www.mirage-hs.si~
	www.oberthur.com
	www.ofs.ch
	www.sdu-identification.nl
	www.setec.fi (Gemalto)
	www.staatsdruckerei.at
	www.trueb.com

Proveedores	www.3m.com
	www.fasver.com
	www.gsi-gmbh.com
	www.hologram-industries.com
	www.infineon.com
	www.kinegram.com
	www.kurz.de
	www.landqart.com
	www.louisenthal.de
	www.luminescence.co.uk
	www.museodellacarta.com/ing/home_page.html
	www.nxp.com
	www.opsecsegurity.com
	www.segurity.arjowiggins.com
	www.sicpa.comwww.tumbabruk.se (Crane AB)
Sistemas de referencia	www.documentchecker.com (Keesing)
Equipos de personalización	www.datacard.com
	www.diletta.com
	www.iai.nl
	www.maurer-electronics.de
	www.muhlbauer.com
	www.secure.ps.de
	www.toppan.co.jp/english/index.html

Tabla 9- 2: Enlaces comerciales

9.1.3 Información específica sobre biometría

La biometría en los documentos de viaje ha sido un tema candente estos últimos años. Además de los de los fabricantes e integradores de sistemas, también hay sitios Web públicos sobre el tema. Una vez más, la selección siguiente no es más que una fracción de lo que puede ofrecer la red mundial.

Gobiernos	www.cesg.gov.uk/ www.engr.sjsu.edu/biometrics/index.htm www.itl.nist.gov/div895/biometrics/index.html
Varios	www.biometría.org, www.eubiometricforum.com

Tabla 9-3: Información relativa a la biometría

9.1.4 Conferencias y ferias

La forma más rápida de recabar información sobre productos, empresas y servicios consiste en visitar una exposición o participar en una conferencia. En todo el mundo se celebran encuentros que fomentan el diálogo entre organismos públicos y privados en la búsqueda de las mejores soluciones. La interacción entre los gobiernos y el sector de la seguridad se debería enfocar sobre todo como una alianza, en cuyo marco las partes se reúnen periódicamente y alcanzan decisiones que fomentan los desarrollos en el ámbito de los productos seguros.

Acontecimiento	**Tema**	**Frecuencia**	**Sitio Web**
Biometrics (Londres)	Biometría	Anual	www.biometrics.elsevier.com
CardTechSecureTech (CTST)	Tarjetas inteligentes, identificación, biometría, ICP	Anual	www.ctst.com
Cartes (París)	Tarjetas inteligentes, identificación, ICP, etc.	Anual	www.cartes.com
Cebit	TI, tarjetas	Anual	www.cebit.com
Conferencia SPIE sobre Seguridad Óptica y disuasión de la falsificación	Elementos de seguridad	Bienal	http://spie.org
Drupa	Sistemas de impresión	4-5 años	www.drupa.com
Intergraf	Impresión de alta seguridad	Bienal	www.intergraf.org
INTERPOL (*nota: la asistencia a las conferencias está reservada a los representantes de los gobiernos. Para mayor información, póngase en contacto con la Oficina Central de INTERPOL de su país)*	Billetes de banco y documentos de viaje fraudulentos	La conferencia mundial se celebra cada cuatro años. La europea es bienal	www.interpol.org
OACI	Documentos de lectura mecánica	Anual	Mrtd.icao.org

PISEC	Protección de marcas, elementos de seguridad	Bienal	www.pisec.com
Security Printing & Alternative Solutions in Central/Eastern Europe and Russia/ CIS	Impresión de seguridad	Anual	www.security-printing.com

Tabla 9-4: Conferencias y ferias

■ 9.2 Cooperación internacional

Los gobiernos están colaborando estrechamente entre sí para conseguir la normalización e interoperabilidad globales. Desde que se han considerado el terrorismo y la delincuencia organizada como las mayores amenazas contra el orden público, se han discutido extensamente y aceptado contramedidas a escala geográfica más amplia. Más concretamente, se trata de las relativas a:

- las normas de seguridad mínimas para los documentos de identidad y de viaje;
- la formación mínima que necesitan los funcionarios de inmigración y los funcionarios responsables de la expedición de documentos;
- el intercambio de planes de formación;
- los procedimientos relativos a la prevención y el apoyo a la investigación de documentos bancarios robados;
- los equipos mínimos necesarios en todos los puertos de entrada y puntos de expedición de documentos;
- el intercambio de funcionarios de inmigración;
- la adopción de normativas uniformes y armonizadas en materia de personalización de documentos, etc.

