OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Parte 2: Especificaciones para la seguridad del diseño, la fabricación y la expedición de MRTD

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Parte 2: Especificaciones para la seguridad del diseño, la fabricación y la expedición de MRTD

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

Publicado por separado en español, árabe, chino, francés, inglés y ruso
por la ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL
999 Robert-Bourassa Boulevard, Montreal, Quebec, Canadá H3C 5H7

En el sitio web www.icao.int/security/mrtd pueden obtenerse descargas
e información adicional

Doc 9303, *Documentos de viaje de lectura mecánica*
Parte 2 — *Especificaciones para la seguridad del diseño, la fabricación y la expedición de MRTD*
ISBN 978-92-9265-508-2 (versión impresa)

© OACI 2021

Reservados todos los derechos. No está permitida la reproducción de ninguna parte de esta publicación, ni su tratamiento informático, ni su transmisión, de ninguna forma ni por ningún medio, sin la autorización previa y por escrito de la Organización de Aviación Civil Internacional.

ENMIENDAS

La publicación de enmiendas se anuncia periódicamente en los suplementos del *Catálogo de productos y servicios*; el Catálogo y sus suplementos pueden consultarse en el sitio web de la OACI: www.icao.int. Las casillas en blanco facilitan la anotación de estas enmiendas.

REGISTRO DE ENMIENDAS Y CORRIGENDAS

ENMIENDAS		
Núm.	Fecha	Anotada por

CORRIGENDAS		
Núm.	Fecha	Anotado por

Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican, de parte de la OACI, juicio alguno sobre la condición jurídica de ninguno de los países, territorios, ciudades o áreas, o de sus autoridades, ni respecto a la delimitación de sus fronteras o límites.

ÍNDICE

Página

1. ALCANCE

En esta parte se proporcionan especificaciones obligatorias y opcionales que han de adoptar las autoridades expedidoras de documentos de viaje para asegurar que sus MRTD, y los medios de personalización y expedición a las personas titulares legítimas, están protegidos contra acciones fraudulentas. También se proporcionan especificaciones obligatorias y opcionales para la seguridad física que ha de brindarse en los locales donde se producen, personalizan y expiden los MRTD así como la inspección y control del personal que participa en tales operaciones.

El aumento mundial del número de personas que viajan y el crecimiento continuo previsto, conjuntamente con el incremento de la delincuencia internacional, el terrorismo y la inmigración ilegal han agudizado la preocupación por la seguridad de los documentos de viaje e impone formular recomendaciones sobre lo que podría hacerse para mejorar su resistencia a las adulteraciones o a un uso indebido. En el pasado, en el Doc 9303 no se han hecho recomendaciones acerca de los elementos de seguridad específicos que han de incorporarse en los documentos de viaje. Cada Estado expedidor ha tenido la libertad de incorporar las medidas de seguridad que haya considerado apropiadas para proteger sus documentos de viaje nacionales contra imitaciones fraudulentas, falsificaciones y otras formas de adulteración, a condición de no incluir nada que pudiera afectar negativamente su lectura mecánica OCR.

Para satisfacer la necesidad de aumentar la seguridad de los documentos, los asesores técnicos de la OACI decidieron que sería conveniente publicar un conjunto de “normas mínimas de seguridad recomendadas” como orientación para todos los Estados que expidan documentos de viaje de lectura mecánica. Así pues,

- el Apéndice A contiene orientaciones sobre el fortalecimiento de la seguridad de los documentos de viaje de lectura mecánica;
- el Apéndice B contiene recomendaciones que abarcan la autenticación mecánica de los elementos de seguridad del documento;
- el Apéndice C describe las medidas de seguridad que han de adoptarse para garantizar la seguridad de las operaciones de personalización y de los documentos en tránsito;
- el Apéndice D describe los riesgos de fraude relacionados con el proceso de solicitud y expedición de MRTD.

2. SEGURIDAD DEL MRTD Y SU EXPEDICIÓN

Antes de la expedición de un documento de viaje, el establecimiento de la persona titular y del derecho a un documento de viaje se hará en consonancia con la *Guía del TRIP de la OACI sobre las pruebas de identidad* [EOI de la OACI], disponible en la siguiente dirección: https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

El MRTD, y su método de expedición, se diseñarán para incorporar garantías de protección del documento contra acciones fraudulentas durante su período de validez. Los métodos y las acciones fraudulentas pueden clasificarse como sigue:

- *Falsificación.* Creación de la totalidad o parte de un documento que se asemeja al MRTD genuino con la intención de utilizarlo como si fuera genuino. También pueden producirse falsificaciones al tratar de duplicar o simular el método genuino de fabricación y los materiales usados en el mismo o mediante técnicas de copia;
- *Alteración fraudulenta.* Como su mismo nombre indica, se trata de la alteración de un documento genuino para permitir su uso en viajes de una persona no autorizada o hacia un destino no autorizado. Los detalles personales de la persona titular genuina en particular el retrato son el primer objetivo de tal alteración;

- *Impostores*. Se define “Impostor” como “persona que asume la identidad de otra persona”. Deberían incorporarse elementos de seguridad para facilitar la detección visual o automática del uso fraudulento del MRTD por un impostor;

- *Suplantación de identidad*. Falsear la dirección del remitente de una transmisión para entrar ilegalmente a un sistema seguro.

  Nota.— La suplantación, el enmascaramiento, el acceso sin autorización (piggybacking) y la imitación, entre otros, son formas de suplantación de identidad.

- *Transformación de imagen (morphing)*. Es la técnica de manipulación de una imagen en la que se transforman o funden los rostros de dos o más personas para obtener un solo rostro en una fotografía.

Existen métodos establecidos para proporcionar seguridad contra los tipos de acciones fraudulentas mencionados. Estos entrañan el uso de materiales que no están fácilmente al alcance del público, combinado en sistemas de diseño altamente especializados y procesos de fabricación que requieren equipos y conocimientos especiales. En el Apéndice A de esta parte se detallan algunas de las técnicas disponibles actualmente para proporcionar seguridad a los MRTD y permitir que los funcionarios de inspección detecten un documento de imitación o falsificado, ya sea por medios visuales o utilizando equipos sencillos como lupas o lámparas ultravioleta.

Todos los MRTD que se ajusten al Doc 9303 utilizarán los elementos básicos de seguridad indicados en la Tabla A-1 del Apéndice A.

3. VERIFICACIÓN DEL DOCUMENTO CON AYUDA DE MÁQUINA

En el ámbito de la autenticación de los documentos de viaje de lectura mecánica (MRTD) con ayuda de máquina, se han hecho progresos considerables a lo largo del último decenio. Las innovaciones técnicas hechas en el diseño de seguridad de los MRTD y en el desarrollo de los sistemas de autenticación (lectores, soporte lógico, etc.) han permitido que la autenticación de los documentos basada en las máquinas se convierta en parte integrante de varias infraestructuras y procesos de control (p. ej., el control fronterizo).

No obstante, a las personas expertas en documentos, fabricantes y autoridades de ese ámbito se les plantean nuevos desafíos a medida que, gracias a las mejoras técnicas, se logran una mayor seguridad y eficiencia en los procesos operacionales. Algunos de los principales desafíos son la falta de armonización y normalización de los procesos establecidos, así como la falta de coordinación entre las principales partes intervinientes en esos procesos, que llevan a que las partes y componentes de los sistemas se desarrollen de forma independiente, sin prestar consideración a las importantes consecuencias resultantes de su interacción. Además, la complejidad y diversidad de los sistemas actualmente disponibles en el mercado hacen especialmente difícil que se puedan evaluar y/o comparar.

En esta sección se proporciona asesoramiento sobre la autenticación con ayuda de máquina de los elementos de seguridad incorporados en los MRTD con arreglo a las especificaciones establecidas en el Doc 9303. El Apéndice A de esta Parte y las normas de seguridad recomendadas en el mismo constituyen la base para las consideraciones de esta sección. El Apéndice B contiene recomendaciones que abarcan la verificación por máquina de esas normas de seguridad (sobre la base de los materiales, la impresión de seguridad y las técnicas de protección frente a las copias) mediante el uso de la capacidad de los lectores de documentos para la adquisición de imágenes de alta resolución en la gama espectral visual, infrarroja y ultravioleta. Por último, el Apéndice C presenta una serie de recomendaciones de mejores prácticas para las principales partes que participan en el diseño, implementación y funcionamiento de los sistemas de autenticación mecánica y los componentes clave.

La meta que persiguen las recomendaciones de esta sección es mejorar la seguridad de los documentos de viaje de lectura mecánica en todo el mundo mediante el uso de procedimientos de verificación de documentos con ayuda de máquina que se ajusten completamente a:

- el diseño de los documentos de viaje de lectura mecánica según se especifica en el Doc 9303 manteniendo la retrocompatibilidad;
- los elementos de seguridad recomendados en el Apéndice A de esta Parte; y
- la utilización de las capacidades técnicas de los lectores avanzados instalados en todo el mundo para hacer lugar a los eMRTD, según se recomienda en los Apéndices B y C de esta Parte.

No obstante, cada Estado debe llevar a cabo una evaluación de riesgos de los elementos de autenticación de documentos con ayuda de máquina en sus fronteras para identificar los aspectos más beneficiosos y minimizar los riesgos. En el Doc 9303 no se especifica ningún elemento como medio de verificación de documentos con ayuda de máquina de interfuncionamiento mundial, dado que el uso de un único elemento en todo el mundo lo haría altamente vulnerable a acciones fraudulentas. Por consiguiente, para minimizar los riesgos los Estados deberían aplicar varios elementos de seguridad.

3.1 Tipos de elementos

Existen tres categorías principales de elementos de seguridad verificables por máquina. Estas se describen a continuación junto con ejemplos concretos de dichos elementos de seguridad que pueden verificarse por máquina.

3.1.1 Elemento estructura

Un elemento estructura entraña la incorporación de una estructura medible en o sobre la página de datos del MRTD. Se trata de un elemento de seguridad que contiene algún tipo de información verificable sobre la base de la construcción física del elemento, por ejemplo:

- la característica de interferencia de un holograma u otro dispositivo ópticamente variable que pueda ser identificado sin ambigüedad por un lector adecuado;
- imágenes retroreflectantes empotradas en un laminado de seguridad; y
- transmisión controlada de la luz a través de determinadas áreas del sustrato.

3.1.2 Elemento sustancia

Un elemento sustancia entraña la incorporación en el MRTD de un material que normalmente no estaría presente y que no está obviamente presente en la inspección visual. La presencia del material puede detectarse mediante la presencia y magnitud de una propiedad adecuada de la sustancia añadida. Esto entraña la identificación de un elemento definido de una sustancia utilizada en la construcción del elemento, por ejemplo:

- uso de pigmentos, normalmente en tintas, que responden de maneras específicas e inusuales a longitudes de ondas específicas de la luz (que pueden incluir luz infrarroja o ultravioleta) o tienen propiedades magnéticas o electromagnéticas; y
- la incorporación en un componente de la página de datos de materiales, por ejemplo, fibras cuyo tamaño individual o distribución de tamaño se ajustan a una especificación predeterminada.

3.1.3 Elemento datos

La imagen visible de la página de datos del MRTD puede contener información oculta que puede detectarse mediante un dispositivo adecuado incorporado al lector. La información oculta puede estar en la imagen impresa de seguridad pero en general se incorpora a los datos de personalización, especialmente el retrato.

La inserción de la información oculta en la página de datos del MRTD puede entrañar la aplicación de elementos sustancia o estructura para lograr varios niveles de seguridad. En este contexto, el término esteganografía describe una clase especial de elementos de datos ordinariamente en forma de información digital que se esconde dentro de una imagen, por lo general el retrato de personalización o la impresión de seguridad del fondo. La información puede descifrarse mediante un dispositivo adecuado incorporado en un lector de página completa calibrado para buscar el elemento en un lugar determinado. La información podría ser, por ejemplo, el número de documento. El lector puede programarse para comparar el número de documento detectado en el elemento con el número de documento que aparece en la ZLM. Dicha comparación no involucra el acceso a los datos almacenados en el CI sin contacto de un eMRTD. Los elementos de este tipo pueden ser:

- datos codificados almacenados en el documento en medios magnéticos tales como los hilos de seguridad especiales; y
- diseños que incorporan los datos ocultos que solo resultan detectables cuando se les mira a longitudes de onda de luz específicas, con filtros ópticos o mediante un soporte lógico de procesamiento de imágenes específico.

En formas más complejas el volumen de datos almacenados puede ser considerable y éstos pueden verificarse mediante comparación electrónica con datos almacenados en el CI sin contacto del eMRTD.

3.2 Principios básicos

Los tres tipos de elemento, estructura, sustancia y datos, pueden incorporarse en los documentos de viaje y verificarse con lectores adecuadamente diseñados. Actualmente se dispone de lectores que pueden detectar tales elementos y utilizan las respuestas para confirmar la autenticidad del documento. El Apéndice B se concentra en los elementos que pueden verificarse mediante equipo de detección incorporado al lector de MRTD y utilizarse durante el proceso de lectura normal.

La verificación de la seguridad del documento con ayuda de máquina utiliza tecnología automática de inspección para ayudar a verificar la autenticidad de un documento de viaje. No debería utilizarse aisladamente para determinar la prueba de identidad, pero cuando se le utiliza en combinación con elementos variables de seguridad del documento, esta tecnología proporciona al examinador una poderosa nueva herramienta para ayudar a la verificación de documentos de viaje.

Los elementos de verificación de la seguridad de documentos con ayuda de máquina son elementos de seguridad opcionales que pueden incluirse en el MRTD a discreción de la autoridad expedidora.

Los elementos verificables por máquina pueden variar en tamaño desde menos de 1mm (0.04 in) cuadrado hasta la totalidad del área del documento. En la figura 1 se proporciona orientación sobre los lugares que estos datos deberían ocupar en la página de datos del MRTD para facilitar el interfuncionamiento. Para mantener la retrocompatibilidad, se recomienda introducir los elementos de autenticación por máquina en los lugares y áreas indicados.

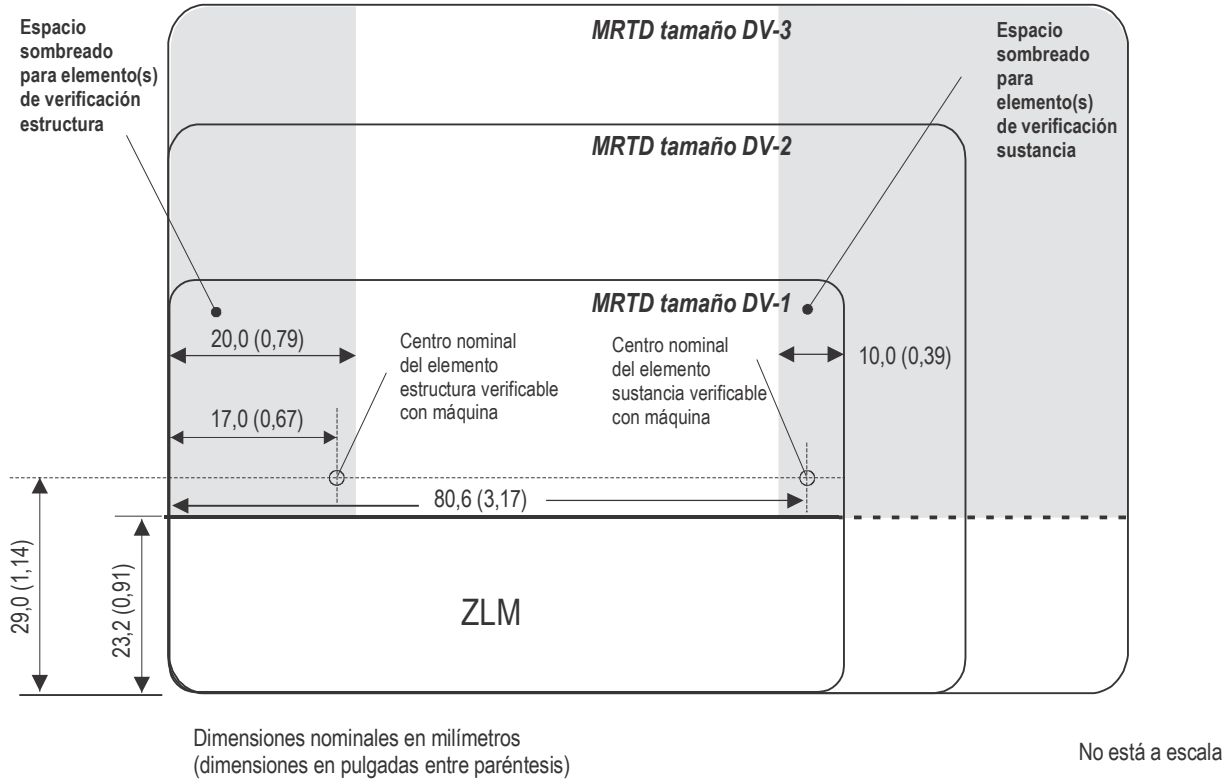

Figura 1. Este diagrama muestra los tres tamaños de MRTD, incluyendo el MRP (tamaño DV3), con la colocación recomendada de los elementos para verificación del documento con ayuda de máquina. El área sombreada de la izquierda se recomienda para la incorporación del elemento estructura y la de la derecha para la incorporación del elemento sustancia.

3.3 Autenticación por máquina y eMRTD

El uso de un CI sin contacto que se ajuste plenamente a las especificaciones en un eMRTD ofrece excelentes oportunidades para la autenticación por máquina. No obstante, dicha autenticación utilizando CI sin contacto no tendrá éxito si:

- el CI sin contacto es defectuoso y no logra comunicarse; o
- no se dispone de certificados para verificar la autenticidad e integridad de los datos en el CI sin contacto.

Por consiguiente, se necesita una autenticación por máquina alternativa. Esto es especialmente pertinente en las situaciones de control fronterizo automatizado (ABC) donde se utiliza un lector de documentos en vez de un funcionario de control fronterizo para leer y validar el eMRTD. En cuanto alternativa fiable, la autenticación óptica mecánica establece confianza en los datos utilizados para la adopción de decisiones en la frontera.

Un CI sin contacto en buen funcionamiento en un eMRTD también puede contribuir a la autenticación óptica mecánica almacenando los elementos de esa autenticación óptica y sus coordenadas en los grupos de datos (DG) pertinentes.

4. SEGURIDAD DE LAS INSTALACIONES DE PRODUCCIÓN (DISEÑO Y FABRICACIÓN) Y EXPEDICIÓN DE MRTD

El Estado que expida el MRTD se cerciorará de que los locales en los que se imprime, encuaderna, personaliza y expide el MRTD son adecuadamente seguros y de que las personas que trabajan en ellos cuentan con una autorización de seguridad apropiada. También se proporcionará seguridad apropiada para los MRTD en tránsito entre instalaciones y desde la instalación a la persona titular del MRTD. En el Apéndice C se proporcionan recomendaciones sobre las formas de satisfacer estos requisitos.

Los factores siguientes deberían tenerse en cuenta en el establecimiento de instalaciones de producción y expedición:

1) resiliencia;

2) seguridad física y control de accesos;

3) materiales de producción y contabilización de MRTD;

4) transporte;

5) personal; y

6) ciberseguridad.

4.1 Resiliencia

Los Estados deberían adoptar medidas adecuadas para cerciorarse de que la producción de MRTD puede mantenerse en caso de situaciones de desastre como inundaciones, incendios y falla de equipo. Algunas consideraciones a tener en cuenta son:

- uso de instalaciones de producción y expedición distribuidas;
- sitios de producción secundarios cuando la producción está centralizada;
- instalaciones de expedición de emergencia;
- rápido acceso a respuestas y apoyo técnico;
- uso de segundas fuentes para todos los componentes de MRTD.

Se recomienda que los Estados consideren posibles modos de falla en el diseño de instalaciones de producción y expedición, con objeto de eliminar fallas comunes y puntos de falla únicos.

4.2 Seguridad física y control de acceso

Los Estados deberían controlar el acceso a las instalaciones de producción y expedición. El control debería ejercerse sobre zonas y los requisitos para el acceso a cada zona deberían ser conmensurables con el valor de los bienes que se protegen.

Algunos ejemplos de buena práctica para instalaciones de producción son:

- enjaulado de alambre o paredes sólidas para segregar áreas de producción;
- cámaras acorazadas para el almacenamiento de MRTD terminados pero no personalizados y componentes de seguridad clave para la producción de MRTD;
- control de acceso de seguridad con contraseña entre zonas;
- vigilancia vídeo dentro y fuera de la instalación;
- seguridad perimetral;
- personal de seguridad a tiempo completo.

Los Estados también deberían considerar la seguridad aplicada en organizaciones que proporcionan componentes de MRTD a la instalación de producción porque el robo o la venta de tales documentos podría facilitar la falsificación de un MRTD.

Las instalaciones de expedición deberían separar las zonas de oficina de las zonas públicas, con control de acceso entre ambas. El personal debería contar con protección adecuada, según lo determinan las circunstancias locales.

4.3 Contabilización de los materiales de producción

Los Estados deberían cerciorarse de que todos los materiales empleados en la producción de MRTD son contabilizados y que la producción de MRTD corresponde con los pedidos de esos documentos, de modo que pueda demostrarse que no faltan MRTD o componentes de MRTD.

Los materiales defectuosos, MRTD y componentes de MRTD deberían destruirse en forma segura y contabilizarse.

En general, la reducción del número de sitios de expedición y producción hace más fácil la contabilización de los materiales. No obstante, esto debe equilibrarse con respecto a la necesidad de proporcionar resiliencia y un servicio a la clientela aceptable.

4.4 Transporte

Se aconseja a los Estados a que apliquen métodos seguros para transportar los MRTD y los componentes de esos documentos; normalmente, el uso de empresas de transporte de fondos resulta adecuado a menos que se transporten activos físicos o bienes de alto valor (p. ej., patrones holográficos).

Los Estados deberían procurar minimizar la cantidad de materiales transportados en un solo envío para reducir el efecto de los robos. En particular, los Estados no deberían transportar juegos completos de planchas de impresión en una sola operación.

4.5 Personal

Los Estados deberían asegurar que todo el personal está sujeto a un proceso de autorización de seguridad, que confirma su identidad y adecuación para el empleo en un entorno en que se producen activos de alto valor. El personal debería contar con credenciales que los permitan identificarse y obtener acceso a las áreas protegidas cuando necesitan ingresar en las mismas en ejercicio de sus funciones.

4.6 Ciberseguridad

Las instalaciones de producción y expedición son vulnerables a varios tipos de ciberataques, a saber:

1) virus y otros programas maliciosos (malware), tanto en las instalaciones informáticas convencionales como en la maquinaria de producción;

2) ataques de denegación de servicio a través de canales de aplicación MRTD en línea y servicios de red expuestos por los sistemas de producción y expedición;

3) puesta en peligro de los sistemas de expedición para permitir a los atacantes expedir pasaportes o robar datos personales o activos criptográficos (p. ej., claves privadas para la producción de eMRTD).

Las contramedidas que pueden aplicarse frente a estos ataques y ataques conexos trascienden el alcance del presente documento. Los Estados deberían procurar asesoramiento de sus autoridades técnicas nacionales.