La cooperación internacional desempeña un papel importante en la elaboración de reglas, procedimientos y recomendaciones sobre los asuntos relacionados con los documentos seguros.

De hecho, existen numerosos foros creados con el propósito específico de debatir la cooperación internacional. Algunos foros se centran en los

aspectos técnicos de la producción de documentos, otros en la detección del fraude, y también se crean redes de intercambio de información (véanse las secciones 2.6.2, 2.6.3, 2.6.4).

En el marco de la Unión Europea se ha constituido el Grupo de Trabajo sobre documentos falsos llamado Comité Visa, y el Grupo de Trabajo sobre documentos falsos de Europol. Esos grupos de trabajo celebran varias reuniones anuales. En lo tocante a la comunidad internacional, figuran la Conferencia sobre Inmigración Fraudulenta (IFC), que agrupa a los países de Europa occidental y América del Norte; la Conferencia de Oficiales de Información sobre Inmigración del Pacífico (PacRim), que engloba a los países de Asia y Pacífico, la Conferencia Internacional del Mediterráneo Occidental (ICWM), que agrupa a los países meridionales de la UE junto con algunos países mediterráneos de África, y la Conferencia de Budapest, cuyos miembros son los países miembros de la UE y los Estados de Europa del Este.

Por último, está la Red Europea de Laboratorios e Institutos de Ciencias Forenses (ENFSI), que estudia la armonización de procedimientos en la comunidad internacional. También pretende conseguir la certificación de la experiencia técnica.

Sin embargo, sigue quedando espacio de intervención para las organizaciones de dimensión mundial. La INTERPOL, por ejemplo, utiliza un sistema de información basado en archivos de trabajo de análisis específicos, y da prioridad al intercambio de información a través de una red en la que participan todos sus miembros.

La cooperación internacional también puede desempeñar un cometido importante, al ayudar a los gobiernos a mejorar la seguridad e integridad de los documentos de viaje y de los documentos de identificación originales, de acuerdo con las normas internacionales.

La Organización Internacional para las Migraciones (OIM) es una organización intergubernamental que también asiste a los gobiernos a mejorar la legislación, las políticas, las estructuras administrativas, los

sistemas operativos y los recursos humanos necesarios para afrontar una serie de temas relacionados con la migración.

En el ámbito de los documentos de viaje y los sistemas de fronteras, la OIM, en calidad de proveedor de servicios imparcial, brinda apoyo a los países para la evaluación de los documentos y sistemas existentes, la planificación de especificaciones, la elaboración de pliegos de condiciones para los concursos públicos lanzados para la creación de dichos sistemas, y – en ocasiones – la gestión de la implantación de proyectos destinados a mejorar y/o actualizar tanto el sistema como el documento.

La OIM subscribe la opinión de que los documentos de viaje más seguros facilitan el control de los flujos transfronterizos (tanto legales como ilegales). A través de su Servicio de Cooperación Técnica sobre Migración, la OIM participa en todas las reuniones pertinentes, incluidas las reuniones de la OACI. La OIM no sólo apoya los empeños de la OACI por fomentar las normas de interoperabilidad para los documentos de lectura mecánica, sino que participa asimismo en las soluciones aportadas por el sector privado en este ámbito.

■ 9.3 Formación y calidad de la formación

La efectividad de los documentos se puede apreciar en el momento de su inspección, y ahí es donde intervienen los inspectores de documentos. Las organizaciones necesitan garantizar que esos funcionarios estén suficientemente informados sobre los nuevos avances y reciban una formación adecuada para mejorar sus resultados.

Habida cuenta del objetivo final, que no es otro que la seguridad, la eficiencia de un servicio o entidad será medido en función del nivel de eficiencia de cada persona involucrada, cuyos buenos resultados dependen en última instancia de que disponga de medios y de niveles de formación e información adecuados.

Figura 9-1: "Clase" del seminario sobre sustratos de polímeros en el marco del programa europeo ARGO, en el que, organizados por el *Serviço de Estrangeiros e Fronteiras* de Portugal, los profesores compartieron sus conocimientos con alumnos miembros de los servicios de policía e inmigración.

De acuerdo con la Organización Internacional del Trabajo (OIT), la "formación profesional es un proceso organizado de educación, gracias al cual las personas pueden ampliar sus conocimientos, desarrollar sus capacidades y mejorar sus actitudes y comportamientos, mejorando con ello sus calificaciones técnicas o profesionales, así como su participación en el desarrollo socioeconómico y cultural de la sociedad, en un proceso continuo para conseguir la realización y felicidad".

Por consiguiente, la formación de inspectores de documentos se debe considerar como un proceso continuo, y habrá de garantizarse no sólo que éstos dispongan de la pericia necesaria, sino que además sepan cómo aplicarla para mejorar la calidad del servicio que prestan y garantizar la seguridad.

Se puede representar en un diagrama esquemático (Figura 9-2):

Figura 9-2: Definición esquemática de formación según la OIT.

Desde este punto de vista, la formación es sin lugar a dudas una inversión, y no un gasto. La formación no sólo es más productiva, sino que además produce efectos sobre todo el sistema a corto, medio y largo plazo. Para comprender mejor este aspecto, es importante ser consciente de la misión y los objetivos de los servicios y fuerzas de seguridad responsables de la inspección de documentos. De ellos depende en última instancia el control de la seguridad y, más concretamente, la regulación de los flujos migratorios legales e ilegales, labor en la que los documentos asumen especial importancia.

Los recursos humanos y materiales son obviamente interdependientes por lo que a la eficiencia se refiere. Sin recursos humanos, los recursos materiales carecen de utilidad: no pueden funcionar ni volverse más eficientes por sí mismos. De forma similar, sin recursos materiales, los recursos humanos no pueden desempeñar las tareas que se les exigen constantemente en esta era de grandes soluciones tecnológicas.

La estrategia, la planificación, la estructura, el poder y la tecnología no bastan en los servicios de seguridad. Los funcionarios de seguridad también tienen que ser dinámicos, observadores, y estar bien preparados. Por ejemplo, tienen que saber transponer esas suposiciones para alcanzar la meta final del servicio, tomando debidamente en consideración todas las circunstancias externas.

A medida que cambian los tiempos, cambian asimismo las necesidades, las materias primas y los objetivos. Por consiguiente, las soluciones

se tienen que adaptar a las nuevas necesidades, en lugar de seguir centrándose en las antiguas. En el contexto del cambio de contingencias internacionales y globales, las organizaciones afrontan una demanda constante de mayor flexibilidad y de rápida adaptación de sus tareas y competencias para atender las nuevas necesidades.

La nueva política de gestión estratégica de los servicios insta a la adopción de mejores estrategias de seguridad. Renovarse y modernizarse es un reto que deben afrontar todas las partes que intervienen en los servicios. Por consiguiente, es importante invertir en la formación de los funcionarios de seguridad habida cuenta de los nuevos valores sociales y de los nuevos métodos y técnicas de intervención probados. También es necesario reducir al mínimo los riesgos resultantes de la falta de motivación y de la falta de reconocimiento de los resultados.

Sin embargo, con independencia de dónde se ponga el énfasis en la formación, también es importante centrarse ante todo en unos buenos procedimientos de contratación de funcionarios. Es sabido que no sólo es más fácil, sino mucho más eficiente formar a gente competente que motivar a una plantilla de bajo nivel. La contratación o reclutamiento de recursos humanos se debe basar en un estudio y evaluación en profundidad de las necesidades del servicio y de las tareas concretas de los funcionarios. Es tan importante identificar el perfil adecuado para el puesto como mantener bien al día a la plantilla existente a través de la formación.