5. SUMINISTRO DE INFORMACIÓN SOBRE MRTD RECIENTEMENTE EXPEDIDOS

Se recomienda que el Estado que introduzca el nuevo diseño de MRTD informe a los otros Estados sobre los detalles del nuevo MRTD, incluyendo los elementos de seguridad evidentes, preferiblemente mediante especímenes personalizados para utilizar como referencia en el departamento del Estado receptor encargado de verificar la autenticidad de los documentos. La distribución de tales especímenes debería dirigirse a puntos de contacto establecidos y convenidos por los Estados receptores.

6. SUMINISTRO DE INFORMACIÓN SOBRE MRTD EXTRAVIADOS Y ROBADOS

El intercambio de información sobre documentos de viaje extraviados, robados o revocados constituye una estrategia clave para fortalecer el control fronterizo y mitigar los impactos del robo de identidad y el fraude de inmigración. Por consiguiente, los Estados deberían considerar la implantación de los siguientes procedimientos operacionales para enfrentar las amenazas que apuntan a socavar la gestión fronteriza y la seguridad pública nacional:

1. comunicar activamente con las personas titulares de los documentos;

2. mantener bases de datos nacionales de documentos de viaje extraviados, robados y revocados;

3. compartir con INTERPOL la información sobre documentos extraviados, robados y revocados y verificar sistemáticamente los documentos respecto de las bases de datos de INTERPOL en la inspección primaria;

4. instalar verificaciones para determinar si una persona titular está presentando un documento extraviado, robado o revocado en un cruce fronterizo.

6.1 Comunicación activa con las personas titulares de los documentos

Los Estados deberían cerciorarse de que las personas titulares de los documentos de viaje son plenamente conscientes de sus responsabilidades con respecto al uso, custodia y procedimientos de notificación para documentos de viaje extraviados o robados. Las directrices para la custodia o conservación de documentos de viaje tanto en el hogar o durante los viajes pueden contribuir a prevenir la pérdida o robo de los documentos de viaje. En el momento que las personas titulares reciben sus documentos, se les debería informar con respecto a las medidas apropiadas (incluyendo la notificación oportuna) y los canales para notificar el extravío o robo de los documentos. Para ayudar en este proceso, los Estados podrían considerar la facilitación a las personas titulares de documentos de viaje de múltiples canales para notificar en condiciones de seguridad el extravío y el robo de los documentos, incluyendo la comunicación telefónica, el correo físico y las diversas formas de comunicación electrónica, incluso por Internet.

Los Estados también deben adoptar medidas apropiadas para asegurar que las personas titulares de documentos de viaje tienen buen conocimiento de las posibles interrupciones, inconvenientes y gastos añadidos que puedan surgir cuando se presentan documentos extraviados, robados o revocados en el control fronterizo para fines de viaje. Este asesoramiento debería hacer hincapié en que una vez que se haya notificado el extravío o robo de un documento de viaje, dicho documento se cancela y no puede continuar utilizándose y puede ser confiscado por las autoridades si se trata de hacerlo.

Debería contarse con legislación nacional o cualquier otro marco adecuado para obligar a las personas titulares de documentos de viaje a que notifiquen inmediatamente el extravío o la pérdida de un documento de viaje. Hasta no haberse presentado dicho informe no debería expedirse ningún documento de viaje nuevo.

6.2 Mantenimiento de bases de datos nacionales de documentos de viaje extraviados, robados y revocados

Los Estados que emplean bases de datos nacionales sobre documentos de viaje para ayudar a verificar el estado o condición de sus documentos de viaje de expedición nacional deberían adoptar medidas para cerciorarse de que la información se mantiene actualizada. Los informes sobre documentos extraviados y robados proporcionados por las personas titulares deberían registrarse en dichos sistemas en forma oportuna para asegurar que las evaluaciones de riesgo llevadas a cabo utilizando estos sistemas son exactas. Los Estados también podrían considerar el registro en esta base de datos de información sobre interceptaciones de documentos de viaje extraviados, robados o revocados. Además de actualizar estas bases de datos, los Estados deberían asegurarse de que las autoridades policiales y de control fronterizo pueden acceder a las mismas con facilidad.

6.3 Compartición de información con INTERPOL sobre documentos de viaje extraviados, robados y revocados y verificación de dichos documentos con respecto a las bases de datos de INTERPOL en forma sistemática en la inspección primaria

Los Estados deberían participar en el intercambio mundial de información oportuna y exacta relativa al estado o condición de los documentos de viaje para ayudar a la vigilancia dentro del país y a la gestión fronteriza, así como las actividades para mitigar las consecuencias del robo de identidad. La compartición de información sobre documentos de viaje extraviados, robados y revocados contribuye a:

a) mejorar la integridad de la gestión y control de fronteras;

b) ayudar a detectar el robo de identidad o el fraude de inmigración en la frontera o en otras situaciones en que se presente el documento como forma de identificación;

c) mejorar las posibilidades de identificar agentes terroristas que viajan con documentos falsos;

d) mejorar las posibilidades de identificar actividades delictivas, incluyendo el contrabando de personas;

e) ayudar en la recuperación de documentos nacionales; y

f) limitar el valor y el uso con fines ilícitos de documentos extraviados, robados o revocados.

El servicio de búsqueda automática (ASF)/base de datos sobre documentos de viaje robados y perdidos (SLTD) de INTERPOL proporciona a los Estados un medio para compartir eficaz y eficientemente información sobre documentos de viaje extraviados, robados y revocados en forma oportuna. Los Estados deberían compartir la información sobre documentos extraviados y robados que se hayan expedido, así como sobre documentos en blanco que hayan sido robados de una instalación de producción o expedición o durante el tránsito. En el Apéndice D se esbozan los factores que deben considerarse antes de participar en la ASF/SLTD.

Los Estados deberían verificar los documentos con respecto a las bases de datos de INTERPOL en forma sistemática en la inspección primaria para asegurar que solamente cruzan los puestos de control fronterizos viajeros con documentos de viaje válidos. La verificación del estado de los documentos de viaje con respecto a estas bases de datos ofrece muchas de las mismas ventajas que se logran compartiendo información sobre documentos extraviados, robados y revocados.

6.4 Instalación de verificaciones para determinar si una persona titular presenta un documento extraviado,robado o revocado en un cruce fronterizo

Los Estados deben actuar dentro de las leyes nacionales existentes y respetar los acuerdos internacionales sobre el uso de documentos de viaje y control fronterizo al procesar viajeros en sus fronteras. Todos los viajeros con documentos de viaje cuyo extravío, robo o revocación se haya notificado serán tratados como si no existiera intención ilícita, hasta que se demuestre lo contrario.

6.4.1 Cuando un documento de viaje aparece en la base de datos sobre documentos extraviados, robados o revocados de INTERPOL

No debería denegarse la entrada a un país o impedirse su salida a un viajero sobre la sola base de que su documento figure en la base de datos de documentos de viaje extraviados, robados o revocados. Los Estados deben realizar varios pasos para apoyar estas medidas. Si un viajero está en posesión de un documento de viaje que haya sido registrado como extraviado, robado o revocado en la ASF/SLTD, los Estados deberían, siempre que sea posible, comunicarse con el país expedidor y notificador para confirmar que el documento ha sido registrado correctamente como documento de viaje extraviado, robado o revocado. Los Estados también deberían entrevistar a la persona que viaja para establecer su identidad o nacionalidad verdadera y determinar si es la persona titular legítima del documento de viaje.

Si el documento contiene una microplaqueta, los Estados deberían realizar verificaciones biométricas en apoyo de sus actividades para determinar la verdadera identidad del viajero. Los Estados también deberían hacer lo posible por determinar si los datos han sido alterados y si el documento es auténtico.

6.4.2 Procesamiento de la persona titular legítima del documento de viaje en el puesto de control fronterizo

Al tratar con las personas titulares legítimas de documentos de viaje, los Estados deberían saber que las personas identificadas como personas titulares legítimas de un documento de viaje que se haya declarado como extraviado, robado o revocado no estarían necesariamente tratando de cometer un delito. En vez de concentrarse en penalizar a estos individuos, los Estados deberían concentrarse en determinadas formas de sacar de circulación dichos documentos, minimizando la interrupción del viaje. Cuando la legislación nacional lo permita, los Estados pueden considerar al tratar a estos viajeros métodos distintos de los que se apliquen a las personas que intencionalmente intentan ingresar en forma ilícita al país cometiendo fraude de la identidad.

Viajeros que ingresan a un país extranjero con un documento que se haya declarado como extraviado, robado o revocado como resultado de un error en los datos	El control fronterizo del Estado receptor debería comunicarse con la autoridad expedidora para confirmar el error de los datos. Una vez confirmado éste, los Estados pueden procesar el documento como documento de viaje válido, pero deberían aconsejar a la persona viajera que se comunique con la autoridad expedidora al regresar a su país. Las autoridades expedidoras de documentos de viaje en el Estado expedidor deberían adoptar todas las medidas necesarias para que dicho documento se elimine de la base de datos de documentos extraviados, robados y revocados. Los Estados también deberían considerar la sustitución del documento en cuestión sin cargo para la persona titular.
Ciudadanos que intentan salir de su país con un documento declarado como extraviado o robado	Cuando existen controles de salida, el control fronterizo debería comunicar a estos viajeros que sus documentos no son válidos para viajar y que deben obtener un documento de viaje válido antes de emprender el viaje, puesto que los documentos extraviados, robados y revocados no se consideran válidos.
Ciudadanos que intentan salir de su país con un documento revocado	Cuando existan controles de salida, el control fronterizo debería consultar a las autoridades policiales nacionales para determinar las medidas o leyes que pueden invocarse para impedir que el viajero abandone el país. Si dichas disposiciones lo permiten, las autoridades de control fronterizo o policiales deberían impedir que los viajeros abandonen el Estado.
Ciudadanos que intentan salir de un país y regresar al suyo con un documento declarado como extraviado, robado o revocado	Cuando existen controles de salida y se haya confirmado la identidad y nacionalidad de la persona titular, el control fronterizo puede permitir que la persona continúe su viaje, pero debería comunicarle que el documento presentado no es válido y que el transportista puede denegarle el embarque. Cuando una persona está reingresando a su país de origen con un documento declarado como extraviado, robado o revocado, el control fronterizo puede, cuando así lo permita la legislación nacional o acuerdos internacionales, decomisar y confiscar el documento para devolverlo al expedidor. Si sus documentos han sido decomisados o confiscados, debería comunicarse a los viajeros que procuren obtener nuevos documentos de viaje válidos.
Ciudadanos que intentan salir de un país extranjero y continuar hacia un tercer país con un documento declarado como extraviado, robado o revocado	Cuando existan controles de salida, el control fronterizo debería comunicar a los viajeros que sus documentos de viaje no son válidos, que el transportista puede denegar su embarque y que pueden enfrentar dificultades a la llegada a su siguiente destino.
Viajeros que ingresan a un país extranjero con un documento declarado como extraviado, robado o revocado	El Estado receptor debería aconsejar a los viajeros cuyo embarque se haya permitido a que se comuniquen con su consulado o embajada para obtener un documento de viaje válido antes de intentar la continuación de su viaje. Los viajeros cuyo ingreso haya sido denegado serán tratados con arreglo a la ley nacional.

6.4.3 Tratamiento de una persona que viaja después de haberse determinado que no es la persona titular legítima de un documento declarado como extraviado, robado o revocado

Una vez que se haya determinado que una persona viajera no es la persona titular legítima de un documento, las autoridades fronterizas o policiales del Estado expedidor o receptor deberían tratar de determinar la forma en que el viajero obtuvo el documento, incluyendo si existió colusión con la persona titular legítima y, si la ley nacional lo permite, cooperar con el Estado del expedidor para determinar si se han expedido otros documentos fraudulentos con la misma identidad. Si se determina que la persona viajera ha presentado un documento de viaje extraviado, robado o revocado, los Estados deberían investigar a la persona y, si corresponde, entablarle un proceso penal o deportarlo del país.

Los Estados deberían confiscar los documentos para fines de procedimientos legales, incluyendo trámites de inmigración y de refugiados, pero deberían devolverlos al Estado expedidor una vez que hayan cumplido su finalidad. También debería tratarse de proporcionar al expedidor tanta información como sea posible sobre la interceptación en cuestión, si la ley nacional lo permite.

Los Estados también deberían asegurarse de que las personas no admisibles están debidamente documentadas con arreglo a las disposiciones del Anexo 9 — *Facilitación* al Convenio sobre Aviación Civil Internacional.

7. REFERENCIAS (NORMATIVAS)

Ciertas disposiciones de las normas internacionales, a las que se hace referencia en este texto, constituyen disposiciones del Doc 9303. Cuando existan diferencias entre las especificaciones del Doc 9303 y las normas de referencia, a efectos de tener en cuenta los requisitos específicos de la realización de documentos de viaje de lectura mecánica, incluidos los visados de lectura mecánica, prevalecerán las especificaciones contenidas en el presente texto.

Anexo 9 — *Facilitación*, del Convenio sobre Aviación Civil Internacional (el “Convenio de Chicago”).

[EOI de la OACI] *Guía del TRIP de la OACI sobre las pruebas de identidad*, disponible en la siguiente dirección: https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

— — — — — — — —

APÉNDICE A DE LA PARTE 2 — NORMAS DE SEGURIDAD PARA LOS MRTD (INFORMATIVO)

A.1 ALCANCE

El presente apéndice contiene orientaciones sobre el fortalecimiento de la seguridad de los documentos de viaje de lectura mecánica producidos conforme a las especificaciones establecidas en el Doc 9303. Las recomendaciones abarcan la seguridad de los materiales empleados para crear los documentos, los métodos de impresión de seguridad y de protección contra las copias que han de utilizarse y los procesos que se aplican en la producción de documentos en blanco. También se tratan las cuestiones de seguridad que se aplican a la personalización y producción de los datos personales en el documento. Todas las autoridades expedidoras de documentos deberán tomar en consideración este apéndice.

A.2 IntroducCIÓN

En este apéndice se señalan los peligros a los que frecuentemente están expuestos los documentos de viaje y las medidas que pueden aplicarse para proteger dichos documentos y sus sistemas de personalización conexos. Las listas de elementos y técnicas de seguridad que ofrecen protección contra estos peligros se han subdividido en: 1) elementos y técnicas de seguridad básicos que se consideran esenciales y; 2) otros elementos y técnicas que se presentan a los Estados para alentarlos a que seleccionen algunos de los aspectos recomendados para lograr un mayor grado de seguridad.

Con este enfoque se reconoce que un elemento o técnica que puede necesitarse para proteger los documentos de un Estado determinado puede resultar innecesario o ser de menor importancia para otro Estado que use sistemas de producción diferentes. Por consiguiente, se prefiere una solución que permite a los Estados elegir entre diferentes tipos de documentos (a base de papel, tarjetas de plástico, etc.) y una combinación de elementos y técnicas de seguridad apropiados a sus necesidades particulares, en lugar de “la misma solución para todos”. No obstante, para asegurarse en elegir un conjunto equilibrado de elementos y técnicas de seguridad, cada Estado debe evaluar los riesgos a que están expuestos sus documentos nacionales de viaje para identificar cuáles son los aspectos de mayor vulnerabilidad y seleccionar los elementos y técnicas complementarios más idóneos para solucionar sus problemas específicos.

La finalidad de las recomendaciones de este apéndice es mejorar la seguridad de los documentos de viaje de lectura mecánica en todo el mundo mediante el establecimiento de un modelo básico para los Estados expedidores. Nada de lo que aquí se recomiende impedirá ni será óbice para que los Estados apliquen otros elementos de seguridad más avanzados, si así lo desean, para alcanzar una norma de seguridad que supere los elementos y técnicas mínimos recomendados que se establecen en el presente apéndice.

Se incluye también una tabla que presenta un resumen de los peligros que característicamente amenazan la seguridad y los documentos de viaje y algunos de los elementos y técnicas de seguridad que pueden ayudar a ofrecer protección contra estos peligros.

A.3 PRINCIPIOS BÁSICOS

La producción y almacenamiento de las libretas de pasaporte y de documentos de viaje, incluidos los procesos de personalización, debe llevarse a cabo en un ambiente seguro y controlado que cuente con las medidas de seguridad apropiadas para impedir el acceso no autorizado a las instalaciones. Si los procesos de personalización están

descentralizados, o si se efectúan en un lugar geográfico apartado del lugar donde se producen los documentos en blanco, deberán tomarse las precauciones necesarias cuando se transporten los documentos en blanco y otros materiales de seguridad conexos con el propósito de garantizar la seguridad de los mismos durante su traslado y almacenamiento a la llegada. Durante el traslado, las libretas en blanco y otros documentos de viaje deberían contener el número de documento unívoco. En el caso de los pasaportes, el número del pasaporte debería figurar en todas las páginas salvo en la página de datos personales, donde puede imprimirse durante la personalización.

Debería asumirse plena responsabilidad por todos los materiales de seguridad empleados en la producción de documentos de viaje tanto válidos como estropeados y, en cada etapa del proceso de producción, deberá hacerse una conciliación completa con los registros que se lleven para dar cuenta de todos los materiales de seguridad que hayan sido usados. La pista de auditoría deberá ser lo suficientemente detallada como para dar razón de cada unidad de material de seguridad empleada en la producción y deberá auditarse en forma independiente por personas que no intervengan directamente en la producción. Conviene mantener registros certificados a nivel de supervisión para asegurar que ha dado cuenta de la destrucción de todo el material de seguridad desechado y de los documentos estropeados.

Los materiales empleados en la producción de documentos de viaje deben ser de variedades controladas y, cuando corresponda, obtenerse exclusivamente de proveedores de materiales de seguridad auténticos. Conviene usar materiales destinados sólo a aplicaciones de alta seguridad y evitar materiales que el público general puede conseguir en el mercado abierto.

Debería evitarse depender exclusivamente del uso de paquetes de soporte lógico accesibles al público para originar los fondos de seguridad. No obstante, dichos paquetes de soporte lógico pueden usarse en combinación con soporte lógico especializado para diseños de seguridad.

En los documentos de viaje deberán incorporarse elementos de seguridad y aplicarse métodos de seguridad que sirvan de protección contra reproducciones y alteraciones no autorizadas y otras formas de modificación fraudulenta, incluida la eliminación y sustitución de páginas de la libreta de pasaporte, especialmente de las que contienen datos personales. Además de incluir esos elementos para proteger los documentos en blanco del peligro de falsificación, hay que procurar, en especial, que los datos personales no puedan eliminarse o alterarse. En un documento de viaje deberán incluirse elementos de seguridad y aplicarse técnicas de seguridad en forma apropiada para hacer patente cualquier intento de alteración fraudulenta.

Se debería elegir bien la combinación de elementos, materiales y técnicas de seguridad de manera que sean compatibles entre sí y protejan el documento durante su vida útil.

Si bien este apéndice trata principalmente de los elementos de seguridad que contribuyen a proteger los documentos de viaje contra falsificaciones y alteraciones fraudulentas, existe otra clave de elementos de seguridad (elementos de nivel 3) integrados por elementos ocultos (secretos) ideados de manera que su autenticación sólo pueda hacerse mediante examen forense o por expertos empleando equipos de verificación especiales. Es evidente que el conocimiento exacto de la sustancia y la estructura de esos elementos debe restringirse a muy pocas personas, es decir "a los que necesitan saberlo". Entre otras cosas, una finalidad de estos elementos es posibilitar la autenticación del documento cuando se requiera prueba inequívoca de su autenticidad (por ejemplo, en los tribunales). Todo documento de viaje debe incluir por lo menos un elemento oculto de seguridad como elemento básico.

En el Anexo 9 — *Facilitación* de la OACI figuran importantes normas generales y métodos recomendados relativos al período de validez de los pasaportes, el principio de pasaportes individuales para cada persona, los plazos para la expedición de pasaportes de lectura mecánica y la retirada de circulación de pasaportes que no son MRP así como otras orientaciones conexas.

No existen para el interfuncionamiento mundial otros medios aceptables de almacenamiento de datos que no sean los CI sin contacto, especificados por la OACI como tecnología de ampliación de capacidad para uso con MRTD.

A.4 PRINCIPALES PELIGROS PARA LA SEGURIDAD DE LOS DOCUMENTOS DE VIAJE

La siguiente lista de peligros para la seguridad de los documentos no sigue ningún orden de importancia en particular y señala las formas en que los documentos, la expedición y uso de los mismos pueden ser objeto de actos fraudulentos:

- falsificación de todo el documento de viaje;
- sustitución de la fotografía;
- supresión o alteración del texto en la zona visual o de lectura mecánica de la página de datos del MRP;
- construcción de un documento fraudulento, o de partes del mismo, empleando materiales de otros documentos legítimos;
- extracción y sustitución de páginas enteras o visados;
- supresión de anotaciones en las páginas de visados y en la página de observaciones;
- robo de documentos genuinos en blanco;
- impostores (que asumen la identidad de la persona titular, alterando la apariencia); y
- manipulación indebida del CI sin contacto (cuando exista), sea por medios físicos o electrónicos.

La detección de los elementos de seguridad puede darse en cualquiera o en la totalidad de los siguientes tres niveles de inspección:

- Nivel 1 – Examen superficial para la inspección rápida en el punto de uso (elementos visuales o táctiles fácilmente identificables);
- Nivel 2 – Examen por inspectores capacitados con equipo sencillo; y
- Nivel 3 – Inspección por especialistas forenses.

Para mantener la seguridad e integridad de los documentos, deberían realizarse exámenes periódicos y cualesquiera revisiones necesarias del diseño del documento. Esto permitirá la incorporación de nuevas medidas de seguridad del documento y certificar la capacidad de éste para resistir situaciones de peligro e intentos de fraude con respecto a:

- sustitución de la fotografía;
- delaminación u otros efectos de deconstrucción;
- ingeniería inversa del CI sin contacto así como de otros componentes;
- modificación de cualquier elemento de datos;
- borrado o modificación de otra información;
- duplicación, reproducción o creación de facsímile;
- eficacia de los elementos de seguridad en los tres niveles: examen superficial, examinadores capacitados con equipo sencillo e inspección por especialistas forenses; y
- confianza y facilidad de la identificación de segundo nivel.

Para proteger los documentos de estos y otros peligros, es esencial que se aplique una gama de elementos y técnicas de seguridad combinados de manera óptima dentro del documento. Aunque algunos elementos pueden proteger contra más de un tipo de peligro, no hay ningún elemento que por sí solo pueda ofrecer protección contra todos ellos. Análogamente, ningún elemento de seguridad es 100% eficaz en eliminar una categoría determinada de peligro. La mejor protección es un conjunto equilibrado de elementos y técnicas que proporcione capas múltiples de seguridad integradas en el documento y que se combine para disuadir o impedir cualquier intento de acto fraudulento.

A.5 ELEMENTOS Y TÉCNICAS DE SEGURIDAD

En las secciones que siguen, los elementos, técnicas y otras medidas de seguridad se clasifican según las etapas de los procesos de producción y personalización y según los componentes de los documentos de viaje que se crearon mediante dichos procesos con respecto a:

1) materiales del sustrato;

2) diseño e impresión de seguridad;

3) protección contra las copias, falsificaciones o alteraciones fraudulentas; y

4) técnicas de personalización.

Se recomienda a los Estados expedidores que incorporen todos los elementos o medidas de seguridad básicos y que, se puede evaluar a fondo los riesgos a los que están expuestos los documentos de viaje, seleccionen de la lista varios elementos y medidas de seguridad adicionales. A menos que se indique otra cosa, puede suponerse que los elementos de seguridad se aplican a todas y a cada una de las partes de un documento de viaje, incluyendo la cubierta y la encuadernación de la libreta así como todas las páginas interiores de un pasaporte, incluida la página de datos personales, las últimas hojas y las páginas de los visados. Hay que asegurarse de que los elementos no interfieran en la lectura mecánica del documento de viaje.

A.5.1 Materiales del sustrato

A.5.1.1 Papel empleado en las páginas de un documento de viaje

Elementos básicos:

- papel opaco a la luz ultravioleta, o un sustrato con una respuesta controlada a la luz UV de manera que al ser iluminado con ella aparezca una fluorescencia distinguible en color de la luminiscencia azul-blanca que se usa en los materiales fluorescentes con blanqueadores ópticos que pueden conseguirse comúnmente;

- filigrana en dos o más niveles de gris en la página de datos personales y en las páginas de visados;

- sensibilizadores químicos apropiados en el papel, o por lo menos en la página de datos personales (si esto es compatible con la técnica de personalización); y

- papel con absorbencia, rugosidad y resistencia superficial al rasgado.

Otros elementos:

- filigrana en el registro con diseño impreso;
- en la página de datos, una filigrana diferente a la utilizada en las páginas de visado para impedir la sustitución de páginas;
- filigrana de molde cilíndrico;
- fibras o planchetes fluorescentes invisibles;
- fibras o planchetes (fluorescentes) visibles;
- hilo de seguridad (incrustado o hilo ventana) con elementos de seguridad adicionales como microimpresión y fluorescencia;
- compuesto marcador diseñado para la detección por equipo especial; y
- elemento de seguridad perforado con láser.

A.5.1.2 Papel u otro sustrato en forma de etiqueta empleado en la página de datos personales de un documento de viaje

Elementos básicos:

- papel opaco a la luz ultravioleta, o un sustrato con una respuesta controlada a la luz UV de manera que al ser iluminado con ella aparezca una fluorescencia distinguible en color de la luminiscencia azul-blanca que se usa en los materiales fluorescentes con blanqueadores ópticos que pueden conseguirse comúnmente;
- sensibilizadores químicos apropiados en el papel (normalmente no es posible en sustrato de etiqueta plástica);
- fibras fluorescentes invisibles;
- fibras fluorescentes visibles; y
- un sistema de adhesivos u otros elementos que imposibiliten el desprendimiento de la etiqueta sin causar un daño visible a la misma o a los laminados o recubrimientos que se utilicen con ella.

Otros elementos:

- hilo de seguridad (incrustado o en ventana) con elementos de seguridad adicionales como micro impresión y fluorescencia;
- puede incorporarse una filigrana al papel de una página de datos en forma de etiqueta de papel;
- elemento de seguridad perforado con láser; y
- patrón de seguridad troquelado dentro de la etiqueta para determinar si hubo manipulación indebida.

A.5.1.3 Aspectos de seguridad del papel empleado en el reverso de la cubierta de la libreta del pasaporte

No es necesario que el papel empleado en el reverso de la cubierta de la libreta de pasaporte tenga una filigrana. Aunque definitivamente no se recomienda, si se utiliza como página de datos personales (véase A.5.5.1), se deberán emplear otras medidas alternativas para lograr un nivel de seguridad frente a todo tipo de ataque equivalente al que proporciona el emplazamiento de la página de datos en una hoja interior.

Cuando el reverso de la cubierta se utilice como página de datos personales, conviene que el papel que constituye el reverso de la cubierta contenga sensibilizadores químicos apropiados. El papel sensibilizado químicamente debería ser compatible con el método de personalización y el adhesivo empleado para adherir el papel final al material de la cubierta del pasaporte.

A.5.1.4 Sustratos sintéticos

Cuando el sustrato empleado en la página de datos personales (o etiqueta insertada) de una libreta de pasaporte o de una tarjeta MRTD esté hecho todo de plástico o de una variación de plástico, generalmente no es posible incorporar muchos de los elementos de seguridad que se describen en 5.1.1 a 5.1.3. En tales casos, se incluirán otros componentes de seguridad, como elementos de seguridad impresos adicionales, técnicas de personalización perfeccionadas o uso de elementos ópticamente variables además de los que se recomiendan en 5.2 a 5.5.2. De preferencia, los Estados deberían asegurar que el sustrato plástico se fabrica en condiciones controladas y contiene propiedades específicas, p. ej., fluorescencia controlada para diferenciarlo de los sustratos estándar para tarjetas bancarias.

Elementos básicos:

- la construcción de la página de datos debería ser resistente a la separación física en capas;
- sustrato opaco a la luz ultravioleta con una respuesta controlada a dicha radiación de modo que al ser iluminado con ella aparezca una fluorescencia distinguible en color de la luminiscencia azul-blanca que se usa en los materiales fluorescentes que pueden conseguirse comúnmente;
- deberían aplicarse medidas apropiadas para incorporar la página de datos en condiciones de seguridad y durabilidad en el documento de viaje de lectura mecánica; y
- elemento ópticamente variable.

Otras características:

- característica de ventana transparente;
- elemento táctil; y
- perforación con láser.

A.5.2 Impresión de seguridad

A.5.2.1 Fondo e impresión del texto

Elementos básicos (véase 9303-1, 4.2 — Términos y definiciones):

- diseño con fondo de seguridad Guilloche a dos tintas [1];
- impresión arco iris;
- texto microimpreso; y
- fondo de seguridad en la página de datos personales impreso con un diseño diferente al de las páginas de visado o de las otras páginas del documento.

Otros elementos:

- impresión calcográfica (intaglio) sencilla o multicolor que incluya un diseño de “líneas negras y blancas” en una o más de las últimas páginas o en las páginas de visados;
- imagen latente (calcografía);
- patrón antiescáner;
- diseño doble de seguridad;
- diseño (tridimensional) en relieve;
- elemento de registro anverso-reverso (transparente);
- error intencional (por ejemplo, de ortografía);
- todas las páginas de visados impresas con un diseño de fondo de seguridad diferente;
- elemento táctil; y
- tipos de letra especiales.

A.5.2.2 Tintas

Elementos básicos:

- tinta fluorescente UV (visible o invisible) en la página de datos personales y en todas las páginas de visados; y
- tinta reactiva, cuando el sustrato de las páginas del documento o de una etiqueta sea de papel, por lo menos en la página de datos personales (de ser compatible con el método de personalización).

1. Cuando el patrón de Guilloche se cree mediante computadora, la imagen que aparezca en el documento ha de ser de tal calidad que no sea posible detectar la estructura de los elementos de imagen. Las líneas de Guilloche pueden mostrarse como imágenes positivas donde sus líneas aparezcan con espacios en blanco entre sí, o bien como imágenes negativas con las líneas en blanco y los espacios entre ellas impresos. Los diseños de Guilloche a dos tintas se crean mediante la sobreimpresión de dos elementos del patrón de Guilloche que se reproducen en colores que contrastan.

Otros elementos:

- tinta con propiedades ópticamente variables;
- tinta metálica;
- tinta de numeración penetrante;
- tinta metamérica;
- tinta invisible en la región infrarroja;
- tinta infrarroja absorbente;
- tinta fosforescente;
- tinta marcada; y
- tinta invisible con fluorescencia en diferentes colores cuando se la expone a diferentes longitudes de onda.

A.5.2.3 Numeración

Se recomienda encarecidamente utilizar el número de documento único como número de pasaporte.

Elementos básicos:

- el número de pasaporte debería aparecer en todas las hojas del documento y en la página de datos personales del mismo;
- en un documento, el número debe aparecer impreso o perforado;
- el número de documento en la etiqueta tendrá un estilo especial de cifras o tipos de letra y se imprimirá con una tinta que sea fluorescente bajo luz ultravioleta, además de tener un color visible;
- el número en la página de datos de un pasaporte hecho de sustrato sintético o en una tarjeta de MRTD puede incorporarse utilizando la misma técnica que la empleada para aplicar los datos personales en el proceso de personalización; y
- en las tarjetas MRTD, el número debería aparecer en ambos lados.

Otros elementos:

- si hay perforación, es preferible utilizar la perforación con láser. La numeración perforada en la página de datos es opcional, pero, en caso de que se utilice, debería tenerse cuidado de no interferir en la claridad del retrato o la ZIV ni obstruir en forma alguna la ZLM. Es conveniente perforar la cubierta del pasaporte; y
- si se imprime, debería tener idealmente un estilo o tipo especial e imprimirse con una tinta que sea fluorescente bajo la luz ultravioleta, además de tener un color visible.

A.5.2.4 Medidas especiales de seguridad para uso con páginas no laminadas de datos personales

La superficie de la página de datos debería protegerse contra la suciedad producida por el uso normal, incluyendo la lectura mecánica ordinaria de la ZLM, así como contra la manipulación indebida.

Si una página de un documento donde se pongan los datos personales no está protegida por un laminado o un recubrimiento protector (véase 5.3.2, 5.4.3 y 5.4.4), se protegerá además mediante la impresión calcográfica incorporando una imagen latente y microtexto utilizando, de preferencia, una tinta de color cambiante (p. ej., tinta con propiedades ópticamente variables).

A.5.2.5 Medidas especiales de seguridad para uso con tarjetas y páginas de datos personales de plástico

Cuando un documento de viaje está hecho completamente de plástico, se añadirán características de seguridad ópticamente variables que cambien de apariencia según el ángulo de observación. Estos recursos pueden incorporarse en forma de imágenes latentes, elementos lenticulares, tintas de color cambiante o difractivas o imágenes ópticamente variables.

A.5.3 Protección contra las copias

A.5.3.1 Necesidad de una protección contra las copias

El perfeccionamiento alcanzado hasta ahora por las técnicas de reproducción digital disponibles al público y las consiguientes posibilidades de fraude obligan a incorporar características de alta seguridad en forma de elementos ópticamente variables u otros equivalentes para protegerse contra la copia y el escaneo. Debe reforzarse la seguridad de la página de datos personales de las libretas de pasaporte, tarjetas de viaje o visados, empleando una tecnología de elementos independientes, complejos y ópticamente variables y otros componentes equivalentes que complementen otras técnicas de seguridad. Debería hacerse especial hincapié en los elementos visuales o táctiles fácilmente identificables que se examinan en la inspección de nivel 1.

La incorporación apropiada de elementos ópticamente variables u otros componentes equivalentes en los estratos de la página de datos personales ha de servir, también, para impedir que los datos sean alterados fraudulentamente. Asimismo, hay que proteger contra imitaciones fraudulentas los elementos ópticamente variables en todos los materiales de seguridad conexos que se emplean para crear la estructura de los estratos.

A.5.3.2 Métodos de protección contra las copias

Con sujeción a las recomendaciones mínimas descritas en 5.4.3 y 5.4.4 sobre la importancia del laminado, se deben incorporar elementos ópticamente variables en la página de datos personales de las libretas de pasaporte, tarjetas de viaje o visados como *elemento básico*.

Cuando la página de datos personales de una libreta de pasaporte, tarjeta de viaje o visado esté protegida por una película de laminado o un recubrimiento, deberá integrarse en la página un elemento ópticamente variable (preferentemente basado en una estructura difractiva con propiedades que pongan en evidencia la manipulación indebida). Dicho elemento no debe afectar a la legibilidad de los datos anotados.

Cuando la página de datos personales es una etiqueta de papel encapsulada, o una página en un pasaporte, los datos personales deben estar adecuadamente protegidos mediante un laminado o mediante medidas que proporcionen una seguridad equivalente a efectos de disuadir alternaciones o eliminaciones.

Cuando la página de datos personales de lectura mecánica de una libreta pasaporte esté hecha totalmente de sustrato sintético debería incorporarse un elemento ópticamente variable. Se recomienda incluir un elemento ópticamente variable difractivo para lograr un mayor nivel de protección contra las reproducciones.

En lugar de un elemento ópticamente variable pueden utilizarse dispositivos como las ventanas transparentes, la perforación con láser y otros elementos que se considera ofrecen protección equivalente.

Cuando el documento de viaje no tiene protección por recubrimiento o laminado se empleará un elemento ópticamente variable (preferentemente basado en una estructura difractiva) con una sobre impresión calcográfica u otra técnica de impresión.

A.5.4 Técnica de personalización

A.5.4.1 Personalización de documentos

Esto se refiere al proceso de incorporar en el documento de viaje el retrato, la firma y otros datos personales de la persona titular. Estos son los datos de la persona titular y son los que corren mayor riesgo de falsificación o alteración fraudulenta, ya que uno de los casos más frecuentes de fraude con documentos es el desprendimiento y sustitución del retrato en un documento robado u obtenido ilegalmente por el de otra persona. Los documentos con un retrato pegado son particularmente susceptibles a los cambios de fotografía. Por lo tanto, NO se permite en los MRTD la colocación de fotografías pegadas.

A.5.4.2 Protección contra alteraciones

Para asegurar que los datos estén debidamente protegidos contra intentos de falsificación o alteración fraudulenta, se recomienda muy encarecidamente integrar al material básico del documento los datos personales, el retrato, la firma (si está incluida en la página de datos personales) y los datos principales respecto a la expedición del documento. Hay una variedad de tecnologías para la personalización del documento de esta forma, sin excluir el surgimiento de nuevas tecnologías; entre ellas figuran las siguientes sin ningún orden particular de importancia:

- impresión con tóner láser;
- impresión por transparencia térmica;
- impresión por chorro de tinta;
- proceso fotográfico; y
- grabado láser.

También pueden usarse las mismas tecnologías de personalización para incorporar datos a las páginas de observaciones del pasaporte. El tóner láser no debería utilizarse para personalizar visados u otros documentos de seguridad que no estén protegidos por un laminado seguro.

Las autoridades deberían realizar ensayos de sus procesos y técnicas de personalización para provocar su eficacia contra actos ilícitos.

A.5.4.3 Elección de la tecnología para crear el documento

La elección de una tecnología en particular es algo que debe decidir cada Estado expedidor ya que esto dependerá de varios factores, como el volumen de producción de documentos de viaje, la construcción del documento y el momento en que se proceda a la incorporación de los datos personales, o sea durante la fabricación del documento o de la libreta de pasaporte o después de que esté terminado y de si el país expide pasaportes en forma centralizada o desde lugares descentralizados.

Independientemente del método que se elija, es esencial tomar precauciones para proteger los elementos personalizados contra alteraciones fraudulentas. Esto es importante pues, si bien eliminar el uso de retratos pegados reduce el riesgo de sustitución de la fotografía, los datos personales no protegidos siguen siendo vulnerables a las alteraciones y es preciso que se protejan mediante la aplicación de un laminado con sellado térmico (o equivalente) con propiedades frangibles, o tecnología equivalente que proporcione pruebas de manipulación indebida.

A.5.4.4 Protección contra la sustitución de la fotografía y la alteración de los datos de la página de datos personales de las libretas de pasaporte

Elementos básicos:

- personalización del retrato y de todos los datos personales integrándolos en el material básico;
- el fondo de seguridad impreso (p. ej., Guilloche) se fundirá dentro del área del retrato;
- uso de tinta reactiva y sensibilizadores químicos en el papel;
- un dispositivo de seguridad visible debería superponerse al retrato sin obstruir la visibilidad de éste; para ello se recomienda un elemento ópticamente variable; y
- uso de un laminado de seguridad con sellado térmico (o equivalente) o la combinación de tecnología de personalización y material de sustrato que proporcione una resistencia equivalente a la sustitución o alteración fraudulenta del retrato y otros datos personales.

Otros elementos:

- la firma presentada de la persona titular puede escanearse e incorporarse a la impresión;
- imágenes esteganográficas incorporadas al documento;
- imagen secundaria del retrato de la persona titular;
- elementos susceptibles de verificación mecánica según se detalla en el Doc 9303, Partes 9 a 12.

A.5.5 Otras medidas de seguridad para las libretas de pasaporte

A.5.5.1 Colocación de la página de datos personales

Se recomienda que los Estados coloquen la página de datos en una de las páginas interiores (segunda o penúltima página). Cuando la página de datos está situada en el reverso de la cubierta del MRP, el método normal de construcción utilizado en la fabricación de cubiertas de pasaporte ha facilitado las acciones fraudulentas en la página de datos,

normalmente la sustitución de la fotografía o la sustitución de una página completa. No obstante, el Estado expedidor puede colocar la página de datos sobre una cubierta siempre que asegure que la construcción de la cubierta utilizada en su pasaporte ofrece un nivel de seguridad similar contra todos los tipos de acciones fraudulentas al ofrecido cuando se coloca la página de datos en una página interior. No obstante, NO se recomienda colocar la página de datos sobre la cubierta.

A.5.5.2 Sustitución de una página completa

Cabe señalar a los Estados expedidores que, al reemplazar las fotografías pegadas en los pasaportes por páginas de datos personales integradas, se ha observado que en algunos casos la página entera de datos personales del pasaporte ha sido desprendida y sustituida por otra fraudulenta. Pese a que la sustitución de páginas enteras es por lo general más difícil de lograr que cambiar una foto pegada, es importante que se adopten las siguientes recomendaciones a fin de combatir esta categoría de riesgo. Al igual que otras categorías de fraude con documentos, es preferible emplear una combinación de elementos de seguridad para evitar la sustitución de páginas enteras en lugar de depender de un solo elemento que, de estar en riesgo, podría socavar la seguridad de todo el documento de viaje.

Elementos básicos:

- la técnica de cosido para encuadernar las páginas en el documento debe ser tal que haga difícil extraer una página sin dejar pruebas claras de que ello ha sucedido;
- impresión de informe de seguridad en la página de datos personales con un diseño distinto al empleado en las páginas de visado;
- números de páginas integrados en el diseño de seguridad de las páginas de visado; y
- número de serie en todas las hojas, de preferencia perforado.

Otros elementos:

- cosido con hilo multicolor o específicamente fluorescente en UV;
- patrón programable de cosido;
- cola curada con UV aplicada al pespunte;
- marcas de referencia o de cotejo impresas en el borde de cada página de visado;
- elementos de seguridad con perforación láser en la página de datos personales; y
- datos personales impresos en una página interior además de en la página de datos.

Cuando se utilicen etiquetas autoadherentes, se aconseja aplicar otras medidas de seguridad como se describen en A.5.1.2 y A.5.2.4, incluso relacionando la etiqueta con el documento de viaje de lectura mecánica mediante el número de éste.

A.5.6 Control de la calidad

Es esencial que se lleven a cabo verificaciones y controles de calidad de todas las etapas del proceso de producción y entre lote y lote para lograr uniformidad en el documento de viaje terminado. Esto debe comprender verificaciones para garantizar la calidad de todos los materiales que se emplean en la fabricación de los documentos y la legibilidad de las líneas de lectura mecánica. La importancia de la uniformidad en el documento de viaje terminado es de suma importancia

ya que los inspectores de inmigración y los funcionarios de control fronterizo confían en la posibilidad de reconocer documentos falsos a partir de variaciones en su apariencia o características. De haber variaciones en la calidad, el aspecto o las características de los documentos de viaje genuinos de un Estado, se dificulta mucho la detección de imitaciones fraudulentas o de documentos falsos.

A.5.7 Control de seguridad de la producción y los productos

Un peligro importante para la seguridad del MRP de un Estado expedidor es el robo en la instalación de producción de MRP genuinos pero no personalizados o de componentes con los cuales pueden fabricarse los MRP.

A.5.7.1 Protección contra el robo y uso indebido de documentos en blanco genuinos o de los componentes de los documentos

Los documentos en blanco deben guardarse bajo llave en instalaciones debidamente supervisadas. Deben adoptarse las siguientes medidas de seguridad:

Medidas básicas:

- buena seguridad física de las instalaciones con acceso controlado a las áreas de entrega, envío y producción y a los lugares donde se almacenan los documentos;
- pista de auditoría completa que incluya el conteo y la conciliación de todos los materiales (usados, no usados, defectuosos o estropeados) y registros certificados de los mismos;
- cuando corresponda, numeración de serie en todos los documentos en blanco y en otros componentes delicados desde el punto de vista de la seguridad con pista de auditoría completa de todos los documentos desde su fabricación hasta el despacho de los mismos;
- cuando corresponda, números de seguimiento y control de otros componentes principales de los documentos (por ejemplo, rollos u hojas de laminados, dispositivos de elementos ópticamente variables);
- vehículos de transporte seguro para el traslado de documentos en blanco y otros componentes principales de los documentos (cuando corresponda);
- datos de todos los documentos de viaje en blanco perdidos o robados para su rápida transmisión entre los gobiernos y a las autoridades de control de fronteras con los detalles enviados a la base de datos de documentos perdidos y robados de INTERPOL;
- controles apropiados implantados para proteger contra el fraude interno los procedimientos de producción; y
- investigación de antecedentes y verificación de seguridad del personal.

Otros elementos:

- televisión en circuito cerrado (CCTV) para vigilar y grabar todas las áreas de producción, donde se permita; y
- almacenamiento y personalización centralizados de los documentos en blanco en el menor número posible de lugares.

Tabla A-1. Resumen de las recomendaciones de seguridad

Elementos	*Elementos básicos*	*Otros elementos*
Materiales del sustrato (A.5.1)		
Sustratos de papel (A.5.1.1)	– respuesta UV controlada – filigrana de dos-tonos – sensibilizadores químicos – absorbencia y características superficiales apropiadas	– filigrana en el registro – filigranas diferentes en la página de datos y la página de visado – filigrana de molde cilíndrico – fibras fluorescentes invisibles – fibras (fluorescentes) visibles – hilo de seguridad – compuesto marcador – elemento de seguridad perforado con láser
Papel u otro sustrato en forma de etiqueta (A.5.1.2)	– respuesta UV controlada – sensibilizadores químicos – fibras fluorescentes invisibles – fibras (fluorescentes) visibles – sistema de adhesivos	– hilo de seguridad – filigrana – elemento de seguridad perforado con láser – patrón de seguridad troquelado
Sustratos sintéticos (A.5.1.4)	– construcción resistente a la división en capas – material ópticamente opaco – incorporación protegida de la página de datos – elementos ópticamente variables – véase 5.2 – 5.5, según corresponda	– característica de ventana transparente – elemento táctil – elemento de perforación láser
Impresión de seguridad (A.5.2)		
Fondo e impresión del texto (A.5.2.1)	– fondo de seguridad Guilloche a dos tintas – impresión arco iris – texto en microimpresión – diseño único de la página de datos	– impresión calcográfica (intaglio) – imagen latente – patrón antiescáner – doble patrón de seguridad – elemento de diseño en relieve – elemento de registro anverso-reverso – error intencional – diseño único en cada página – elemento táctil – tipos de letra únicos
Tintas (A.5.2.2)	– tinta fluorescente UV – tinta reactiva	– tinta con propiedades ópticamente variables – tinta metálica – tinta de numeración penetrante – tinta metamérica – tinta invisible en la región infrarroja – tinta absorbente en la región infrarroja – tinta fosforescente – tinta marcada – tinta invisible

Elementos	*Elementos básicos*	*Otros elementos*
Numeración (A.5.2.3)	– numeración en todas las páginas – número impreso o perforado – numeración de tipo especial para etiquetas – la misma técnica para aplicar la numeración y los datos personales en sustratos y tarjetas sintéticas	– número de documento perforado con láser – tipo especial
Técnica de personalización (A.5.4)		
Protección contra la sustitución y alteración de la fotografía (A.5.4.4)	– datos personales integrados – fondo de seguridad fundido dentro del área del retrato – tintas reactivas y sensibilizadores químicos en el papel – dispositivo de seguridad visible superpuesto al área del retrato – laminado de seguridad sellado térmicamente o equivalente	– firma presentada – imagen esteganográfica – imágenes del retrato adicionales – elemento biométrico según la Parte 9
Otras medidas de seguridad para las libretas de pasaporte (A.5.5)		
Sustitución de una página (A.5.5.2)	– tecnología de cosido segura – cosido con hilo fluorescente en UV – diseño único de página de datos – número de serie integrado en un diseño de seguridad – número de serie en cada página	– cosido con hilo multicolor – patrón de cosido programable – cola curada UV para el pespunte – marcas de referencia en cada página – elemento de seguridad perforado con láser – datos personales en una página interior
Control de seguridad de la producción y los productos (A.5.7)		
Protección contra el robo y uso indebido (A.5.7.1)	– buena seguridad física – pista de auditoría completa – números de serie en los documentos en blanco, según corresponda – números de seguimiento y control de los componentes, según corresponda – transporte seguro de documentos en blanco – intercambio internacional de información sobre documentos extraviados y robados – procedimientos internos de protección contra fraudes – investigación y control de seguridad del personal	– CCTV en las áreas de producción – almacenamiento y personalización centralizados

Nota 1.— La lista de otros elementos no es exhaustiva y se exhorta a los Estados y organizaciones expedidores a que adopten otros elementos de seguridad que no se mencionan explícitamente en este apéndice.