La existencia de un nuevo modelo y un nuevo orden es una realidad, reforzada por el conocimiento y la información, que son los principales instrumentos que necesitan manejarse con la mayor habilidad. Quien sepa utilizarlos mejor tendrá la mayor ventaja competitiva. Esta idea de "ventaja competitiva", que se aplica a los mercados y empresas, ha sido reinventada por Porter, basándose en estudios de Igor Ansoff sobre el "valor" que cada organización es capaz de desarrollar y de añadir a su "actividad", generando de ese modo una cadena de valor.

Por lo que se refiere a la reestructuración orgánica, las autoridades de control y los servicios de inmigración en particular tienen que saber cómo elegir y tomar decisiones serias sobre su "valor añadido" en el contexto de sus conocimientos específicos y de su cultura institucional

particular, para desarrollar y modelar su propia "cadena de valor". Se trata de un proceso dinámico de búsqueda de la mejor "ventaja competitiva", que expone los posibles fallos derivados de la falta de profesionalidad.

El ciudadano se encuentra en el extremo receptor de este proceso complejo, junto con la entidad de servicio de seguridad privilegiada. Por tanto, tendrá que ser el ciudadano el que valore la calidad del servicio. En otras palabras, el producto debe satisfacer las necesidades del ciudadano en materia de seguridad. El producto dotado de esta calidad representa el valor de los servicios.

A este respecto, la aceptación pública desempeña un papel decisivo en el éxito final de todo el proceso. Las autoridades nacionales deben tener presente que ofrecer información y educación al público en general es la fundamental para conseguir el mejor resultado posible. La información sobre los documentos seguros debe ser objeto de una amplia difusión. Hay que prestar la atención debida a los aspectos de seguridad y a la relevancia jurídica de los documentos de identidad y de viaje, así como a las posibles consecuencias de su utilización indebida.

La forma más sencilla de hacerlo consiste en organizar una campaña que difunda la información más pertinente relativa a un documento. Esa campaña se debe concentrar en los elementos de seguridad de primera línea. La información debe ser precisa, y se debe transmitir en un lenguaje claro y sencillo, evitando estrictamente la jerga técnica. Siempre que sea posible, se debe completar con ilustraciones y diagramas que mejoren la claridad y la comprensión. Las autoridades nacionales también tienen la responsabilidad de velar por la actualización constante de la información. El criterio básico es que estar mal informado es mucho peor que no estar informado en absoluto!

En resumen, sólo la información concisa, precisa y puntual propicia la buena comunicación que, a su vez, mejora la interacción entre las autoridades responsables de la aplicación de la ley y la ciudadanía en general.

En última instancia, se conseguirá desarrollar una conciencia pública y la sensación de estar implicado, que permitirán una contribución espontánea y genuina a la seguridad.

Esta actitud edificante lleva al público general a sentirse más seguro y a confiar en el sistema. El ciudadano se sentirá animado a contribuir de forma más positiva y activa al éxito de todo el proceso que, con el tiempo, incluirá la lucha contra la delincuencia. Así, los ciudadanos informados ayudarán activamente a detectar el fraude. Pueden incluso anticipar e impedir el delito alertando a las autoridades competentes. Esa actitud animará a los ciudadanos a intervenir activamente en el conjunto del proceso de seguridad. El resultado será una demanda de más y mejor seguridad, lo cual, en última instancia, constituye el objetivo final de todo el mundo.

El ciudadano es el primero en evaluar la eficiencia de un documento diseñado para su seguridad. En primer lugar debe resultar práctico, tanto para el ciudadano que lo utiliza como para el funcionario de inspección que evalúa su autenticidad. En ello reside el mérito del servicio para ambas partes. Sin embargo, no hay que subestimar las crecientes exigencias tecnológicas que se afrontan tanto en el proceso de verificación de la autenticidad de un documento como en el proceso de concepción. Los servicios de inmigración y las autoridades de control deben mantenerse alerta para que no los supere la profesionalidad de los falsificadores y los impostores.