Nota 2.— Las descripciones que figuran en la tabla anterior son, necesariamente, más breves que las del texto principal. Para facilitar su localización, en la columna "Elementos" de la tabla se indican entre paréntesis los números de las secciones pertinentes de este apéndice.

Nota 3.— Ciertos elementos se repiten una o más veces en la tabla, lo cual indica que el elemento de que se trata protege contra más de un peligro, pero solo es necesario incluirlos una vez en un documento en particular.

Nota 4.— Hay muchos otros factores relacionados con la seguridad de los pasaportes que los descritos aquí. En los Apéndices B y C se proporciona orientación adicional. Por lo tanto, los Apéndices A, B y C deben considerarse colectivamente para asegurar la integridad de la expedición de los documentos.

Nota 5.— Toda referencia, directa o implícita, a términos o tecnologías específicos tiene por único objeto captar en su forma genérica dichos términos y tecnologías y no tienen relación alguna con vendedores o proveedores de tecnología específicos.

— — — — — — — —

APÉNDICE B DE LA PARTE 2 — VERIFICACIÓN DE LA SEGURIDAD DEL DOCUMENTO CON AYUDA DE MÁQUINA (INFORMATIVO)

B.1 ALCANCE

El presente apéndice contiene recomendaciones que abarcan la autenticación mecánica de los elementos de seguridad del propio documento (sobre la base del material, la impresión de seguridad y las técnicas de protección frente a las copias) así como asesoramiento sobre tecnologías de lectores que permiten la autenticación mecánica de documentos.

B.2 LECTORES DE DOCUMENTOS Y SISTEMAS PARA AUTENTICACIÓN MECÁNICA

A efectos de verificar los elementos de seguridad tradicionales e innovadores de los MRTD, es importante contar con una tecnología de lectura que haga lugar a la amplia variedad de documentos de viaje en circulación. Estos lectores deben estar equipados con los sensores apropiados para los elementos de autenticación mecánica comunes y avanzados. Por supuesto, esto constituye una cuestión mundial que entraña costos e infraestructura.

B.2.1 Lectores estándar

Los lectores estándar que se emplean en las fronteras tienen normalmente los equipos sensores siguientes:

- capacidad de captura de imágenes en las regiones espectrales VIS, UV e IR así como de alta resolución (resolución mínima 300 dpi) – esto permite leer la ZLM (preferiblemente en la región espectral IR) y el procesamiento de imágenes de otros elementos (en la región espectral VIS); y
- lectores de CI sin contacto que cumplen la norma ISO 14443 (@ frecuencia de 13,56 MHz).

Normalmente, los lectores estándar pueden detectar y verificar los siguientes elementos de seguridad:

- lectura de la ZLM y dígito de verificación;
- lectura de CI sin contacto y autenticación pasiva (y, como opción, autenticación activa); y
- verificaciones de seguridad genéricas (papel opaco a la luz UV, ZLM legible en IR, …).

Una mayor “inteligencia” de estos lectores depende únicamente del soporte lógico y no de equipos sensores adicionales y, por consiguiente podría emplearse fácilmente a discreción del Estado receptor sin invertir más recursos en equipo especializado. Las capacidades del soporte lógico de los lectores pueden comprender:

- reconocimiento de patrones utilizando bases de datos (basándose en imágenes VIS, UV e IR);
- lectura y autenticación de filigranas digitales (elementos esteganográficos) para verificar la autenticidad de la expedición;
- detección y lectura en pantallas (alfanuméricas) y sus futuros elementos de seguridad; y
- detección y lectura de elementos de seguridad basados en “LED en plástico”.

B.2.2 Lectores avanzados

Además, los lectores avanzados pueden tener los siguientes equipos sensores, adecuados para autenticar elementos de seguridad especiales:

- iluminación coaxial para la verificación de recubrimientos de seguridad retrorreflexivos;
- diodo láser o iluminación LED para la verificación de elementos estructura especiales, p. ej., dispositivos de imágenes difractivas ópticamente variables (DOVID);
- sensores magnéticos para elementos sustrato especiales, p. ej., para la verificación de fibras magnéticas;
- dispositivos de análisis espectral o detención de polarización; y
- la iluminación de transmisión de la página de datos del MRP para verificar filigranas registradas, perforación con láser, ventanas y registros transparentes, requiere una geometría de lector especial que permita colocar la página de datos solamente en el lector (sin cubierta detrás).

Normalmente, las capacidades de lectura avanzadas se basan en acuerdos de propiedad nacionales, bilaterales o multilaterales y requieren soporte físico especial.

B.2.3 Sistemas de fondo, infraestructura de clave pública (PKI)

Para autenticar ciertos tipos de elementos verificables con máquina puede ser necesario contar con un sistema de fondo o una PKI. Esta podía ser la PKI actual para MRTD (la parte más prominente es la PKI de la OACI) donde los Estados pueden intercambiar información sobre sus elementos de seguridad dentro de la estructura lógica de datos, protegida por medio de certificados.

B.3 ELEMENTOS DE SEGURIDAD Y SU APLICACIÓN A LA AUTENTICACIÓN MECÁNICA

En los párrafos siguientes se describen los principales elementos y técnicas de seguridad identificados en el Apéndice A sobre normas de seguridad y se explica la forma de emplear la autenticación mecánica para estos mecanismos de seguridad. Las autoridades expedidoras que seleccionan elementos de seguridad del Apéndice A pueden usar las tablas siguientes para verificar las posibilidades de autenticación mecánica que existen para tales elementos.

B.3.1 Materiales del sustrato

B.3.1.1 Papel empleado en las páginas de un documento de viaje

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Respuesta UV controlada		X					Intensidad UV
Filigrana de dos tonos					Transmisión	F	Cotejo con patrón
Sensibilizadores químicos							N/A
Absorbencia y características superficiales apropiadas							N/A
Otros elementos							
Filigrana en el registro					Transmisión	F	Cotejo con patrón
Filigrana diferente en página de datos y página de visado					Transmisión	F	Cotejo con patrón*
Filigrana de molde cilíndrico					Transmisión	F	Cotejo con patrón
Fibras fluorescentes invisibles		X	X			F/V	Cotejo con patrón
Fibras (fluorescentes) visibles	X	X				F/V	Cotejo con patrón
Hilo de seguridad	X	X			Transmisión, magnético	F	Cotejo con patrón
Compuesto marcador					Especial	F/V	Depende del marcador
Elemento de seguridad perforado con láser					Transmisión	F/V	Cotejo con patrón

* Se requiere la interacción del usuario y no es adecuado para sistemas automáticos de control fronterizo

B.3.1.2 Papel u otro sustrato en forma de etiqueta

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Respuesta UV controlada		X					Intensidad UV
Sensibilizadores químicos							N/A
Fibras fluorescentes invisibles		X	X			F/V	Cotejo con patrón
Fibras (fluorescentes) visibles	X	X				F/V	Cotejo con patrón
Sistema de adhesivos							N/A
Otros elementos							
Hilo de seguridad	X				Transmisión, magnético	F	Cotejo con patrón
Filigrana					Transmisión	F	N/A
Elemento de seguridad perforado con láser					Transmisión	F/V	Cotejo con patrón
Patrón de seguridad troquelado					Transmisión	F	Cotejo con patrón

B.3.1.3 Sustratos sintéticos

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Construcción resistente a división en capas							N/A
Material ópticamente opaco		X					Intensidad UV
Incorporación protegida de página de datos							N/A
Elementos ópticamente variables							Véase 5.3
Véase 5.2 – 5.5, según corresponda							
Otros elementos							
Ventana o elemento transparente					Transmisión	F	Cotejo con patrón
Elemento táctil					Retrorreflectante	F/V	Cotejo con patrón
Elemento perforado con láser					Transmisión	F/V	Cotejo con patrón
Características superficiales	X		X		Retrorreflectante	F	Cotejo con patrón

B.3.2 Impresión de seguridad

B.3.2.1 Fondo e impresión del texto

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Fondo Guilloche a dos tintas	X	X	X			F	Cotejo con patrón
Impresión arco iris	X	X			Cámara alta resolución	F	Cotejo con patrón
Texto en microimpresión	X	X	X		Cámara alta resolución	F	Cotejo con patrón
Diseño único de página de datos	X					F	Cotejo con patrón
Otros elementos							
Impresión calcográfica	X	X	X			F	Cotejo con patrón*
Imagen latente							N/A
Patrón antiescáner	X				Cámara de alta resolución	F	Cotejo con patrón
Diseño doble de seguridad					Transmisión	F	Cotejo con patrón*
Diseño en relieve					Retrorreflectante	F	Cotejo con patrón
Elemento de registro anverso-reverso					Transmisión	F	Cotejo con patrón
Error intencional	X	X	X			F	OCR, cotejo con patrón
Diseño único en cada página	X	X				F	Cotejo con patrón**
Elemento táctil					Retrorreflectante	F	Cotejo con patrón
Tipos de letra únicos	X	X	X				Cotejo con patrón

* La implantación no resulta práctica para lectores de pasaportes

** Se requiere la interacción del usuario y no es adecuado para sistemas automáticos de control fronterizo

B.3.2.2 Tintas

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Tinta fluorescente UV		X				F/V	Cotejo con patrón
Tintas reactivas					Especial		Depende de la tinta
Otros elementos							
Tinta con propiedades ópticamente variables	X				Iluminación variable	F/V	Cotejo con patrón
Tinta metálica			X			F/V	Cotejo con patrón
Tinta de numeración penetrante					Especial	V	Cotejo con patrón en ambos lados
Tintas metaméricas	X	X	X			F	Filtros ópticos y cotejo con patrón
Tinta invisible en la región infrarroja	X		X			F/V	Cotejo con patrón
Tinta absorbente en la región infrarroja			X			F/V	Cotejo con patrón
Tinta fosforescente		X	X			F/V	Cotejo con patrón
Tinta marcada					Especial	F	Cotejo con patrón
Tinta invisible		X	X			F	Cotejo con patrón
Tinta magnética					Magnético	F/V	Cotejo con patrón
Tinta Anti-Stokes			X			F/V	Filtros ópticos y cotejo con patrón

B.3.2.3 Numeración

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Numeración en todas las páginas Número impreso o perforado	X		X			F/V	OCR, Cotejo con patrón
Numeración con tipo especial para etiquetas	X		X			F/V	OCR, Cotejo con patrón
Misma técnica para aplicar numeración y datos personales en sustratos sintéticos y tarjetas							N/A
Otros elementos							
Número de documento perforado con láser					Transmisión	F/V	Cotejo con patrón
Tipos especiales	X					F/V	OCR, Cotejo con patrón

B.3.3 Protección contra las copias

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Elementos ópticamente variables en la página de datos personales	X				Iluminación variable	F/V	Cotejo con patrón
OVD con sobreimpresión calcográfica si no hay laminado							N/A
Otros elementos							
Dispositivo difrangente ópticamente variable para lectura mecánica					Láser	F/V	Descrifrado
Elemento de seguridad perforado con láser					Transmisión	F/V	Cotejo con patrón
Patrón antiescáner	X				Cámara alta resolución	F	Cotejo con patrón

B.3.4 Técnicas de personalización

B 3.4.1 Protección contra sustitución de la fotografía y alteración de los datos

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Datos personales integrados							N/A
Fondo de seguridad fundido dentro del área del retrato							N/A
Tintas reactivas y sensibilizadores químicos en el papel							N/A
Dispositivo de seguridad visible superpuesto al área del retrato	X				Iluminación variable	F/V	Cotejo con patrón
Laminado de seguridad con sellado térmico o equivalente	X					F/V	Cotejo con patrón
Otros elementos							
Firma exhibida							N/A
Elemento esteganográfico	X	X	X			F/V	Decodificación
Imágenes de retrato adicionales	X	X	X	X		V	Cotejo con patrón
Elemento biométrico según Parte 9				X		V	Lector RF

B.3.5 Otras medidas de seguridad para las libretas de pasaportes

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Tecnología de cosido seguro							N/A
Hilo de cosido fluorescente en UV		X				F	Cotejo con patrón
Diseño único de página de datos	X					F	Cotejo con patrón
Números de página integrados en diseño de seguridad	X	X			Cámara alta resolución		Cotejo con patrón
Número de serie en cada página							N/A
Otros elementos							
Cosido con hilo multicolor	X	X				F	Cotejo con patrón
Patrón de cosido programable	X	X				F	Cotejo con patrón
Cola curada con UV para pespunte							N/A
Marcas de referencia en cada página							N/A
Elemento de seguridad perforado con láser					Transmisión	F/V	Cotejo con patrón
Datos personales en página interior							N/A

B.3.6 Otras medidas de seguridad adecuadas a la autenticación mecánica

Los siguientes elementos de seguridad se adecuan a la autenticación mecánica pero no figuran en la lista del Apéndice A.

Elementos de seguridad	*Se requiere sensor para autenticación mecánica*					*Patrón fijo/variable*	*Método de autenticación mecánica*
	Lector estándar				*Lector avanzado*		
	VIS	*UV*	*IR*	*RF*	*Sensor especial*		
Elementos básicos							
Lectura ZLM y verificación por dígitos	X		X			F/V	Cálculo de suma total
Lectura de CI sin contacto y autenticación pasiva (+AA)				X			Lector RF
Detección y lectura de elementos de seguridad basados en LED en plástico	X	X	X	X		F/V	Uso de R/F para alimentar LED en plástico
Detección y lectura de presentaciones (alfanuméricas) y sus futuros elementos de seguridad	X	X	X	X		F/V	Uso de R/F para alimentar presentación en plástico
Detección y verificación de material de lámina retrorreflectante	X				Iluminación coaxial	F/V	Cotejo con patrón
Códigos de barra	X	X	X			V	Descifrado

B.4 CRITERIOS DE SELECCIÓN PARA Elementos de seguridad VERIFICABLES POR MÁQUINA

Si un Estado expedidor considera incorporar en sus MRTD elementos de seguridad para la autenticación mecánica o si un Estado receptor prevé emplear sistemas lectores que pueden autenticar mecánicamente los MRTD, deben considerarse diversos criterios para la selección de dichos elementos.

Análogamente al proceso de selección para la característica biométrica de interfuncionamiento mundial o la tecnología de almacenamiento, estos criterios comprenden:

- seguridad – el criterio más importante;
- disponibilidad, pero exclusividad para documentos de seguridad (preferiblemente más de un proveedor disponible);
- uso doble, es decir, finalidad adicional del elemento más allá de la autenticación mecánica, p. ej., propiedad general antircopias o inspección visual;
- potencial de personalizar (es decir, individualizar) el elemento de autenticación mecánica con información extraída del pasaporte para proteger los datos personales (p. ej., número de pasaporte, nombre) a efectos de evitar la reutilización de partes de pasaportes genuinos;
- compatibilidad con los procesos de expedición de MRTD;
- compatibilidad (con propiedades existentes y estándar de los MRTD);
- compatibilidad con el proceso de control en la frontera y en otras partes (p. ej., no obstrucción de elementos de seguridad básicos, no se necesita tiempo adicional);
- interfuncionamiento;
- disponibilidad de sensores;
- costo (para elemento y sensor);
- aspectos de propiedad intelectual (PI), por ejemplo, patentes;
- inspección primaria e inspección secundaria;
- tiempo necesario para utilizar realmente el elemento;
- posibles dificultades relacionadas con la fabricación de la libreta o los procesos de personalización; y
- durabilidad, es decir, con arreglo a las especificaciones pertinentes de la ISO y la OACI para MRTD.

— — — — — — — —

APÉNDICE C DE LA PARTE 2 — AUTENTICACIÓN ÓPTICA MECÁNICA (INFORMATIVO)

C.1 INTRODUCCIÓN

Para la autenticación de los documentos de viaje de lectura mecánica (MRTD) como parte de los controles fronterizos estacionarios, incluidas las puertas de control fronterizo automatizado (ABC), va en aumento el uso de sistemas de tecnología de la información, que van mucho más allá de la mera extracción y verificación de la ZLM de los documentos y de la inspección automática de las características de seguridad óptica. Las importantes mejoras de las tecnologías utilizadas en el contexto de la autenticación mecánica de los documentos han contribuido al crecimiento de la cantidad y diversidad de sistemas de autenticación. No obstante, el significativo incremento del volumen de público viajero sigue constituyendo un reto para todas las personas que participan en el diseño, la producción y el despliegue de los sistemas de autenticación y los MRTD.

Los sistemas de autenticación utilizados para realizar la autenticación mecánica de los MRTD incluyen varios componentes que son necesarios para interactuar adecuadamente entre sí. Además, las características de seguridad de los documentos de lectura mecánica tienen que diseñarse e implantarse de conformidad con las capacidades de los sistemas de autenticación y los conocimientos de las personas profesionales experimentadas.

En este apéndice se formulan una serie de recomendaciones para las principales partes intervinientes en el diseño, implementación y funcionamiento de los sistemas afectados y los componentes clave, cuyas principales metas son las siguientes:

- elevar el nivel de concienciación en cuanto a las cuestiones relacionadas con la seguridad de la autenticación mecánica, que atañen a las principales partes interesadas, como por ejemplo los productores de documentos de seguridad, los fabricantes de equipos de lectura y los gobiernos;
- proponer un catálogo de rutinas de verificación genérica con terminología uniforme; y
- definir recomendaciones para las/os diseñadoras/es de documentos de seguridad, fabricantes de sistemas de auhenticación y niveles operacionales.

La finalidad de este apéndice es apoyar a los profesionales en el diseño y desarrollo de los sistemas de autenticación. No obstante, es importante tener presente que un sistema de autenticación debería usarse para facilitar la adjudicación a su operador/a y no debería considerarse como el único mecanismo de toma de decisiones, particularmente con respecto a las características de seguridad que no pueden ser verificadas por la máquina, sino únicamente por la persona operadora[1].

Este apéndice se ocupa solamente de la parte óptica de la autenticación de los MRTD y el alcance de las recomendaciones formuladas se limita a los datos adquiridos a través de lectores de página completa, i.e. imágenes de tamaño completo del documento, como se describe en el Apéndice B de esta Parte. Además, en las directrices no se hace distinción entre las inspecciones de 1º, 2º y 3º nivel ya que los lectores de página completa pueden utilizarse en todos y cada uno de esos supuestos. Los dispositivos móviles no se toman en consideración (hasta el momento) debido a sus limitadas capacidades ópticas con respecto a las diferentes fuentes de luz (ni UV ni IR), por lo que no cumplen los requisitos propuestos.

1. Operador/a: Persona que interactúa directamente con el sistema de autenticación (p. ej., interacción manual con el lector de documentos) en el contexto de la verificación de un documento.

En la sección C.2 se introducen los conceptos básicos y la terminología necesarios para una mejor comprensión de la autenticación óptica mecánica. Las cuestiones de la armonización y la normalización de las rutinas de verificación se tratan en la sección C.3, donde se define un catálogo de rutinas de verificación genérica. La sección C.4 se centra en recomendaciones detalladas para los fabricantes de sistemas de autenticación y la sección C.5 pone de relieve varios enfoques y métodos de procesamiento de datos conformes con las políticas de protección de datos.

C.1.1 Terminología

Aunque las recomendaciones y directrices no sean vinculantes para las partes directamente afectadas, la terminología se ha adoptado e integrado en la Parte 1 del Doc 9303 para que exista una descripción inequívoca de qué aspectos deberían observarse para alcanzar los objetivos definidos en este documento.

La terminología debería considerarse como una forma práctica de organizar las recomendaciones y directrices por orden de importancia y no debería tomarse por un conjunto de requisitos restrictivos similares a los utilizados en las normas clásicas (p. ej., ISO). La presente terminología se utilizará para que el grupo destinatario disponga de orientaciones claras, precisas e inequívocas acerca de qué es lo que se ajusta y lo que no a las mejores prácticas.

C.1.2 Influencia de la verificación electrónica en el proceso de autenticación

Aunque la atención se centra en la parte óptica de la autenticación de los MRTD, ha de tomarse en consideración la parte electrónica. Sobre la base del estado actual de la tecnología, es altamente probable y cabe esperar que se produzca una interacción entre una microplaqueta (eMRTD) y un módulo RF (lector de página completa) durante el proceso de autenticación. La mejor forma de entender algunas de las recomendaciones formuladas en el presente documento es teniendo presente que las verificaciones ópticas y electrónicas (si se aplica) son procesos complementarios que convergen hacia un resultado global.

Dos aspectos de la interacción entre las verificaciones ópticas y electrónicas revisten particular interés, a saber: la comparación entre los datos ópticos y electrónicos; y las repercusiones de la verificación en cuanto a la presencia de una microplaqueta si se prevé que haya una. Para ninguno de estos dos aspectos puede descartarse la influencia de la verificación electrónica, que se destaca en las recomendaciones correspondientes.

C.2 DEFINICIONES

En la siguiente sección se introduce una terminología uniforme para su uso ulterior. El proceso de inspección de los MRTD se describe en general en la sección C.2.1 y de forma detallada en la sección C.2.2. En la sección C.1.2 se aborda la influencia de la parte electrónica del proceso de autenticación.

C.2.1 Proceso de identificación y verificación de los MRTD

La verificación de la autenticidad de un documento de viaje incluye la verificación de las características de seguridad óptica del documento. Esa verificación se lleva a cabo por medio de un sistema de autenticación[2] que consta de los siguientes componentes: un lector de página completa, un programa informático de autenticación[3], una base de datos de autenticación y, opcionalmente, una base de datos de referencia.

2. Un sistema de autenticación describe la combinación de un lector de página completa, un programa informático de autenticación, incluida una base de datos de autenticación, y, opcionalmente, una base de datos especializada de referencia.

3. El programa informático de autenticación recibe el conjunto de datos reales del lector de página completa. Ofrece varios algoritmos de autenticación para que se apliquen las rutinas de verificación al conjunto de datos reales.

El lector de página completa crea imágenes a tamaño normal del documento de viaje para que se verifiquen con diferentes fuentes de luz. Este denominado conjunto de datos reales (imágenes a tamaño normal del documento)[4] se transfiere al programa informático de autenticación por medio del lector de página completa.

Por lo general, el programa informático de autenticación identifica el denominado *modelo de documento* del documento que usa la zona de lectura mecánica (ZLM) y/o información adicional (p. ej., patrón específico del diseño del documento, fecha de expedición, elementos ópticos específicos, etc.) como datos de entrada. Un modelo de documento abarca las series de documentos de un país/nación que tienen la misma apariencia óptica.

De conformidad con la orientación técnica [BSI-TR-03135], un modelo de documento se define por medio del código del país (C), el tipo de documento (T), un número de identificación único (N) y el valor del año de la primera expedición (Y):

Modelo de documento: = (C, T, N, Y)[5]

El código del país C tiene que rellenarse como código de tres letras de conformidad con las especificaciones del Doc 9303 de la OACI.

El tipo de documento T también está especificado por la OACI en el Doc 9303.

El número de identificación N debe ser un número entero único en orden cronológico creciente, que empiece por 1 y referencie el modelo – o generación – del documento.

El año Y se refiere, mediante un valor entero de 4 dígitos, al año en el que un documento de ese modelo particular se expidió por primera vez. Si se desconoce el año, se omitirá este valor.

Por ejemplo, los dos modelos de pasaporte/documento británico de 2008 y 2010 en circulación constan de los siguientes identificadores: (GBR, P, 1, 2008) y (GBR, P, 2, 2010).

Existen varios planteamientos técnicos para identificar el modelo de documento. La adquisición de la ZLM es uno de ellos (véase la sección C.4.3.2). Si se usa la ZLM, pero no es suficiente para la determinación inequívoca del modelo de documento, tienen que usarse parámetros de documentos adicionales (p. ej., patrones) para ayudar a restringir los resultados de la identificación; especialmente cuando existen varios modelos de documentos válidos del mismo país (p. ej., el pasaporte británico)[6].

El programa informático de autenticación envía el identificador del modelo de documento a la base de datos de autenticación, donde se almacenan las denominadas *rutinas de verificación*. Estas rutinas de verificación definen qué procedimientos de prueba tienen que aplicarse al conjunto de datos reales de ese modelo de documento de viaje particular. Para cada modelo de documento se determina un conjunto específico de rutinas de verificación, el denominado *conjunto de datos de autenticación*. Después de recibir el identificador del modelo de documento, la base de datos de la autenticación envía el conjunto de datos correspondiente al programa informático de autenticación. En la sección C.2.2 (véase la figura C-1) se incluyen más detalles sobre el establecimiento de una base de datos de autenticación.

---

4. Conjunto de datos reales: La foto normal, IR y UV del documento objeto de prueba que se va a verificar con el sistema de lectura. Estas fotos se usan para la inspección del documento.

5. Este apéndice se centra únicamente en la parte óptica de la autenticación mecánica de documentos. Eso significa que los documentos que son idénticos desde el punto de vista óptico, pero cuyas características electrónicas difieren, se considera que pertenecen al mismo modelo de documento.

6. Algunos países, como Australia, usan una serie de una letra para distinguir diferentes modelos o series de documentos (p. ej., la serie N). Aun cuando este método pudiera ser suficiente a nivel nacional, no resulta muy eficaz para la clasificación internacional debido a la falta de normalización. Así pues, este documento sigue las recomendaciones de [BSI-TR-03135], que se consideran más adecuadas para los fines de la clasificación internacional.

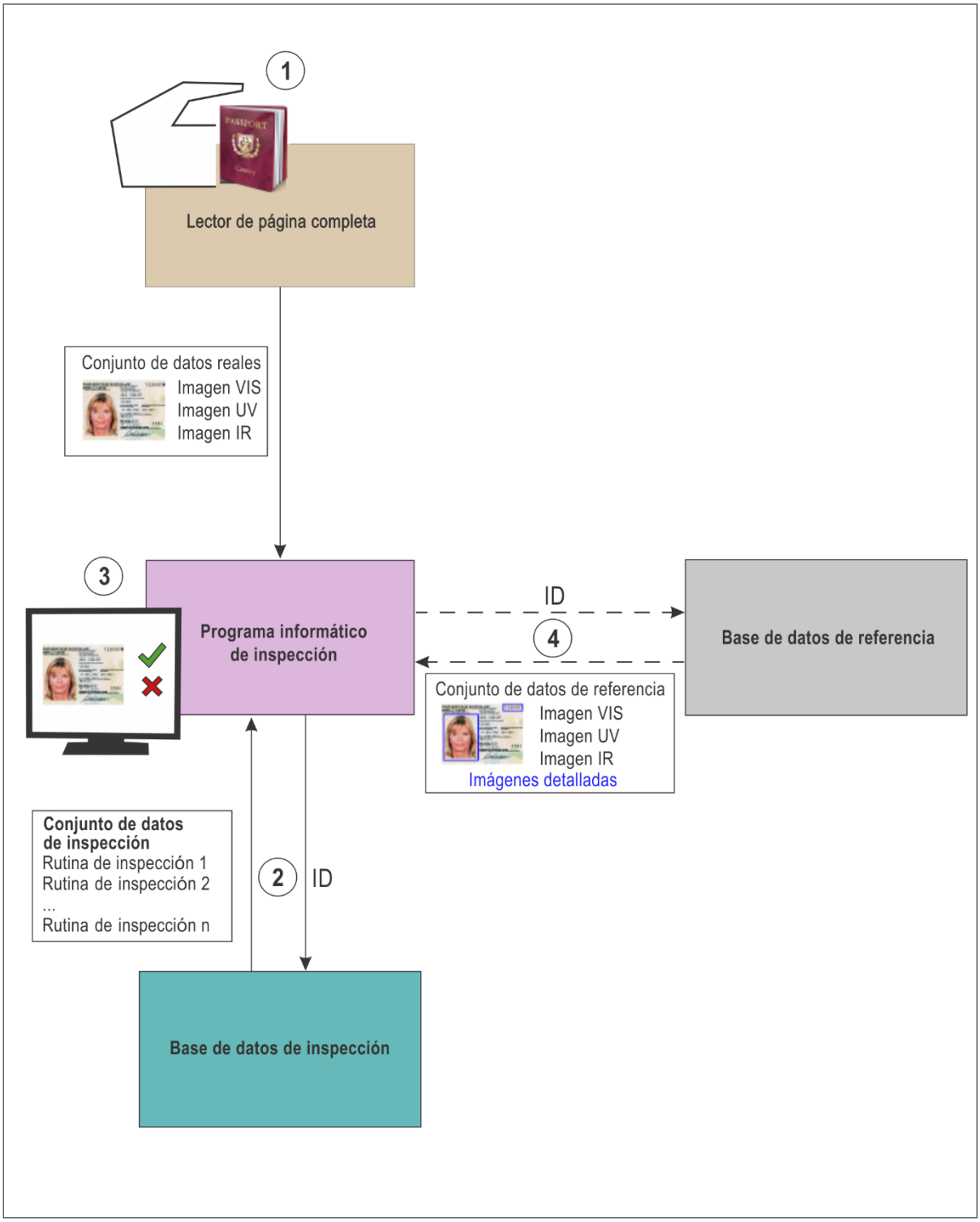

Figura C-1. Proceso de identificación y verificación de documentos; los números indican el orden de los diferentes pasos del proceso

Posteriormente, el programa informático de autenticación realiza la verificación. Las rutinas de verificación se aplican al conjunto de datos reales del documento de viaje. Habitualmente, este examen lleva a un resultado de aprobado o reprobado. Un resultado de aprobado significa que el documento verificado no presenta ninguna anomalía, mientras que un resultado de reprobado significa lo contrario. En función del escenario de aplicación, la interpretación del resultado (aprobado o reprobado) recae en la persona operadora a cargo.

Si un conjunto de datos reales no se puede asignar inequívocamente a un modelo de documento particular, cabe efectuar un subconjunto de rutinas de verificación (opcionalmente). Tales rutinas se especifican con independencia del modelo de documento.

A fin de ayudar a la persona operadora en una verificación manual, el programa informático de autenticación puede solicitar el denominado *conjunto de datos de referencia* de la base de datos de referencia sobre la base del modelo de documento identificado. El conjunto de datos de referencia contiene la luz visible (blanca), las imágenes IR y UV del modelo de documento; asimismo, puede incluir fotos más detalladas de las partes del documento, así como más textos descriptivos. No obstante, esta denominada base de datos de referencia, también denominada *base de datos especializada* en la práctica, no es un componente obligatorio del sistema de autenticación propiamente dicho. El proceso de identificación y verificación de documentos se ilustra en la figura C-1.

C.2.2 Pasos del establecimiento/ de una base de datos de autenticación

En la base de datos de autenticación se almacena un conjunto bien definido de rutinas de verificación para cada modelo de documento. Por ejemplo, las rutinas de verificación para el modelo de documento alemán de 2007 difieren de las rutinas que tienen que aplicarse al modelo de documento británico de 2008.

La rutina de verificación de un conjunto indica una especificación de ensayos de la propiedad de una característica de seguridad óptica. Por ejemplo, la rutina de verificación 1 de la figura C-2 verifica si la foto es absorbente en la luz visible. En este caso, la foto es la característica óptica, cuya propiedad de absorción se prueba a la luz visible (véase fuente de luz 1 en la rutina de verificación 1). La implementación de esta rutina de verificación la lleva a cabo un algoritmo de autenticación proporcionado por el programa informático de autenticación (véase el algoritmo de autenticación 1 en la rutina de verificación 1). En este caso, el algoritmo 1 es un algoritmo de autenticación que verifica el brillo de la característica de que se trate. En cambio, la rutina de verificación x de la figura C-2 verifica si la tinta es luminiscente a la luz ultravioleta dentro de la superficie de la foto utilizando el algoritmo de “verificación de patrones” (algoritmo de verificación n del programa informático de autenticación de la figura C-2). Este ejemplo muestra claramente que una característica de seguridad óptica puede presentar propiedades diferentes según la fuente de luz (véase la figura C-3).

Según la normativa de la Unión Europea sobre las normas mínimas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje[7], puede hacerse una división razonable de estas rutinas de verificación en tres categorías: material, técnica de impresión y personalización.

7. Reglamento (CE) Nº 2252/2004 del Consejo de 13 de diciembre de 2004.

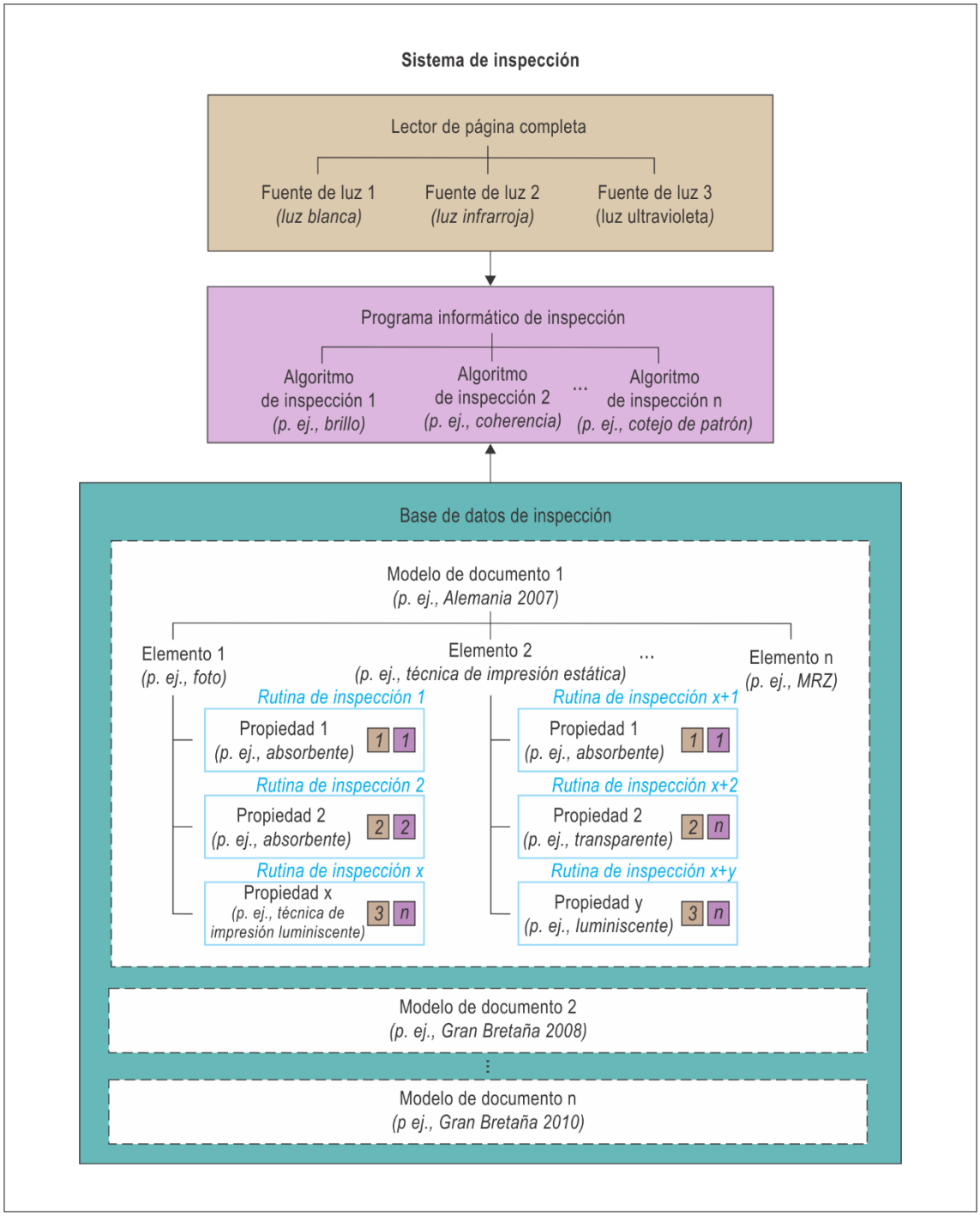

Figura C-2. Diagrama esquemático del establecimiento de un sistema de autenticación

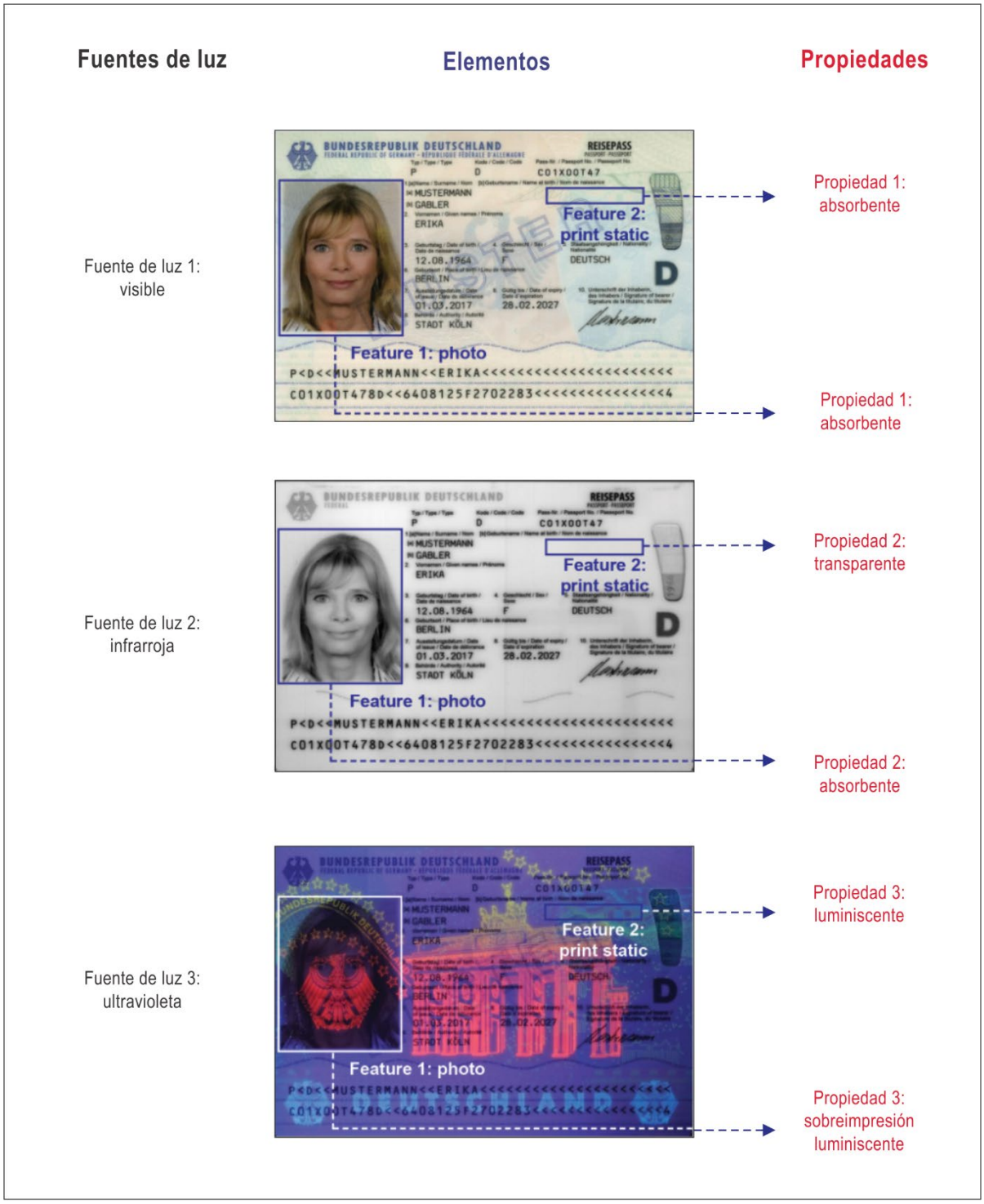

Figura C-3. Características y propiedades de un pasaporte alemán con diferentes fuentes de luz

C.3 CATÁLOGO DE RUTINAS DE VERIFICACIÓN GENÉRICA

Todas las personas que desarrollan un sistema de autenticación definen sus propios identificadores para las rutinas de verificación. Cada modelo de documento tiene sus propias rutinas de verificación; sin embargo, con frecuencia el significado de los identificadores de esas rutinas de verificación no resulta evidente. De ahí que, en general, no se puedan comparar las rutinas de verificación aplicadas al mismo modelo de documento en diferentes sistemas de autenticación.

Para resolver este problema es posible definir un catálogo de rutinas de verificación viables sobre la base de elementos de seguridad de espectro selectivo de los documentos de viaje. El contenido de este catálogo puede extenderse a futuras versiones de esta orientación preservando la nomenclatura propuesta. Las rutinas de verificación correspondientes, denominadas rutinas de verificación de espectro selectivo, registran las reacciones diferentes que se producen en un documento verificado con luz visible (VI – luz visible) o luz extravisible (UV – ultravioleta, IR - infrarroja). Sobre la base de los tres registros (VI, UV, IR), pueden verificarse las reacciones absorbentes, reflectantes o luminiscentes de esos elementos. Secuencialmente, estas rutinas de verificación de espectro selectivo se refieren a las rutinas de verificación genérica definidas en [BSI-TR-03135].

La aplicación de este catálogo de rutinas de verificación genérica mejoraría sobremanera la situación mencionada y permitiría una comprensión más cabal de los mecanismos de autenticación mecánica.

C.3.1 Descripción de las rutinas de verificación genérica

Los identificadores inequívocos (definidos más adelante) de las rutinas de verificación para la autenticación óptica mecánica se han definido sobre la base de la reacción espectral de los elementos de seguridad de los documentos de viaje. Puede hacerse una división razonable de los mismos en las cuatro categorías siguientes, definidas en el Apéndice A:

- verificación de las propiedades materiales (sustrato): Se verifican las reacciones del sustrato de impresión, p. ej., el brillo con luz ultravioleta

- verificación de las propiedades de las técnicas de impresión: Se prueban los elementos que están impresos en el documento, independientemente de la personalización, p. ej., menciones fijas de un documento)

- verificación de los elementos que protegen contra las copias: por lo general elementos o laminados difractivos u holográficos

- verificación para expedir propiedades técnicas (personalización): Se prueban las características de personalización, p. ej., el nombre de la persona titular del documento.

La apariencia óptica de las características de la categoría “protección anticopia” depende en gran medida del esquema de iluminación. Así pues, en general, las características de esta categoría –que estén adaptadas a la inspección humana– pueden resultar sumamente problemáticas para la autenticación mecánica en general. Por este motivo, las características de esta categoría no se abordan en las rutinas de verificación propuestas.

Las 48 rutinas de verificación genérica definidas más adelante consisten en las denominadas *rutinas básicas de verificación* (BR) y *rutinas compuestas de verificación* (CR). Las rutinas básicas de verificación son rutinas individuales, que se refieren a una propiedad (p. ej., la absorción de IR) de una sola característica. Las rutinas compuestas de verificación se definen como combinaciones lógicas de rutinas básicas de verificación. Por consiguiente, puede probarse una sola característica para determinar múltiples propiedades, tales como la absorción de IR y la transparencia en la luz visible.

Para las rutinas básicas de verificación se utilizan las siguientes definiciones abreviadas de conformidad con [BSI-TR-03135]:

Rutina básica de verificación: = (XX, YY, ZZ)

XX especifica la fuente de luz para la imagen en la que se realiza la rutina de verificación:

- **IR** – Luz infrarroja
- **UV** – Luz ultravioleta
- **VI** – Luz visible (blanca)

YY es un identificador de la propiedad óptica de la característica determinada:

- **AB** – absorbente, propiedad de la tinta
- **BR** – brillo, propiedad del sustrato (p. ej., brillo en la exposición a la luz UV)
- **FR** – propiedad de frecuencia espacial de los patrones (p. ej., características de los patrones obtenidos después de la transformación de la frecuencia espacial, tales como la transformación de Fourier espacial)
- **LU** – luminiscente, propiedad de los patrones (p. ej., visible en la exposición a la luz UV)
- **TL** – translúcido, propiedad de la tinta que brilla a través del sustrato
- **TR** – transparente, propiedad de la tinta (p. ej., transparente en la exposición a la luz IR)

ZZ es un identificador[8] de la propia característica o la posición en el documento:

- **FI** – Fibras
- **FU** – Página de datos llena (completa)
- **IS** – elemento impreso, que ya existe en el sustrato (tinta estática)
- **MR** – Zona de lectura mecánica (ZLM)
- **OM** – ZLM sobreimpresa
- **CA** – Número de acceso de la tarjeta (forma abreviada: CAN)
- **BC** – Característica del código de barras

8. En esta nomenclatura las propiedades específicas del modelo de documento se denominan “estáticas” (tales como la sobreimpresión UV de un escudo), mientras que las propiedades específicas (individuales/personalizadas) del documento se denominan “dinámicas” (tales como la sobreimpresión UV que repite el número del documento).

- **PD** – Personalizado, perforación “dinámica”
- **PS** – Perforación que muestra un contenido “estático”
- **PH** – Superficie de la foto
- **SP** – Superficie de la foto secundaria
- **OP** – Foto sobreimpresa
- **TH** – Hilo de seguridad
- **VZ** – Zona de inspección visual (ZIV)
- **WM** – Filigrana
- **ID** – Cualquier otra característica “dinámica” personalizada (tinta dinámica), p. ej., una fotografía secundaria
- **AF** – Cualquier otra característica adicional que no pueda atribuirse a los puntos especificados anteriormente

Si una rutina de verificación genérica consiste en más de una sola rutina de verificación, tiene que asignarse un número secuencial a cada una de las rutinas de verificación.