A tal efecto, se pueden adoptar las siguientes medidas para que desempeñen una función disuasoria o sirvan de contramedida en la lucha contra el fraude en los documentos:

- el intercambio de información sobre los medios y técnicas utilizados por los falsificadores;
- una supervisión concienzuda de la industria de los documentos seguros;
- mantener contactos periódicos con los fabricantes y proveedores de seguridad responsables de la producción del documentos;
- proporcionar equipos adecuados a los servicios encargados de la inspección de documentos.

En resumen, el diálogo constante entre las entidades públicas y privadas puede beneficiar a todas las partes interesadas.

Dependiendo de los niveles de control (controles de primera, segunda o tercera línea) y de la mayor o menor sofisticación de los equipos técnicos disponibles, los servicios también deben tener acceso a los manuales de referencia para su consulta. Evidentemente, tanto los equipos como las referencias se deben mantener actualizados para garantizar los mejores resultados posibles.

Esto mismo se aplica al público general. Para conseguir los mejores resultados, el ciudadano corriente tiene que tener acceso a una información clara y accesible, por ejemplo, en forma de folletos, prospectos, sitios Web, centros de atención nacionales y teléfonos de información pública. Los expertos en marketing saben cómo ofrecer las máximas posibilidades. Cuanto más precisa y eficiente sea la difusión de información, mayor credibilidad tendrá el sistema y mejor será la colaboración de los ciudadanos a la seguridad.

El ciudadano otorga una gran importancia a la confianza y credibilidad ofrecida por el sistema. Acatará los requisitos de buena gana, aunque eso suponga que lo interroguen o "molesten" con respecto a su identidad, si cree que con ello se protege su seguridad personal. Ese es uno de los factores más importantes para cualquier inspector en el ejercicio de su deber. Por ello, es fundamental que todo funcionario de inspección tenga el perfil adecuado y disponga de los conocimientos y competencias que el puesto requiere. El mejor enfoque consiste en contratar y preparar concienzudamente a los funcionarios, una labor que deben llevar a cabo tanto los cuadros medios, como los agentes de primera línea que reciben la formación. Su misión es hacerlo bien y con los medios apropiados que tienen a su disposición.

Por consiguiente, la inversión en formación continua y especializada es más que una necesidad: constituye todo un desafío. Los funcionarios de inmigración son los representantes y la conciencia nacional de los servicios de inmigración. Son responsables de la transparencia, y la garantía de que se está prestando un servicio de calidad de forma efectiva y eficiente.

9.3.1 Definición de la calidad de la formación

Si queremos aplicar esta idea a las autoridades de control, y en especial a los servicios de inmigración, podemos suponer que calidad significa "estar en conformidad con los requisitos de seguridad, que a su vez son acordes con las necesidades de los ciudadanos". Así pues, la idea de "calidad" se debe enfocar en el marco de un proceso integrado y exhaustivo en el que todos los servicios regionales, pese a su diseminación geográfica, tendrán que aplicar y observar las mismas normas de calidad. A este respecto, el funcionario de inmigración no sólo tiene que ser competente y estar informado, sino que además deberá ser consciente de los aspectos sociales de interés de la población para la cual trabaja.

9.3.2 Cómo mejorar la formación

Ampliar las capacidades de los funcionarios de inmigración debe ser una preocupación constante del sistema, pues lo cierto es que las instituciones tienen sistemas dinámicos, el cambio es ineludible y nada sigue siendo correcto, estable y uniforme indefinidamente.

Por lo tanto, la formación y la mejora profesional deben estimular al funcionario a seguir formándose, al tiempo que la institución sigue teniendo el deber de ofrecer formación a los funcionarios. Basándose en sus nuevas competencias profesionales y personales, los funcionarios deben mostrar una nueva actitud mental y conductual como consecuencia de una formación profesional basada en la filosofía de *saber, saber hacer, y saber estar*.

Sólo entonces habrá alcanzado un funcionario el entendimiento adecuado y la formación necesaria para prestar servicio y desempeñar su labor. Los conocimientos teóricos y prácticos adquiridos, y la capacidad de comprender y respaldar la causa, combinados con un sentido de la responsabilidad, permitirán que al funcionario logre automotivarse cuando trabaje en condiciones estresantes o difíciles.

Si los funcionarios del servicio de inmigración interesado en renovarse *saben estar*, no cabe duda de que estarán deseosos de aplicar las últimas

novedades tecnológicas, lo cual, a su vez, creará unas condiciones de trabajo que permitirán a los funcionarios automatizar los procesos, mejorando con ello la productividad y las tasas de respuesta.

Las autoridades de inspección, incluidos los servicios de inmigración, han realizado esfuerzos considerables, pero aún queda mucho por invertir para mejorar la calidad y alcanzar un mayor grado de desarrollo y motivación de los funcionarios de inmigración. Éste es un factor estratégico fundamental para el éxito de los servicios de inmigración y seguridad. La clave reside en la innovación en la gestión de los recursos humanos. Una buena gestión y prestación del servicio requiere una nueva mentalidad, comunidad de intereses y coordinación de los recursos humanos. Para empezar, esto supone destacar a la persona adecuada al lugar adecuado, o, como suele decirse, "zapatero a tus zapatos", teniendo en cuenta el nivel de conocimiento del empleado, sus preferencias y la satisfacción personal generada por la disposición a servir con disciplina, lealtad y adaptabilidad.

Los departamentos de formación, que desempeñan un papel importante en todas las etapas del proceso de calidad, colaboran en la búsqueda de las mejores soluciones. Junto con las partes responsables, se encargan de impartir los diversos tipos y niveles de formación, adaptados a las necesidades específicas tanto de los funcionarios como de los servicios de seguridad. Las diversas necesidades de formación se pueden satisfacer mediante la formación presencial, a distancia, o incluso el estudio personal.

Es importante que los diversos niveles de gestión reconozcan y apoyen la formación profesional de los inspectores, pues ésta es un requisito previo para que los servicios puedan funcionar eficazmente. En otras palabras, la formación se debería considerar obligatoria.

Pero cuando se trata de buscar las mejores soluciones, informar es tan importante como impartir formación. Hay que seleccionar concienzudamente a los destinatarios, y transmitir el mensaje de forma adecuada, es decir con objetividad, precisión y brevedad, en el momento oportuno. El mensaje debe destacar claramente los puntos

principales, y se debe difundir a través de los canales apropiados. De igual importancia es el intercambio de información entre entidades, la designación de puntos de contacto específicos y el filtrado de los casos o expedientes sospechosos, y el seguimiento de los mismos en el marco de la cooperación internacional.

La aceptación de un documento seguro determinado por parte del público en general, y la actitud de éste hacia el mismo, como, de hecho, hacia cualquier cuestión en general, depende de lo bien informado que esté el ciudadano corriente. Un público informado puede hacer una aportación positiva para mejorar los resultados generales del sistema, y contribuir con ello a la seguridad. La opinión pública varía de una nación a otra, y depende de diversos factores. La cultura, el desarrollo tecnológico y la historia de un colectivo determinado desembocan en actitudes distintas. Por lo general, una actitud determinada dura una generación, y su influencia puede ser perceptible sólo de medio a largo plazo. Por lo que se refiere a la aceptación de un documento seguro, la tolerancia del público a las nuevas tecnologías reviste una gran importancia. En la actualidad, los Estados tienen que centrar su atención y ser muy cautelosos en lo tocante a la petición de datos biométricos como medio de identificación. Aunque por una parte la biometría es la mejor respuesta a los últimos acontecimientos relacionados con la seguridad, por otra parte la biometría conlleva un nuevo concepto de seguridad y, por extensión, una nueva conciencia pública.

De hecho, el fomento de una relación de confianza entre un Estado y sus ciudadanos contribuye sin duda alguna a la aceptación de cualquier medida en este campo.