De estas formas abreviadas resultan las siguientes rutinas de verificación genérica[9]:

Verificación de las propiedades del material: (12 BR + 1 CR)

- **(IR, AB, PS)** → (IR, absorbente, perforación estática): Verificar si la perforación estática es visible a la luz IR.
- **(IR, AB, TH)** → (IR, absorbente, hilo): Verificar si el hilo de seguridad es visible a la luz IR.
- **(IR, AB, WM)** → (IR, absorbente, filigrana): Verificar si la filigrana es visible a la luz IR.
- **(UV, BR, FU)** → (UV, brillo, completa): Verificar el brillo de la página de datos completa a la luz UV.
- **(UV, BR, MR)** → (UV, brillo, ZLM): Verificar el brillo de la ZLM a la luz UV.
- **(UV, BR, PH)** → (UV, brillo, foto): Verificar el brillo de la superficie de la foto a la luz UV.
- **(UV, BR, VZ)** → (UV, brillo, ZIV): Verificar el brillo de la zona de inspección visual (ZIV) a la luz UV.
- **(UV, LU, FI)** → (UV, luminiscente, fibras): Verificar la presencia de fibras que sean luminiscentes a la luz UV.
- **(UV, LU, PS)** → (UV, luminiscente, perforación estática): Verificar si las trazas de una perforación estática son luminiscentes a la luz UV.
- **(UV, LU, TH)** → (UV, luminiscente, hilo): Verificar la presencia de un hilo de seguridad que sea luminiscente a la luz UV.

9. Las rutinas de verificación basadas en la característica AF no se enumeran explícitamente porque pueden combinarse con cada una de las fuentes de luz y propiedades ópticas mencionadas.

- **(VI, TR, TH)** → (VI, transparente, hilo): Verificar si el hilo de seguridad es transparente a la luz visible.
- **(VI, AB, PS)** → (VI, absorbente, perforación estática): Verificar si una perforación estática es visible a la luz visible.
- **(IR, AB, TH)** ° **(VI, TR, TH)** → (IR, absorbente, hilo) en combinación con (VI, transparente, hilo): Verificar si un hilo de seguridad, que es visible a la luz IR, es transparente a la luz visible.

Verificación de las propiedades de las técnicas de impresión: (8 BR + 2 CR)

- **(IR, AB, IS)** → (IR, absorbente, tinta estática): Verificar si la tinta de la impresión estática es absorbente a la luz IR.
- **(IR, TL, IS)** → (IR, translúcido, tinta estática): Verificar si la tinta del reverso de la página de datos (por lo general la página del título) es translúcida a la luz IR y puede detectarse en la imagen IR de la página de datos.
- **(IR, TR, IS)** → (IR, transparente, tinta estática): Verificar si la tinta de la impresión estática es transparente a la luz IR.
- **(UV, LU, IS)** → (UV, luminiscente, tinta estática): Verificar si la tinta de la impresión estática es luminiscente a la luz UV.
- **(UV, LU, OM)** → (UV, luminiscente, ZLM sobreimpresa): Verificar si la tinta de la impresión estática es luminiscente en la ZLM a la luz UV.
- **(UV, LU, OP)** → (UV, luminiscente, foto sobreimpresa): Verificar si la tinta de impresión estática es luminiscente en la zona de la foto a la luz UV.
- **(VI, AB, IS)** → (VI, absorbente, tinta estática): Verificar si la tinta de la impresión estática es absorbente a la luz visible.
- **(VI, TR, IS)** → (VI, transparente, tinta estática): Verificar si la tinta de la impresión estática es transparente a la luz visible.
- **(IR, TR, IS)** ° **(IR, AB, IS)** → (IR, transparente, tinta estática) en combinación con (IR, absorbente, tinta estática): Verificar si las partes de la impresión estática son absorbentes a la luz IR, mientras otras partes de la misma característica son transparentes a la luz IR.
- **(IR, TR, IS)** ° **(VI, AB, IS)** → (IR, transparente, tinta estática) en combinación con (VI, absorbente, tinta estática): Verificar si la tinta de la impresión estática es transparente a la luz IR y absorbente a la luz visible.

Verificación de las propiedades de personalización: (28 BR + 3 CR)

- **(IR, AB, ID)** → (IR, absorbente, tinta dinámica): Verificar si la tinta de la impresión dinámica es absorbente a la luz IR.
- **(IR, AB, MR)** → (IR, absorbente, verificación B900 de la ZLM): Verificar si la ZLM es visible a la luz IR.
- **(IR, AB, CA)** → (IR, absorbente, CAN): Verificar si el CAN es visible a la luz IR.
- **(IR, AB, BC)** → (IR, absorbente, código de barras): Verificar si el código de barras es visible a la luz IR.
- **(IR, AB, PD)** → (IR, absorbente, perforación dinámica): Verificar si una perforación dinámica es visible a la luz IR.

- **(IR, AB, PH)** → (IR, absorbente, foto): Verificar si la foto es visible a la luz IR.
- **(IR, FR, PH)** → (IR, frecuencia, foto): Verificar si el patrón tiene las características esperadas después de la transformación de la frecuencia espacial.
- **(IR, AB, SP)** → (IR, absorbente, foto secundaria): Verificar si la foto secundaria es visible a la luz IR.
- **(IR, TR, SP)** → (IR, transparente, foto secundaria): Verificar si la foto secundaria es transparente a la luz IR.
- **(IR, TR, ID)** → (IR, transparente, tinta dinámica): Verificar si la tinta de la impresión dinámica es transparente a la luz IR.
- **(IR, TR, PH)** → (IR, transparente, foto): Verificar la transparencia de la foto a la luz IR.
- **(UV, FR, PH)** → (UV, frecuencia, foto): Verificar si el patrón tiene las características esperadas después de la transformación de la frecuencia espacial.
- **(UV, LU, SP)** → (UV, luminiscente, foto secundaria): Verificar si la foto secundaria es luminiscente a la luz UV.
- **(UV, LU, BC)** → (UV, luminiscente, código de barras): Verificar si el código de barras es luminiscente a la luz UV.
- **(UV, LU, ID)** → (UV, luminiscente, tinta dinámica): Verificar si la tinta de la impresión dinámica es luminiscente a la luz UV.
- **(UV, LU, PD)** → (UV, luminiscente, perforación dinámica): Verificar si las marcas de una perforación dinámica son luminiscentes a la luz UV.
- **(VI, AB, ID)** → (VI, absorbente, tinta dinámica): Verificar si la tinta de la impresión dinámica es visible a la luz visible.
- **(VI, AB, MR)** → (VI, absorbente, ZLM): Verificar si la ZLM es visible a la luz visible.
- **(VI, AB, CA)** → (VI, absorbente, CAN): Verificar si el CAN es visible a la luz visible.
- **(VI, AB, BC)** → (VI, absorbente, código de barras): Verificar si el código de barras es visible a la luz visible.
- **(VI, TR, BC)** → (VI, transparente, código de barras): Verificar si el código de barras es transparente a la luz visible.
- **(VI, AB, PD)** → (VI, absorbente, perforación dinámica): Verificar si una perforación dinámica es visible a la luz visible.
- **(VI, AB, PH)** → (VI, absorbente, foto): Verificar si la foto es visible a la luz visible.
- **(VI, AB, SP)** → (VI, absorbente, foto secundaria): Verificar si la foto secundaria es visible a la luz visible.
- **(VI, TR, SP)** → (VI, transparente, foto secundaria): Verificar si la foto secundaria es transparente a la luz visible.
- **(VI, FR, PH**) → (VI, frecuencia, foto): Verificar si el patrón tiene las características esperadas después de la transformación de la frecuencia espacial.
- **(VI, AB, SP)** → (VI, absorbente, foto secundaria): Verificar si la foto secundaria es visible a la luz visible.
- **(VI, TR, ID)** → (VI, transparente, tinta dinámica): Verificar si la tinta de la impresión dinámica es transparente a la luz visible.

- **(IR, TR, ID) (VI, AB, ID)** → (IR, transparente, tinta dinámica) en combinación con (VI, absorbente, tinta dinámica): Verificar si la tinta de la impresión dinámica es transparente a la luz IR, así como absorbente a la luz visible.

- **(IR, TR, SP)** ° **(VI, AB, SP)** → (IR, transparente, foto secundaria) en combinación con (VI, absorbente, foto secundaria): Verificar si la foto secundaria es transparente a la luz IR, así como absorbente a la luz visible.

- **(VI, TR, BC)** ° **(IR, AB, BC)** → (VI, transparente, código de barras) en combinación con (IR, absorbente, código de barras): Verificar si el código de barras es transparente a la luz visible, así como absorbente a la luz IR.

La siguiente rutina compuesta de verificación se define conjuntamente para las dos clases de inspección: impresión y personalización:

- **(IR, TR, IS)** ° **(VI, AB, IS)** ° **(IR, AB, ID)** → (IR, transparente, tinta estática) en combinación con (VI, absorbente, tinta estática) en combinación con (IR, absorbente, tinta dinámica): Verificar si la tinta de la impresión estática es absorbente a la luz visible y transparente a la luz IR. Además, un elemento impreso de forma dinámica es visible a la luz IR en la misma posición.

Las rutinas de verificación especificadas anteriormente no tienen la misma importancia desde el punto de vista de la inspección. Por ejemplo, el resultado de la rutina de verificación (VI, AB, ID) no tiene validez por sí solo. Sin embargo, adquiere una importancia crucial para la detección de falsificaciones cuando se combina con la rutina de verificación (IR, TR, ID).

Las propiedades o características específicas de las falsificaciones deberían incorporarse invirtiendo la lógica de las rutinas de verificación: p. ej., debería verificarse si este patrón (i.e. VI, TR, IS) está ausente en una configuración específica de fibras de seguridad de imitación.

En la tabla C-1 se ofrece un panorama general de la clasificación del sistema de rutina de verificación genérica. Los tres componentes de los identificadores de las rutinas –característica, fuente de luz y propiedad – se agrupan en una matriz. El contenido de las filas, columnas y celdas describe una rutina básica de verificación genérica. Las clases de inspección asignadas se marcan mediante los colores verde (material), azul (técnica de impresión) y amarillo (personalización).

Tabla C 1. Representación por matriz de las rutinas básicas de verificación genéricas. Las propiedades ópticas se abrevian de la siguiente manera: AB – absorbente, propiedad de la tinta; BR – brillo, propiedad del sustrato; FR – frecuencia espacial, propiedad de los patrones; LU – luminiscente, propiedad de los patrones; TL – translúcida, propiedad de la tinta que brilla a través del sustrato; TR – transparente, propiedad de las clases de inspección de tinta se marcan mediante los colores verde (material), azul (técnica de impresión) y amarillo (personalización).

Elemento		*Fuente de luz*		
		VI	*UV*	*IR*
Fibras	FI		LU	
Página de datos completa	FU		BR	
Elemento de impresión estático	IS	{AB. TR}	LU	{AB, TR, TL}
ZLM	MR	AB	BR	AB
ZLM sobreimpresa	OM		LU	
CAN	CA	AB		AB
Código de barras	BC	{AB, TR}	LU	AB
Perforación personalizada (dinámica)	PD	AB	LU	AB
Perforación en el sustrato (estática)	PS	AB	LU	AB
Foto	PH	{AB, FR}	{BR, FR}	{AB, FR, TR}
Foto secundaria	SP	{AB, TR}	LU	{AB, TR}
Foto sobreimpresa	OP		LU	
Hilo de seguridad	TH	TR	LU	AB
Zona de inspección visual, ZIV	VZ		BR	
Filigrana	WM			AB
Característica “dinámica” personalizada	ID	{AB, TR}	LU	{AB, TR}
Característica adicional	AF	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}

C.4 RECOMENDACIONES PARA LA AUTENTICACIÓN MECÁNICA DE LOS MRTD

En el proceso de autenticación mecánica automatizada intervienen los siguientes componentes clave: el documento, el lector de página completa y el programa informático de autenticación (incluida la base de datos de autenticación, véase la sección C.2.2). Sin embargo, por lo general estos componentes se diseñan/fabrican sin tener en cuenta sus interdependencias, especialmente con respecto al diseño del documento de seguridad. Para que se pueda realizar una autenticación mecánica óptima, es crucial que estos componentes interactúen entre sí a la perfección.

En las siguientes secciones se ofrecen recomendaciones para el diseño eficiente y efectivo del documento (véase la sección C.4.1), el lector de página completa (véase la sección C.4.2), el programa informático de autenticación (véase la sección C.4.3), la base de datos de autenticación (véase la sección C.4.4) y la base de datos de referencia (véase la sección C.4.5). En la sección C.4.6, las recomendaciones formuladas en las secciones anteriores se asocian a hipótesis de uso tipo con el fin de ayudar a la dirección de operaciones[10] a planificar el funcionamiento de los sistemas de autenticación óptica.

Al analizar las recomendaciones para los diferentes componentes, deberían respetarse las diferencias entre los plazos habituales al hacer referencia a los cambios que deben hacerse:

- programa informático del sistema de inspección: 1 a 12 meses
- equipo informático de inspección: 3 a 5 años
- documento de seguridad: 10 a 20 años (resultante de un período de expedición habitual de 5 a 10 años y un período de validez de 5 a 10 años)

C.4.1 Diseñadores de documentos

Para diseñar un documento con elementos ópticos lo más seguros posible, la inspección humana no debería ser el único objetivo de un/a diseñador/a de documentos. Los elementos de seguridad que ofrece el documento también deberían ser aplicables a la autenticación mecánica. Además del diseño de base de los MRTD, de conformidad con el Doc 9303 de la OACI, en las siguientes secciones se resumen los elementos adecuados para la autenticación mecánica. Además, en las secciones que siguen se resumen también los elementos que –aun cuando tengan valor para la inspección humana– pueden reducir la eficacia de la autenticación mecánica (véase la sección C.4.1.2). En el contexto de la autenticación mecánica se alude a estos elementos como elementos que “podrían interferir”. Los/as diseñadores/as de documentos no deberían renunciar a incluir estos elementos en un documento, sino que deberían considerar la posibilidad de incluirlas, teniendo presente al mismo tiempo su posible impacto (negativo) en el proceso de autenticación mecánica.

C.4.1.1 Elementos adecuados para la autenticación mecánica

A continuación se enuncian varias recomendaciones sobre los elementos adecuados para la autenticación mecánica. Estos elementos se han seleccionado porque se detectan fácilmente en las imágenes VI, IR y UV, pero al mismo tiempo porque dificultan considerablemente la labor de falsificación.

10. Dirección de operaciones: Organización encargada de la administración y gestión de todos los procesos relacionados con el funcionamiento de la infraestructura de autenticación. Se encarga de establecer y mantener los canales de comunicación con los proveedores/fabricantes de los productos utilizados en el sistema de autenticación final.

A.1 **Definir unos elementos de identificación sin ambigüedades**: En determinados países es una práctica habitual sacar modelos de documentos sucesivos en un período de tiempo relativamente corto con el fin de mejorar las propiedades de la seguridad de sus MRTD. Los modelos de pasaporte británico (GBR, P, 1, 2008) y (GBR, P, 2, 2010) son un buen ejemplo de modelos de documentos sucesivos. Así pues, es preciso que, durante el proceso de diseño de un documento, se definan características que permitan la identificación sin ambigüedades del modelo de documento (p. ej., código de barras[11] asociado a un modelo de documento específico).

A.2 **Definir los elementos con las tres fuentes de luz**: Si bien es un elemento habitual de los lectores de página completa captar imágenes con las tres fuentes de luz, la experiencia sobre el terreno ha demostrado que a las personas que hacen falsificaciones les resulta muy difícil reproducir adecuadamente elementos que se vean de forma genuina con más de una de estas fuentes de luz. Así pues, es preciso que la definición de los elementos de seguridad óptica con las tres fuentes de luz (VI, IR y UV) aumente significativamente el esfuerzo necesario para hacer falsificaciones.

A.3 **Definir los elementos en tres categorías**: Proporcionar una distribución equilibrada de los elementos de seguridad en las clases “material”, “técnica de impresión” y “personalización” también aumenta el esfuerzo de falsificación necesario. Así pues, los elementos deben definirse en cada clase de conformidad con el Doc 9303 de la OACI.

A.4 **Definir los elementos en ambos lados de las tarjetas de identidad**: Las tarjetas de identidad de tamaño ID-1 pueden colocarse en un lector de página completa por ambos lados. Por tanto, los/as diseñadores/as de documentos diseñarán tarjetas de identidad de tamaño ID-1 con elementos de identificación y verificación en ambos lados para permitir la identificación y verificación independientemente del lado de la tarjeta.

A.5 **Definir elementos que reaccionan de forma diferente según las fuentes de luz**: Los elementos de documentos que reaccionan de forma diferente según la fuente de luz (véase la figura C-4), ayudan a reducir considerablemente la probabilidad de que se hagan buenas falsificaciones. Así pues, para la autenticación mecánica, se requiere utilizar elementos que puedan verificarse por su presencia y/o por su ausencia, dependiendo de la fuente de luz correspondiente (p. ej., tintas metaméricas, denominadas también división del espectro IR en la figura C-4, verificable por medio de una rutina (IR, TR, IS) (VI, AB, IS)).

11. Este ejemplo de uso del código de barras no contradice las recomendaciones del Doc 9303, Partes 9 y 10, para el almacenamiento electrónico de los datos biométricos.

Figura C-4. Pasaporte (CZE, P, 1, 2011): división del espectro IR en el texto del título

A.6 **Definir elementos con diferentes colores a la luz UV**: Los elementos de diferentes colores luminiscentes a la luz UV (véase la figura C-5) dificultan todavía más su reproducción, por lo que se recomienda utilizarlos. Al mismo tiempo, la paleta de colores de este elemento puede verificarse durante la autenticación mecánica, además de verificar la simple presencia de ese elemento. Se recomienda también usar colores que difieran significativamente con respecto a sus coordenadas de cromaticidad con el fin de facilitar la distinción por las máquinas. Las propiedades de luminiscencia de las tintas utilizadas tienden a degradarse, lo que aumenta aún más la dificultad de hacer una detección automática fiable.

Figura C-5. Pasaporte (GBR, P, 2, 2010): patrón UV con dos colores[12]

12. Fuente: http://edisontd.net/

A.7 **Definir patrones con contenido individual, p. ej., imagen facial secundaria**: Se recomienda definir patrones individuales que puedan verificarse por sus propiedades y compararse con contenido dinámico ya existente en la página de datos. Por ejemplo, una imagen facial secundaria puede compararse con la imagen facial primaria, y estas dos representaciones pueden tener propiedades espectrales iguales o diferentes. La lista de los patrones siguientes con las imágenes faciales secundarias tiene por objeto ilustrar esta recomendación, pero ni está completa ni pretende ser una recomendación explícita para estos elementos específicos:

a) La imagen facial secundaria como repetición más pequeña de la imagen facial que es visible a la luz visible y transparente a la luz IR (verificable por (VI, AB, ID) ° (IR, TR, ID)).

b) Tinta ópticamente variable (OVI) y dispositivo difractivo con imagen ópticamente variable (DOVID) que se han personalizado, p. ej., con grabado por láser o ablación por láser (véase la figura C-6). El ejemplo de elemento ilustrado en la figura C-6 muestra colores diferentes desde distintos ángulos de visión con luz visible (primera y segunda imágenes) y una imagen facial secundaria ligeramente visible al trasluz (tercera imagen). A la luz IR, la imagen facial secundaria puede captarse claramente y compararse con la imagen facial. El elemento es verificable mediante la siguiente rutina compuesta de verificación: (IR, AB, ID) ° (VI, AB, IS) ° (IR, TR, IS), que es una combinación triple.

c) Gabado láser personalizado que reacciona de forma opuesta (“negativa”) (véase la figura C-7). El ejemplo de elemento ilustrado en la figura C-7 puede captarse a la luz visible, donde muestra una imagen facial secundaria negativa bajo dos ángulos diferentes.

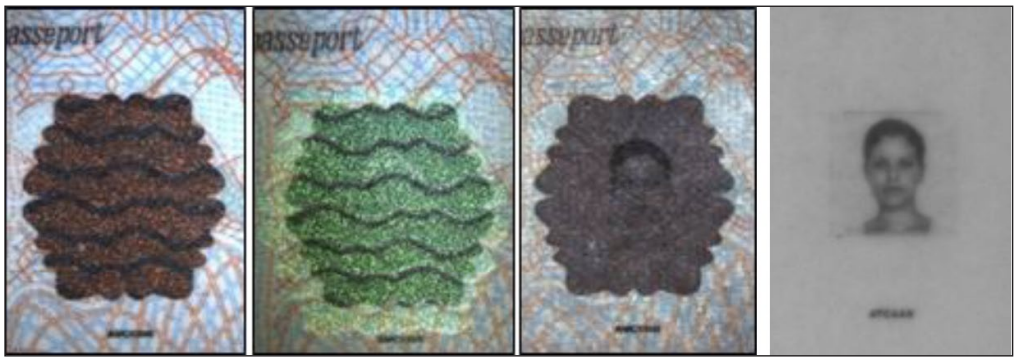

Figura C-6. Pasaporte (HUN, P, 1, 2006): OVI personalizada vista desde dos ángulos diferentes al trasluz y a la luz IR

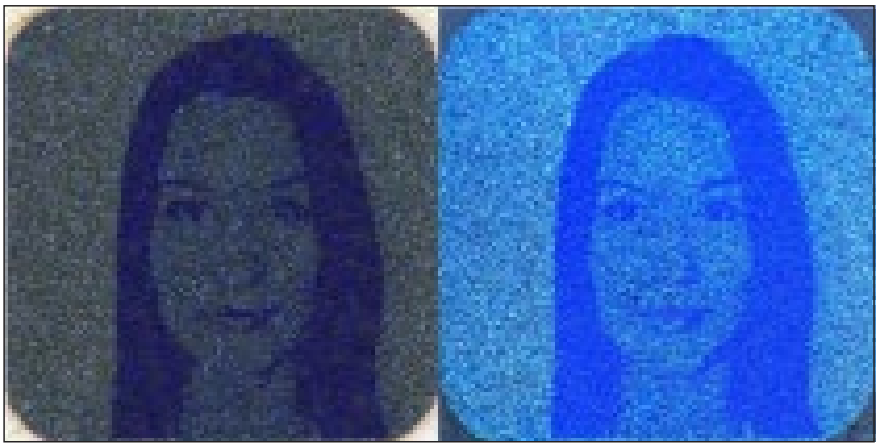

Figura C-7. Pasaporte (LVA, P, 1, 2015): Personalización "negativa" por medio de grabado por láser desde ángulos de visión diferentes a la luz visible

A.8 **Definir elementos que permanezcan estables a lo largo del período de validez del MRTD**: Algunos elementos tienden a desgastarse con el tiempo. Los colores de los patrones UV, por ejemplo, pueden perder intensidad a lo largo del período de validez del MRTD. Las colas superpuestas pueden hacer que los patrones UV pierdan considerablemente su nitidez con el tiempo, lo que puede dar lugar a resultados de verificación inexactos para el elemento. Por ello, se recomienda definir elementos que se mantengan lo más estables posible a lo largo del período de validez del MRTD.

A.9 **Definir una nacionalidad utópica para la persona titular de un documento de muestra**: A fin de establecer una forma normalizada de identificar los documentos de muestra, se recomienda establecer "UTO" como nacionalidad de la persona titular del documento para los documentos de muestra.