Por último, no debemos dejar de apreciar la importancia de los recursos humanos en el proceso general de la seguridad. Y es que son los funcionarios, y sólo ellos, quienes, guiados por un plan estratégico y operativo general, llevan a la práctica e imprimen dinamismo al proceso de seguridad. Son ellos los responsables del éxito o del fracaso de la institución. Citando a H. Mintzberg: “la estrategia no se planifica, sino que se construye”. Y el ser humano es la única especie que posee esas capacidades constructivas.

A partir de todo lo antedicho, podemos concluir que la formación puede generar las ventajas potenciales siguientes para el individuo o la institución:

Para el individuo:

- mayor motivación
- conocimientos específicos
- mejores competencias técnicas y capacidades de comunicación
- apertura al cambio
- capacidad de tomar decisiones
- confianza en sí mismo
- realización personal
- sentido de pertenencia a la institución
- sentido de progreso en el proceso de aprendizaje
- control de la tensión y el conflicto
- capacidad de superar la frustración

Para la institución:

- mejorar los resultados a todos los niveles
- incrementar la identificación con los objetivos de la institución
- aumentar la productividad
- mejorar el ambiente de la organización
- mejorar la motivación y los niveles de participación
- facilitar la comunicación y el control de conflictos
- contribuir a la mejora de la imagen de la institución.

Citando a *Formar* (1997) al respecto de la formación profesional de los trabajadores: "*el arma competitiva dominante en el siglo XXI será fundamentalmente la educación y las capacidades que haya adquirido la mano de obra*" (Lester Thurow).

Referencias

IEFP
1997 *Formar, Training magazine of the Employment and Professional Training Centre*, 29:4.
Morna Gomes, M.
1995 "*Estratégia e Planeamento na Gestão e Administração Pública*", ISCSP

ABREVIATURAS

AAMVA	*American Association of Motor Vehicle Administrators*
ABS	Acrilonitrilo butadieno estireno
ACP	Acuerdo sobre Contratación Pública
ADN	Ácido desoxirribonucleico
AFIS	Sistemas automáticos de identificación de huellas dactilares
BCE	Banco Central Europeo
CAO	Comunidad del África Oriental
CARICOM	Comunidad del Caribe
CBEFF	*Common Biometric Exchange File Format*
CEDEAO	Comunidad Económica de los Estados del África Occidental
CJIS	*Criminal Justice Information Services*
CTST	*CardTechSecureTech*
D2T2	Difusión de tinta por transferencia térmica
DEG	Derechos especiales de giro
DET	Compensación de errores de decisión
DVLM/MRTD	Documento de viaje de lectura mecánica
EEV	Expedición electrónica de visados
EFPWG	Grupo de trabajo europeo sobre huellas dactilares
ENFSI	Red Europea de Laboratorios e Institutos de Ciencias Forenses
FSAAWG	Grupo de trabajo de análisis forense auditivo y del habla

IBIS	*Interagency Border Inspection System*
ICP/PKI	Infraestructura de clave pública
ID	Identidad
ICT	*Information and Communication Technology*
ICWM	Conferencia Internacional del Mediterráneo Occidental
IFC	Conferencia sobre Inmigración Fraudulenta
IHMA	Asociación Internacional de Fabricantes de Hologramas
INSPASS	Sistema de servicio acelerado para pasajeros del Servicio de Inmigración y Naturalización de los Estados Unidos
IPS	Escuela de ciencias forenses
ISO	Organización Internacional de Normalización
JTC	Comité Técnico Conjunto
MERCOSUR	Mercado Común del Sur
MLI	Imagen múltiple a láser
Nd:YAG	Granate de itrio y aluminio dopado con neodimio Garnet (cristal)
NTWG	Grupo de trabajo sobre nuevas tecnologías
OACI	Organización de Aviación Civil Internacional
OCR	Reconocimiento óptico de caracteres
OIM	Organización Internacional para las Migraciones
OMC	Organización Mundial del Comercio
OIT	Organización Internacional del Trabajo
OVD	Dispositivos ópticamente variables
OVI	Tinta ópticamente variable
PDCA	Planificar-hacer-verificar-actuar
PVC	Cloruro de polivinilo
NIP/PIN	Número de identificación personal
RFC	*Request for Comments*
RFID	Identificación por radiofrecuencia
SC	Subcomité