C.4.1.2 Elementos que pueden interferir en la autenticación mecánica

Esta sección trata de los elementos que pueden interferir en la autenticación mecánica (en el contexto mencionado al inicio de la sección C.4.1):

- **Elementos superpuestos**: Los elementos superpuestos que se definen sin tener en cuenta su interdependencia pueden interactuar negativamente bajo la influencia de una fuente de luz. Los efectos difractivos de un DOVID pueden interferir en la adquisición de la página de datos (véase la figura C-8).

Figura C-8. Pasaporte (AUT, P, 1, 2006): Laminado holográfico de seguridad con efectos ópticamente difractivos

- **Elementos cerca del borde superior del documento**: La experiencia sobre el terreno ha demostrado que los elementos ópticos cercanos al borde superior del documento (p. ej., en el caso de que haya un cuadernillo) pueden interferir en la autenticación mecánica y pueden suponer un corte de la zona captada. Una captura parcial de ese elemento podría provocar errores.

- **Elementos visibles únicamente con alta resolución**: En la tecnología actual, la mayoría de los lectores existentes de página completa que se usan en los sistemas de autenticación ofrecen una resolución nominal máxima de 400 píxeles por pulgada (ppp) con resoluciones ópticas reales que son incluso inferiores a ese valor. Los elementos que solo son visibles con una alta resolución de más de 400 ppp (p. ej., microtexto, guilloches) siguen sin ser detectables para la mayoría de los lectores de página completa actualmente disponibles en el mercado (véase la figura C-9). Sin embargo, quizás en un futuro próximo estos elementos sean verificables por los lectores de página completa con 600 ppp o más.

Figura C-9. Pasaporte (D, P, 1, 2017): Comparación entre una imagen de alta resolución del microtexto (1000 ppp) y una imagen del mismo microtexto tomada de un lector de página completa (resolución nominal 400 ppp)

- **Elementos para los que la apariencia depende del manejo individual**: Algunos elementos no son potencialmente adecuados a la autenticación mecánica porque pueden modificar considerablemente la apariencia del documento, i.e. en función de cómo se sitúe la página en el lector de documentos, el contenido de la imagen real es más o menos diferente. A continuación se mencionan dos de esos elementos a modo de ejemplo:

    a) *Ventana transparente*: En función de cómo se coloque la página de datos y la cubierta en el lector de documentos se puede ver el contenido de la cubierta a través de la ventana, la carcasa del lector, la yema del dedo o el contenido de la ventana está vacío (véase la figura C-10), provocando una luz incidente.

    Una ventana monofaz en tarjetas de identidad de tamaño ID-1, i.e. un elemento que puede verse solamente desde la parte frontal es más adecuado para la autenticación mecánica porque el contenido de la ventana no varía tanto como en la figura C-10 y no obstruye el proceso de verificación en el reverso de la tarjeta.

    b) *Lámina transparente superpuesta de página completa*: Estas hojas pueden dar diferentes resultados en función de su presencia (o ausencia) durante el proceso de captura de la imagen (véase la figura C-11).

    Las dificultades relacionadas con el uso de estos elementos pueden superarse proporcionando la instrucción adecuada a la persona operadora (en el caso de la inspección de documentos con asistencia humana) o la orientación de las personas usuarias (p. ej., para el control fronterizo automatizado).

- **Páginas de visado adicionales**: Los pasaportes a los que se añaden páginas de visado adicionales pueden llegar a ser demasiado gruesos para las dimensiones de los lectores normales de página completa.

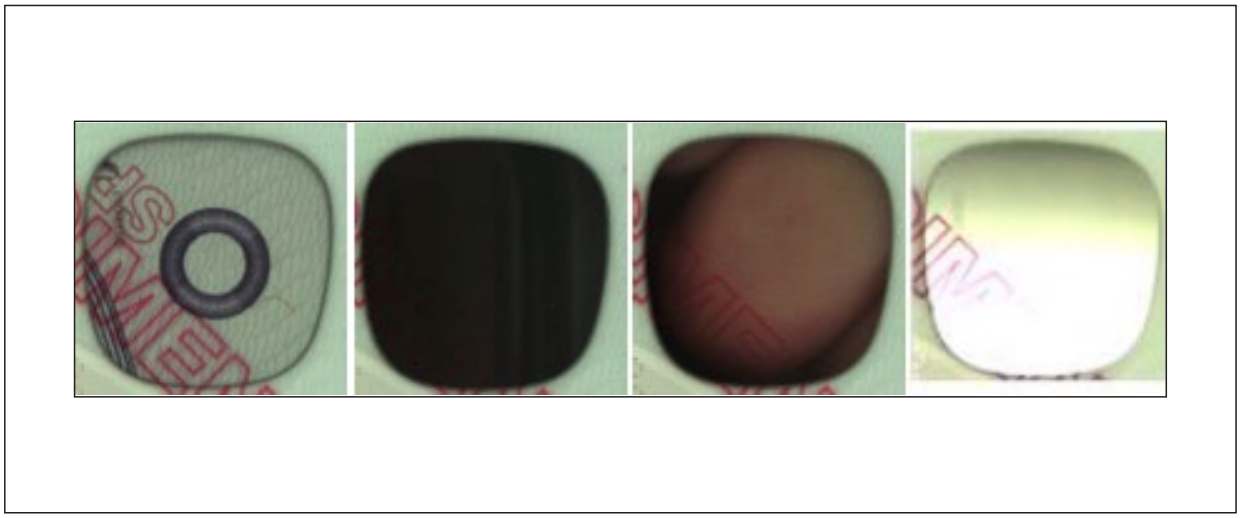

Figura C-10. Pasaporte (SWE, P, 1, 2012): Ventana con contenido variable; de izquierda a derecha: cubierta frontal interior; carcasa del lector; yema del dedo; reflejo provocado por la luz incidente

Figura C-11. Pasaporte (BEL, P, 1, 2008); izquierda: página de datos normal; derecha: página de datos con una lámina transparente superpuesta para inspección visual

C.4.2 Fabricante de lectores de página completa

La fiabilidad de un proceso de autenticación no solo depende del conjunto de funciones que ofrece el lector de página completa utilizado en el proceso; un manejo práctico y fácil del lector de página completa empleado también tiene un impacto directo en la calidad de las imágenes transmitidas al programa informático de autenticación (véase la sección C.4.3) y, por consiguiente automáticamente influye en el resultado global del proceso de autenticación. Las recomendaciones genéricas formuladas en esta sección deberían tomarse en consideración en el proceso de diseño de los lectores de página completa:

B.1 **Longitudes de onda adecuadas del espectro de luz**: El registro de imágenes mediante el uso de longitudes de onda adecuadas es un requisito previo para que se pueda realizar un análisis apropiado de las propiedades/características ópticas. Por ejemplo, una característica que se supone que es transparente a la luz IR podría volverse visible en una imagen IR si la captura se hace con una longitud de onda inadecuada del espectro de luz correspondiente. Esto podría llevar a unos conjuntos de datos reales inexactos y, por lo tanto, a una interpretación equivocada de los resultados de la verificación óptica. Para registrar las imágenes de conjuntos de datos reales se necesitan las siguientes longitudes de onda para los espectros de luz correspondientes:

- VI: gama espectral de 400 – 700 nm
- IR: una longitud de onda en la gama de 850 – 950 nm[13]
- UV: 365 nm

Aun cuando algunos lectores de pasaportes admiten longitudes de onda UV más cortas (p. ej., 254 y 313 nm), esta tecnología todavía no está muy extendida, por lo que ya no se tratará en este documento.

B.2 **Garantía de una resolución mínima**: La calidad de los conjuntos de datos reales transmitidos al programa informático de autenticación, medidos en píxeles por pulgada (ppp), tiene un impacto directo en la exactitud del proceso de autenticación. La experiencia sobre el terreno ha mostrado que los conjuntos de datos reales tendrán una resolución mínima de 385 ppp [BSI-TR-03135], aunque muchas propiedades de la impresión de seguridad saldrían ganando con una resolución de adquisición de 600 ppp o mayor.

B.3 **Presentación de un formato estándar de las imágenes**: Los conjuntos de datos reales se presentarán en los formatos más comúnmente utilizados/aceptados). Algunos de los formatos que pueden utilizarse son los siguientes: BMP, JPG (incluido el JPG2000) y PNG.

B.4 **Captura de un tamaño de hasta ID-3**: El lector de página completa debería permitir la verificación de MRTD de todos los tamaños especificados en el Doc 9303. Así pues, la zona de captura debería ser adecuada hasta para los documentos de tamaño ID-3. Aunque el presente documento se centra en los lectores de página completa, debería tenerse presente que para ciertas solicitudes no se requiere la verificación de los MRTD de todos los tamaños, sino que solo hace falta que el lector de página completa escanee los documentos de un tamaño específico (p. ej., dispositivos móviles).

B.5 **Captura de todas las superficies con la misma calidad**: El lector de página completa podrá captar la página de datos completa con una calidad de imagen constante. Esto puede conseguirse, por ejemplo, mediante la iluminación homogénea de la superficie de captura.

13. Este valor se ha sacado de las recomendaciones formuladas en el Doc 9303, Parte 3.

B.6 **Tiempo de respuesta breve e intensidad constante**: La fuente de luz utilizada para la captura deberá tener un tiempo de respuesta breve y proporcionará una intensidad de luz constante ya que todo deterioro de la luz durante el proceso de autenticación podría generar conjuntos de datos reales inadecuados.

B.7 **Calidad de la imagen constante**: Las fuentes de luz de los lectores de página completa del mismo tipo podrían emitir luz de forma diferente debido a desviaciones relacionadas con la producción. Además, estas fuentes de luz de un lector de página completa pueden cambiar de intensidad con el tiempo. Por tanto, el lector de página completa dispondrá de funciones que ayuden a compensar las desviaciones, proporcionando así una calidad de imagen constante a lo largo del tiempo e independiente del dispositivo concreto que se utilice. A continuación se brindan dos ejemplos para ilustrar cómo puede aplicarse esta recomendación:

a) El fabricante ofrece funciones para realizar la gestión del color y una calibración adicional (p. ej., por medio de una tarjeta de calibración) y adapta los parámetros del lector de página completa (p. ej., brillo, tiempo de exposición).

b) El fabricante incorpora sensores al lector que permiten la compensación automática de las desviaciones.

B.8 **Ajuste de la exposición de la luz UV por medio del programa informático de autenticación**: Por lo general, los distintos modelos de documentos requieren una exposición a la luz UV diferente para poder iluminar el documento de forma óptima. En este caso, la información sobre la exposición a la luz UV se almacena en la base de datos de autenticación. Así pues, el lector de página completa deberá permitir el ajuste de la exposición de la luz UV por medio del programa informático de autenticación mediante la transmisión de los datos sobre la configuración UV almacenados en la base de datos de autenticación (véase la sección C.4.4.2, punto D.8.).

B.9 **Captura de múltiples imágenes UV**: El lector de página completa debería poder admitir múltiples imágenes captadas con diferentes configuraciones de exposición, p. ej., para una combinación de características UV que muestran un marcado contraste de luminiscencia (p. ej., gama de gran dinamismo).

B.10 **Imágenes sin reflejos**: En la imagen captada pueden aparecer reflejos que, a menudo, cubren datos personales o características de seguridad de la página de datos. Por consiguiente, las imágenes obtenidas del lector de página completa deberían tener el menor reflejo posible. Esto puede lograrse captando múltiples imágenes de luz visible (blanca) desde diferentes ángulos o utilizando una iluminación difusa.

B.11 **Mecanismo para presionar el documento y que quede plano en la zona de captura**: Como se indicó anteriormente, la sencillez de uso del lector de página completa influye directamente en la eficiencia y la velocidad del proceso de autenticación. Por tanto, el lector de página completa debería ofrecer mecanismos que ejerzan una presión mecánica sobre el documento de modo que quede plano en la ventana y se puedan captar imágenes adecuadas de las páginas del documento.

B.12 **Funcionamiento con una sola mano**: Además, debería ser posible manejar el lector con una sola mano y el proceso de lectura debería ser simétrico de modo que lo puedan utilizar tanto personas diestras como zurdas.

B.13 **Orientación interactiva para el público usuario**: La orientación interactiva para el público usuario no solo hace que el uso de los lectores de documentos resulte más cómodo para ese público usuario, sino que también ayuda a reducir significativamente la duración de todo el proceso de autenticación. La orientación para el público usuario es crucial, especialmente en los puestos de control fronterizo automatizado (ABC), que generalmente son de autoservicio: al revés que en el control estacionario de documentos, el equipo informático de autenticación de documentos lo usan las propias personas titulares del documento. Por ello, el lector de documentos debería ser capaz de proporcionar orientación interactiva al público usuario. Ello

puede hacerse, por ejemplo, facilitando una transmisión en directo del documento situado en la superficie de captura que indique la progresión de la captura de la imagen (p. ej., metáfora del escáner). De esa forma, a la persona usuaria le llega información directa y puede darse cuenta mucho más rápido de si el documento está colocado correctamente en el lector.

B.14 **Equipo informático con un alto grado de solidez**: En función del lugar en que se encuentren, los lectores de página completa están sujetos a diversos factores externos (manejo indebido, humedad, etc.). Con el tiempo, esos factores externos pueden llegar a dañar en mayor o menor grado componentes fundamentales (p. ej., arañazos en la superficie de captura) del lector de página completa, acelerando así el desgaste o, incluso, la rotura del dispositivo. Por eso, se recomienda equipar el lector de página completa con componentes informáticos sólidos.

C.4.3 Fabricante de programas informáticos de autenticación

Las siguientes propuestas toman como modelo la orientación técnica [BSI-TR-03135] de la Oficina Federal de Seguridad de la Información (BSI), ya que actualmente es la única solución que se ofrece al sector público en este ámbito. Se recomienda encarecidamente aplicar el programa informático de autenticación de conformidad con esta orientación. Las ulteriores recomendaciones deberían entenderse como una extensión de la orientación [BSI-TR-03135].

Conviene tener en cuenta las siguientes recomendaciones técnicas para el programa informático de autenticación:

C.1 **Procesamiento de imágenes previamente grabadas**: El programa informático de autenticación también trabajará sin equipo informático y debe ser capaz de procesar imágenes previamente grabadas (los requisitos mínimos para las imágenes se indican en la sección C.4.2, puntos B.1, B.2 y B.3). Esta función es especialmente importante para los procesos de evaluación automatizados. No obstante, es necesario impedir que el programa informático de autenticación procese imágenes previamente grabadas durante su funcionamiento normal, ya que eso puede utilizarse como vector potencial de ataques. Por lo tanto, el uso de la interfaz utilizada para procesar imágenes previamente grabadas debe restringirse a configuraciones específicas (p. ej., sistema de evaluación).

C.2 **Procesamiento de imágenes de diferentes fuentes de equipo informático**: El programa informático podrá procesar imágenes tomadas de, al menos, dos lectores de página completa diferentes sin degradación de los resultados de verificación. Por consiguiente, el fabricante del programa informático de autenticación proporcionará una especificación que describa las propiedades de las imágenes transmitidas a ese programa informático (espacio cromático, contraste, etc.).

C.3 **Abstracción de la GUI (interfaz gráfica de usuario) del programa y equipo informáticos de autenticación**: El proceso de autenticación óptica de un MRTD va acompañado, la mayoría de las veces, de la verificación electrónica del MRTD y de una verificación biométrica del rostro de la persona titular del documento y quizás también de la huella digital. Además, tienen que hacerse controles de antecedentes, p. ej., en el Sistema de Información de Schengen (SIS). Por ello, se recomienda utilizar una capa de abstracción entre la GUI y los componentes concretos del programa y equipo informáticos necesarios para las verificaciones de documentos, biometría y antecedentes. De esta forma, la GUI es independiente de esos componentes. Además, los componentes mencionados pueden intercambiarse fácilmente sin tener que cambiar la GUI.

En las siguientes secciones figuran recomendaciones para los fabricantes de programas informáticos de autenticación, que se estructuran de conformidad con los pasos ejecutados durante el proceso de autenticación. El documento debe detectarse (véase la sección C.4.3.1), identificarse (véase la sección C.4.3.2) y, posteriormente, verificarse (véase la sección C.4.3.3). Además, debe visualizarse el proceso completo (véase la sección C.4.3.4) y documentarse usando mecanismos de registro apropiados (véase la sección C.4.3.5).

C.4.3.1 Detección de documentos

Para la detección de documentos colocados en la superficie del lector, se brindan las siguientes recomendaciones:

C.4 **Detección automática y manual de documentos**: El programa informático de autenticación proporcionará mecanismos para la activación automática y manual de la detección de documentos. La activación del mecanismo manual es especialmente decisiva en el caso de que la detección automática de documentos no funcione correctamente.

C.5 **Compensación de la rotación y consiguiente recorte de la página de datos captada**: La captura de la imagen se inicia automáticamente una vez que se ha colocado la página completa de datos personales en la superficie de captura. El programa informático de autenticación podrá compensar la rotación potencial y realinear la imagen automáticamente. Además, la autenticación permitirá el correspondiente recorte de la página de datos captada para su ulterior procesamiento.

C.6 **Detección del documento sobre la base de su presencia óptica**: La presencia de un documento se detectará únicamente utilizando sus propiedades ópticas. El proceso de detección seguirá haciéndose de forma óptica, aun cuando una microplaqueta que estaba prevista falte o funcione mal (véase la sección C.1.3).

C.4.3.2 Identificación

Un requisito previo para la verificación de documentos es la correcta identificación del modelo de documento. Se brindan las siguientes recomendaciones para la identificación de un conjunto de datos reales:

C.7 **Identificación del modelo de documento**: Es necesario identificar el modelo de documento, independientemente de los métodos aplicados, siempre que el método aplicado garantice una correcta identificación del modelo de documento. Los métodos más comunes empleados para la identificación de modelos de documentos son la ZLM (incluido el análisis de patrones) o el análisis de patrones solamente.

C.8 **Identificación rápida por medio de la ZLM**: Si la ZLM se usa como información primaria para la identificación de modelos de documentos, el programa informático de autenticación debería aplicar métodos y rutinas que permitan un rápido proceso de identificación. A continuación se brindan dos ejemplos para ilustrar cómo puede llevarse a la práctica esta recomendación:

a) empezar con la captura de la imagen IR con el fin de extraer la ZLM y obtener el modelo de documento.

b) puesto que la generación de imágenes de resolución total puede requerir mucho tiempo, cabe la posibilidad de hacer una captura rápida de imagen IR para realizar un análisis inicial de la ZLM con una resolución menor que la mínima recomendada para la imagen IR utilizada con fines de identificación.

C.9 **Opción de reserva en caso de que la ZLM no sea legible a la luz IR**: La identificación inequívoca del modelo de documento debería poder hacerse por todos los medios, siempre que el documento lo permita. Aun cuando la ZLM no sea legible a la luz IR (no conforme a la OACI), el documento tiene que ser identificado correctamente. Por ello, el fabricante de programas informáticos debe prever soluciones de reserva como la realización del OCR en la imagen VI para el análisis de la ZLM si esta no se ha impreso utilizando tinta absorbente IR.

C.10 **Modelo de documento inequívoco**: El fabricante de programas informáticos debe proporcionar un enlace inequívoco al modelo de documento con el fin de permitir el acceso al conjunto de datos de autenticación de este modelo de documento en la base de datos de autenticación.

C.11 **Posibilidad de identificación parcial**: El programa informático de autenticación debería permitir que se configurase una identificación parcial con el fin de reducir considerablemente las tasas de identificación falsa y de no identificación. No obstante, la evaluación de la identificación parcial requiere la interacción humana y el conocimiento específico de los MRTD para seleccionar el modelo de documento correcto manualmente, por lo que no es adecuado para todo tipo de situaciones, p. ej., los puestos ABC.

C.12 **Posibilidad de identificación manual posible**: El sistema debería permitir la elección enteramente manual del modelo de documento –en lugar del proceso automático y/o anulando la elección de la máquina– para aquellos casos en que falle el proceso automático de identificación del sistema. Además, el sistema solo debería permitir la identificación manual en caso de que no pueda hacerse la identificación parcial. La identificación manual requiere la interacción humana y el conocimiento específico de los MRTD, por lo que no es adecuado para todo tipo de situaciones (p. ej., no resulta práctica para los ABC).

C.13 **Identificación de las tarjetas ID por ambos lados**: Los documentos de tamaño ID-1 son un caso especial en el sentido de que la ZLM no es la página de datos personales (en la que se muestra la imagen del rostro). Sin embargo, las tarjetas de identidad de tamaño ID-1 pueden colocarse en un lector de página completa por ambos lados. Así pues, los documentos de tamaño ID-1 deberían ser identificables por cualquier lado del documento (véase la recomendación A.4 en la sección C.4.1.1).

C.14 **Identificación de los documentos de muestra**: El programa informático de autenticación debería identificar también los documentos de muestra como tales e informar a la persona operadora en consecuencia, sin interrumpir el proceso de autenticación (véase la recomendación A.9 en la sección C.4.1.1).

En la sección C.4.3.4 pueden consultarse recomendaciones relativas a la visualización del procedimiento de identificación en la interfaz gráfica de usuario.

C.4.3.3 Verificación

A continuación se brindan recomendaciones para la verificación de documentos:

C.15 **Realización de un número mínimo de verificaciones espectralmente selectivas**: Deben realizarse rutinas de verificación espectralmente selectivas con el fin de verificar las reacciones absorbentes, reflectantes o luminiscentes de un conjunto de datos reales. Aun cuando un documento no pueda identificarse, deben realizarse las siguientes verificaciones obligatorias:

a) (IR, AB, MR): esta rutina de verificación, conocida también como prueba B900, puede realizarse sin la selección de un modelo de documento; y

b) (UV, BR, FU): con algunas restricciones sobre la exactitud, esta rutina de verificación también puede realizarse en conjuntos de datos reales no identificados.

Si se identifica el modelo de documento, se realizarán además las siguientes verificaciones espectralmente selectivas, complementarias de las mencionadas anteriormente (i.e. verificación de la propiedad óptica opuesta):

c) (IR, TR, ZZ): se realizará al menos una verificación que investigue la propiedad complementaria “transparente a la luz IR”, en comparación con (IR, AB, MR); y

d) (UV, LU, ZZ): se realizará al menos una verificación que investigue la propiedad complementaria “luminiscente a la luz UV”, en comparación con (UV, BR, FU).

C.16 **Verificación de la coherencia de la ZLM**: Además del número mínimo de verificaciones espectralmente selectivas, deben realizarse verificaciones de plausibilidad (p. ej., errores en la ZLM, código de tres letras de la OACI) de todos los documentos a fin de garantizar la seguridad mínima, incluso en el caso de la no identificación.

C.17 **Realización de verificaciones en todas las categorías**: El programa informático de autenticación efectuará rutinas de verificación en las tres categorías (material, técnica de impresión y técnica de expedición) y abarcará la captura de imágenes con las tres fuentes de luz (véase la recomendación A.3 para los/as diseñadores/as de documentos en la sección C.4.1.1).

C.18 **Verificación de la presencia de microplaquetas**: Si está prevista la existencia de una microplaqueta RF para un modelo de documento particular, que no funciona o parece que no existe, esto debe representar un aviso claro, además de los resultados ópticos (véase la sección C.1.3).

C.19 **Verificación de patrones dinámicos**: Se recomienda proporcionar algoritmos que comparen patrones dinámicos individuales (p. ej., foto, firma). Por ejemplo, la imagen del rostro podría compararse con una imagen facial secundaria situada en la página de datos (véanse la figura C-12 y la recomendación A.7 para los/as diseñadores/as de documentos en la sección C.4.1.1).