SIA	Asociación suiza de ingenieros y arquitectos
TAG	Grupo consultivo técnico
TLI	*Tilted Laser Image*
UIMRTDWG	Grupo de Trabajo sobre la Implantación Universal de Documentos de Viaje de Lectura Mecánica
UV	Ultravioleta
WSQ	*Wavelet Scalar Quantization*
ZLM	Zona de lectura mecánica

Proteger la integridad de los documentos de identidad y de viaje se ha convertido en un problema cada vez más importante y complejo para los Estados. En particular, la cuestión de saber cómo invertir eficazmente en las tecnologías emergentes constituye un reto notable para numerosos países.

Además, resulta difícil encontrar publicaciones e información en el dominio público acerca de cómo desarrollar documentos de identidad seguros. Con el objetivo de colmar esta falta de información publica, dos especialistas en documentos de identidad - Diana Ombelli y Fons Knopjes – decidieron compilar y editar un libro sobre los métodos que permiten desarrollar documentos seguros. Trabajaron junto con numerosos expertos internacionales, quienes documentaron sus respectivos conocimientos y experiencias en esta misma publicación.

Este Manual para desarrolladores se propone dar una visión global de las problemáticas clave que se deben tener cuenta durante cada proceso de desarrollo de documentos de identidad. Entre otras cosas presenta a sus lectores la importancia de la infraestructura logística o de la cadena de seguridad, en la cual el fallo de un diminuto factor puede poner en peligro la integridad del documento de identidad.

Colaboradores

Nils Ångström
Antiguo experto en documentos en el "Swedish National Laboratory of Forensic Science", Linköping (Suecia)

Chuck Baggeroer
Antiguo director de la división "Tecnologías de Seguridad" del "Datacard Group", Minneapolis (Estados Unidos)

Isabel Baltazar
Directora de la unidad "Identidad y Fraude" del "Serviço de Estrangeiros e Fronteiras", Lisboa (Portugal)

Jan-Heim van Blankenstein y Mike Dell
Consultores y jefes de proyecto en temas de seguridad de la información, para "Montelbaan Internet & ICT BV", La Haya (Holanda)

Sjef Broekhaar
Especialista en temas de capacitación, formación y cooperación técnica, Organización Internacional para las Migraciones (OIM), Manila (Filipinas)

Cor Buursma y Paul Ponsioention
Antiguos jefes de proyecto para Sdu Identification", Haarlem (Holanda)

Birgit Cardell
Directora del "Documents Department" en el "Swedish National Laboratory of Forensic Science", Linköping (Suecia)

Charles Chatwin
Consultor en temas de impresión de seguridad e identificación, antiguo director de la impresora de seguridad "De La Rue", Basingstoke (Reino Unido)

Idius Felix
Consultor para "Atos Origin", Utrecht (Holanda)

Daniele Graber
Consejero legal en la "Swiss Society of Engineers and Architects" (SIA), Zurich (Suiza)

Piet Lakeman
Administrador en temas de riesgo de fraude,"Visa International", Bruselas (Bélgica)

Didier Meuwly
Experto forense en el "National Forensic Institute", Ypenburg (Holanda)

Tommy Nordberg
Vicepresidente de "Gemalto", Vantaa (Finlandia)

Diana Ombelli
Jefe de proyecto en "Sdu Identification", Haarlem, (Holanda)

Ineke Ruiter y Fons Knopjes
Directores del "ID Management Centre", La Haya (Holanda)

Jim Wayman
Director del "Biometric Test Centre" del Instituto de ingeniería de la Universidad de Estado de San José, San José (Estados Unidos)

OIM Organización Internacional para las Migraciones