C.20 **Combinación de rutinas de verificación en caso necesario**: Algunos elementos pueden verificarse por medio de diferentes rutinas. Por ejemplo, los elementos que se comportan de modo distinto según la fuente de luz sirven como datos de entrada para rutinas separadas de verificación (véase la recomendación A.5 para diseñadoras/es de documentos de la sección C.4.1.1). Así pues, se recomienda combinar los resultados de tales rutinas de verificación de forma lógica o combinar la puntuación de las verificaciones por medio de una función de decisión. Por ejemplo, una rutina compuesta de verificación todavía podría obtener un resultado de aprobado, aun cuando la puntuación de una rutina básica de verificación esté ligeramente por debajo de su umbral.

C.21 **Realización de rutinas de verificación redundantes en múltiples posiciones**: Para los elementos que aparezcan más de una vez en el documento, la rutina de verificación correspondiente debería realizarse también en múltiples posiciones del conjunto de datos reales. Por ejemplo, para el modelo de documento (D, P, 1, 2007) de la figura C-13, el patrón del águila con luz UV puede verificarse en múltiples posiciones. Una rutina de verificación realizada en múltiples posiciones se denomina rutina de verificación redundante.

Además de las múltiples apariciones de un elemento, estadísticamente algunos elementos están más sujetos a la falsificación que otra. Por ejemplo, en muchos casos, las personas que hacen falsificaciones cambian la fecha de caducidad o sustituyen la imagen facial. Así pues, se recomienda que se hagan rutinas de verificación redundantes, que sean capaces de detectar ataques a estos elementos “sensibles”.

C.22 **Rutinas de verificación redundantes en múltiples colores bajo la luz UV**: Asimismo, se recomienda la ejecución de rutinas de verificación redundantes para las características bajo la luz UV, que aparecen en múltiples colores en el documento (véanse la recomendación A.6 y la figura C-5 para las/os diseñadoras/es de documentos en la sección C.4.1.1).

C.23 **Vinculación y verificación de ambas páginas de una tarjeta ID**: Un segundo escaneado de la página estará vinculado automáticamente al escaneado previo si ambos son del mismo documento ID. Además, se recomienda verificar ambos lados de los documentos de tamaño ID-1 con el fin de obtener un resultado de verificación global para ambos lados y de aumentar al máximo el número de elementos ópticos utilizados para la autenticación del documento (véase la recomendación A.4 para las/os diseñadoras/es de documentos en la C.4.1.1).

Figura C-12. Pasaporte (EST, P, 1, 2013): Verificar la imagen del rostro en la imagen de luz visible frente a la imagen impresa con tinta luminiscente UV

Figura C-13. Verificación redundante de patrones

C.24 **Verificación cruzada en múltiples páginas de los datos personales**: Los datos personales de la persona titular del documento deberían ser idénticos, independientemente de la página en la que aparezcan. Por ejemplo, se supone que los datos personales de la página de la libreta de un pasaporte son idénticos a los datos personales de un visado potencialmente existente. Por ello, se recomienda realizar verificaciones cruzadas de múltiples lados si, por ejemplo, se prevé que el contenido de carácter personal sea idéntico/redundante.

C.25 **Realización de rutinas de verificación en función de su importancia**: No siempre es necesario o útil realizar una serie completa de rutinas de verificación, simplemente porque sea técnicamente posible aplicarlas al conjunto de datos reales. Resulta más eficaz evaluar la relevancia de las verificaciones en relación con el proceso de verificación. Con determinadas rutinas de verificación existen más posibilidades de obtener resultados útiles que con otras y de obtener información que permita un análisis más exacto de los resultados de verificación. Así pues:

a) las verificaciones deberían realizarse por orden de relevancia/importancia y mostrarse sus resultados inmediatamente en la interfaz gráfica de usuario (véase la visualización en la sección C.4.3.4); y

b) los resultados de las verificaciones deberían ser combinables mediante funciones de decisión distintas de la sola realización de una simple combinación lógica con Y (i.e. uso de resultados de verificación ponderados). Las funciones de decisión tienen que incluirse en el catálogo XML (véase la recomendación C.46 sobre el registro en la sección C.4.3.5).

C.26 **Consideración de la degradación de los elementos**: Los elementos de seguridad pueden ir desvirtuándose con el tiempo debido al desgaste natural del MRTD, p. ej., algunos colores UV pueden degradarse. Sin embargo, para poder verificar un MRTD es preciso que la fiabilidad de estos elementos se mantenga constante a lo largo de todo el período de validez del documento. Por ello, debería considerarse la posibilidad de las tolerancias de las rutinas de verificación.

C.27 **Detección de ataques genéricos**: Además de la pura verificación de las propiedades de los elementos del documento, el programa informático de autenticación debería proporcionar herramientas para la detección de trazas de ataques genéricos, tales como el “daño del papel”, “marcas de corte”, “sustitución de la fotografía” o “arrugas en el laminado” si las condiciones de iluminación lo permiten. El esquema de las rutinas de verificación genéricas también puede aplicarse a las verificaciones para detectar falsificaciones.

En la próxima sección pueden encontrarse recomendaciones relativas a la visualización del procedimiento de verificación en la interfaz gráfica de usuario.

C.4.3.4 Visualización

La visualización de los resultados de autenticación es el proceso por el que se facilita a la persona usuaria del sistema de autenticación retroinformación visual e información sobre los resultados del proceso de autenticación. La visualización debería realizarse en forma de interfaz gráfica de usuario (forma abreviada: GUI).

La GUI para la visualización de los resultados de las verificaciones ópticas debería proporcionar a la persona usuaria únicamente la información más relevante con el fin de determinar las irregularidades a primera vista. Esta información se divide en la denominada “zona de resumen del proceso” (véase C.29), la denominada “zona de vista general óptica” (véase C.30) e información más detallada en la denominada “zona de detalles ópticos” (véase C.35).

A continuación se indican recomendaciones para seleccionar la información admisible y mostrarla de forma compacta y minimalista:

C.28 **Presentación de todas las verificaciones del documento en una GUI**: La GUI puede formar parte integrante del programa informático de autenticación suministrado o bien suministrarse y ejecutarse en una capa de abstracción separada. Independientemente de esto, se recomienda presentar todos los tipos de verificaciones realizadas (electrónicas, biométricas, ópticas y de antecedentes) en una GUI. Esto reduce considerablemente el esfuerzo que ha de realizar la persona operadora del sistema y facilita la evaluación de los resultados de la verificación gracias a un mejor panorama general del proceso. Además, habría que prestar especial atención a la aparición de anomalías o irregularidades (véanse las recomendaciones C.41 a C.45).

C.29 **Visibilidad obligada de la *zona de resumen del proceso***: Esta zona debería mostrar el resultado global de la autenticación óptica y debe mostrarse a la persona usuaria en la página de inicio (véase un ejemplo de GUI de control fronterizo estacionario en la figura C-14). Esta zona siempre debería ser visible para la persona usuaria, independientemente de otros detalles seleccionados en los resultados de verificación específicos. La zona de resumen del proceso debería mostrar un resultado global de la autenticación óptica con los códigos de color de un semáforo. Además, la zona debería mostrar una imagen facial recortada de la página de datos situada al lado de la imagen facial almacenada en la microplaqueta, si existe.

C.30 **Muestra de la *zona de vista general óptica* en la página de inicio**: Esta zona muestra una vista general de las rutinas de verificación óptica y debería mostrarse a la persona operadora en la página de inicio.

a) Esta zona debería contener la siguiente información (véase la figura C-14):

- La imagen VI (luz visible) del documento por defecto. El personal operador debería poder cambiar la imagen preestablecida a IR o UV, en función de los requisitos específicos.
- Los datos personales de la persona titular del documento contenidos en la ZLM: apellido(s), nombre, fecha de nacimiento, sexo, nacionalidad y datos opcionales.
- Los datos del documento: tipo de documento, número de documento, Estado expedidor u organización expedidora, fecha de caducidad y datos opcionales.
- La ZLM extraída para que esta se pueda comparar con la ZLM impresa en el documento.
- Un botón para permitir la activación manual del proceso de lectura del documento.
- Una imagen facial recortada de la página de datos situada al lado de la imagen facial almacenada en la microplaqueta, si existe, (véase la sección C.1.3) para que se pueda detectar fácilmente la sustitución de la foto.

b) Se recomienda también presentar la siguiente información en la zona de vista general óptica:

- La edad de la persona titular del documento, así como el período de validez restante. La persona operadora puede reconocer esta información de forma más fácil y rápida que las fechas contenidas en la ZLM.

C.31 **Selección de más detalles mediante un clic**: Desde la zona de vista general óptica, a la persona operadora debería bastarle un clic para tener acceso a una página adicional que contenga más detalles de la verificación óptica: la zona de *detalles ópticos* (véase C.35). Por ejemplo, si se considera la GUI de la figura C-14, pueden conseguirse más detalles haciendo clic en la zona “Datos del documento”.

Figura C-14. Ejemplo de página de inicio para una GUI de control fronterizo estacionario

C.32 **Presentación de los resultados con los colores del semáforo**: Según lo especificado en [BSI-TR-03135], los resultados de los procesos de verificación óptica deberían mostrarse utilizando el sistema de colores de un semáforo (p. ej., luces de color rojo/verde /amarillo/gris). Además del color, los semáforos deberían contener símbolos inequívocos que indiquen los resultados de la verificación (p. ej., verificación, cruce). Esto es especialmente importante para las personas usuarias que sean daltónicas. Además, el esquema de representación debería ser el mismo para todas las zonas de la GUI (p. ej., todos los resultados negativos se muestran con el mismo símbolo y color).

C.33 **Correspondencia de los resultados acorde con [BSI-TR-03135]**: El sistema del semáforo debería proporcionar una correspondencia coherente con los siguientes resultados de verificación: **éxito**, **fracaso**, **indeterminado** y **no apoyado/no realizado**, definidos en [BSI-TR-03135]. En la Tabla C-2 figura una visión global de la correspondencia utilizada en este documento. Esta correspondencia se basa en [BSI-TR-03135] y debería utilizarse para las implementaciones prácticas de la GUI.

Tabla C-2. Correspondencia mediante el sistema de colores del semáforo

Resultado de verificación	*Color del semáforo*
Éxito	verde
Fracaso	rojo
Indeterminado	amarillo
No apoyado/no realizado	gris
Suspendido	negro

C.34 **Correspondencia minimalista para los resultados**: Otra posibilidad para el sistema del semáforo es utilizar una correlación minimalista que emplee únicamente los colores verde y rojo. Como se indica en la tabla C-3, el color verde puede usarse para mostrar un resultado de verificación positivo, en el que el color rojo puede usarse para mostrar cualquier otro resultado de verificación.

Tabla C 3. Correspondencia minimalista mediante el sistema del semáforo

Resultado de verificación	*Color del semáforo*
Éxito	verde
Fracaso Indeterminado	rojo
No apoyado/no realizado	gris
Suspendido	

Una reducción todavía mayor de la correlación consistiría en mostrar las cuatro últimas verificaciones de la tabla C-3 en rojo.

C.35 **Presentación de la información detallada en una *zona de detalles ópticos* específica**: La vista de la información detallada solo está disponible cuando se amplía la zona y se trata de información relativa a los diferentes procesos y resultados de la autenticación óptica. Tiene por objeto proporcionar a la persona usuaria la información necesaria para realizar más análisis en caso necesario.

a) La zona de información detallada óptica debería contener los siguientes datos (véase el ejemplo de la figura C-15):

- La imagen VI, IR y UV del documento. Las tres imágenes deberían presentarse juntas.

Figura C-15. Ejemplo de presentación de zona de detalles ópticos

- El identificador del modelo de documento patentado del fabricante del programa informático de autenticación, si el identificador del modelo de documento propuesto en la sección C.2.1 no puede mostrarse de forma genérica.

- Una lista de rutinas de verificación seleccionadas, que muestren sus resultados por medio del código de colores del semáforo: En el contexto del control fronterizo, al guardia de control fronterizo debería aparecerle únicamente la información de verificación más importante, presentada en una versión legible por el ser humano. Así pues, los resultados de las rutinas de verificación genéricas se resumen en tres categorías, descritas por medio de términos sencillos y comprensibles, de la siguiente manera:

  — ZLM legible en IR: El semáforo correspondiente muestra el resultado de la rutina de verificación genérica (IR, AB, MR).

— brillo UV: El semáforo correspondiente muestra el resultado combinado de las rutinas de verificación genéricas (UV, BR, FU), (UV, BR, VZ), (UV, BR, PH) y (UV, BR, MR).

— verificación del patrón: El semáforo correspondiente muestra el resultado combinado de las rutinas de verificación genéricas restantes que se han llevado a cabo para este documento (véase la sección C.3).

- Además, los resultados de las siguientes verificaciones, obligatorias de conformidad con [BSI-TR-03135], deberían visualizarse mediante el sistema del semáforo:

  — coherencia de la ZLM

  — fecha de caducidad

- la ZLM extraída.

- durante el proceso de autenticación, los datos extraídos de la ZLM de lectura óptica se comparan con los elementos de la ZLM almacenados en la microplaqueta (en caso de disponibilidad). Los datos de la ZLM óptica deberían mostrarse junto con el o los resultados de esta comparación. Los resultados deberían mostrarse utilizando el mismo sistema de colores del semáforo empleado en toda la GUI.

b) Se recomienda asimismo mostrar la siguiente información en la zona para detalles ópticos:

- modelo de documento identificado en formato legible por el ser humano, p. ej., D 2007. Utilizar el identificador del modelo de documento estándar de [BSI-TR-03135] probablemente podría confundir más que aclarar a las personas usuarias de la GUI. Por tanto, la representación del identificador del modelo de documento en la GUI debería especificarse sobre la base de un acuerdo común con la persona operadora del sistema de autenticación.

- tanto los datos extraídos de la ZLM de lectura óptica como los extraídos de la microplaqueta deberían mostrarse juntos (véase la sección C.1.3).

C.36 **Orientación al público usuario durante la lectura del documento**: Durante el proceso de lectura tiene que darse a la persona usuaria una indicación para que no retire el documento antes de que se haya completado el proceso de lectura (véase la recomendación B.13 en la sección C.4.2). Una forma de hacerlo podría ser mediante un indicador de proceso que aparezca durante el proceso de lectura. Tal indicador puede colocarse encima de la zona de resumen del proceso.

C.37 **Presentación de la información de bases de datos centrales**: Si el proceso de autenticación requiere que se consulte a un sistema de bases de datos de antecedentes, la página de detalles ópticos puede mostrar la información extraída de ese sistema si está correlacionada con la autenticación óptica, p. ej., la imagen facial recuperada del sistema central de información de visados (C-VIS).

C.38 **Configuración homogénea de los MRTD**: La configuración de la GUI debería ser la misma para todos los tipos de documentos de lectura mecánica (p. ej., pasaportes, tarjetas de identidad nacionales, permisos de residente, etc.). Por ejemplo, la información de autenticación óptica obtenida de ambos lados de una tarjeta de tipo ID-1 debería mostrarse de modo análogo a la visualización de la verificación de pasaportes (una zona de zona de resumen del proceso, una zona de vista general óptica y una zona de detalles ópticos).

C.39 **Orientación a la persona operadora a lo largo del proceso de verificación multipáginas**: Para la verificación de ambos lados de un documento de tamaño ID-1, la persona usuaria necesita orientación interactiva. Cuando se coloque una tarjeta en la superficie de captura, la persona usuaria debería recibir una indicación, que apunte a que el siguiente paso podría consistir en presentar la segunda página.

C.40 **Comparación del contenido del pasaporte y el visado/permiso de residencia electrónico (eRP)**

a) *Orientación a la persona operadora a lo largo del proceso de verificación multipáginas*: Durante la verificación de un pasaporte, es preciso que la persona usuaria quede advertida de que la persona titular del pasaporte necesita un visado/eRP para poder cruzar la frontera. Esto puede hacerse, por ejemplo, mediante un aviso que aparezca en la página de vista general. Ese aviso debería ser una indicación para la persona usuaria de que la presentación del visado/eRP en el lector de página completa puede ser el siguiente paso.

b) *Mantener la información del pasaporte disponible*: Durante la autenticación del visado óptico/eRP, las zonas de vista general y de detalles que muestran los resultados de la autenticación del pasaporte deben seguir estando disponibles para que se pueda acceder a esos detalles si se desea.

c) *Posibilidad de comparación en la zona de resumen del proceso*: Además de la imagen facial capturada ópticamente de la página de datos, debería aparecer la imagen facial del visado/eRP (véase el ejemplo de la figura C-16). Deberían aparecer también la imagen de la persona titular del pasaporte almacenada en la microplaqueta (si está disponible, véase la sección C.1.3) y la imagen recuperada de un sistema de consulta de información sobre visados (p. ej., Sistema de Información de Visados (VIS) de la Unión Europea) o de la microplaqueta del eRP (véase C.37).

d) *Posibilidad de comparación en la zona de detalles ópticos del visado*: Durante el proceso de autenticación, los datos sobre apellido(s), nombre, fecha de nacimiento, sexo y nacionalidad extraídos de la ZLM óptica del visado se comparan con estos mismos datos de la ZLM que figuran en la página de datos del pasaporte y/o de la microplaqueta (véase la sección C.1.3). Los datos del visado ZLM deberían presentarse con el o los resultados de esta comparación. Los resultados deberían presentarse con el mismo sistema de colores de un semáforo utilizado en el resto de la GUI. La edad de la persona titular del documento y el período de validez restante del visado deberían mostrarse también en esta zona ya que la persona operadora puede reconocer más fácil y rápidamente esta información que las fechas que figuran en la ZLM.

A continuación se brindan recomendaciones relativas a la presentación de errores:

C.41 **Destacado únicamente de las irregularidades**: Solo debe utilizarse el destacado con colores para señalar irregularidades en el proceso de autenticación (p. ej., en la figura C-14 figura un ejemplo de falla de verificación). Este sistema ayuda considerablemente a la persona usuaria a reconocer la información más relevante ofrecida en la GUI a primera vista.

C.42 **Presentación de errores en la zona de resumen del proceso**: Si un documento no es auténtico, el semáforo de la autenticación óptica debe mostrar un resultado global negativo. Si no se pudo identificar el modelo de documento, el semáforo del resultado global de la autenticación óptica debería mostrar un aviso.

Figura C-16. Ejemplo de presentación para la comparación del pasaporte y el visado

C.43 **Presentación de errores en la zona de vista general óptica**: Si se producen errores debidos a irregularidades ópticas, deberían mostrarse de la siguiente manera:

a) *Irregularidad de una propiedad espectralmente selectiva*: Si se produce un error debido a una rutina de verificación espectralmente selectiva, la imagen del espectro de luz correspondiente debería mostrarse en la zona de datos ópticos del documento en lugar de la imagen VI estándar (p. ej., si falla (UV, BR, FU), debería mostrarse la imagen UV). Además, la zona de vista general óptica debería aparecer enmarcada en rojo.

b) *ZLM no coherente*: Si se produce un error debido a la verificación de la coherencia de la ZLM, la parte correspondiente de la ZLM extraída, incluida la suma de la verificación, debería destacarse en rojo. Y los datos personales incoherentes correspondientes y la zona que contiene los datos personales deberían destacarse también en rojo (véase un ejemplo en la figura C-17). La persona operadora debería ser capaz de corregir manualmente la ZLM y de poner en marcha otro proceso de lectura manualmente por medio de un botón.

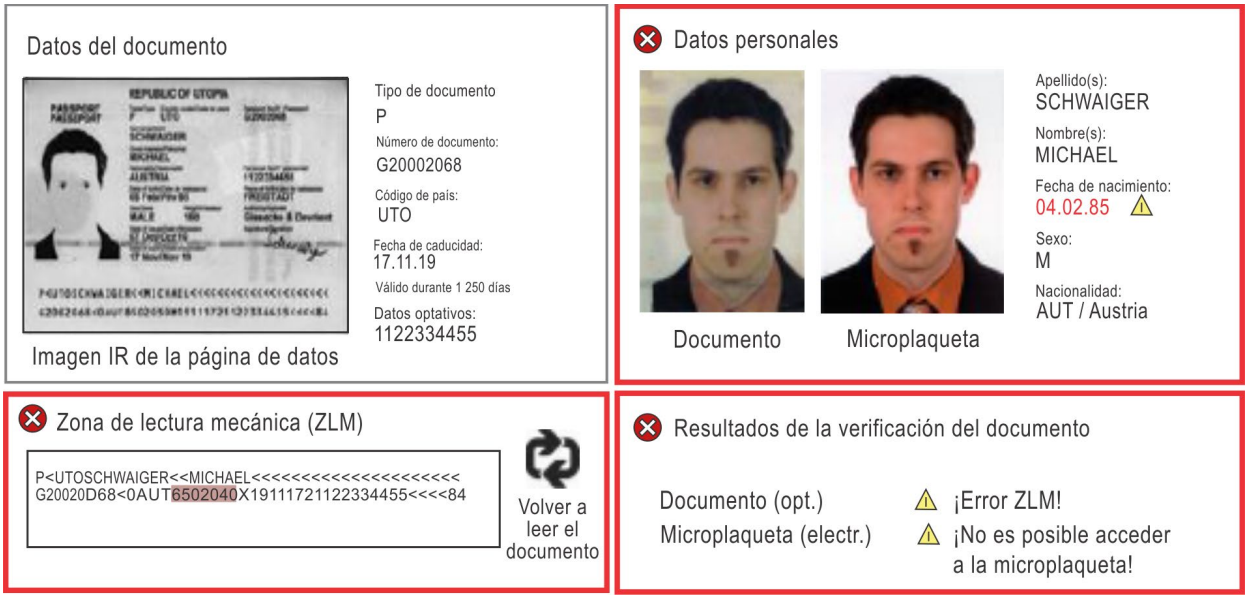

Figura C-17. Ejemplo de visualización de error: Coherencia de la ZLM

c) *Documento caducado*: Si el documento está caducado, la fecha de caducidad debería aparecer destacada en rojo.

d) *Microplaqueta no detectada*: Si está previsto que haya una microplaqueta electrónica en el modelo de documento identificado, pero no se detecta (véase la sección C.1.3), debería aparecer una advertencia. El símbolo de esa advertencia debería ser claramente distinguible de los símbolos del semáforo utilizados para mostrar los resultados de la verificación (p. ej., triángulo amarillo de advertencia).

C.44 **Indicación de errores en la zona de detalles ópticos**: Si se producen errores debido a irregularidades ópticas, deberían indicarse de la siguiente manera:

a) *Documento no identificado*: Si el modelo de documento no se pudo identificar, debería aparecer un símbolo de advertencia como resultado de la identificación del modelo de documento. El símbolo de advertencia debería ser claramente distinguible de los símbolos del semáforo utilizados para mostrar los resultados de la verificación (p. ej., triángulo amarillo de advertencia, véase la figura C-18). Al lado de ese símbolo debería aparecer un texto de advertencia, p. ej., “El modelo de documento no se pudo identificar”.

b) *Rutina de verificación negativa:* Cuando en la rutina de verificación de la página de detalles (véase la figura C-18) aparezca un resultado de verificación negativo, este debería ir acompañado de la luz roja del semáforo. Los elementos respectivos de la verificación espectralmente selectiva fallida deberían destacarse en la imagen correspondiente, p. ej., mediante un rectángulo rojo alrededor de la zona de búsqueda del elemento (p. ej., la ZLM de la imagen IR debido a una legibilidad negativa de la ZLM en IR).

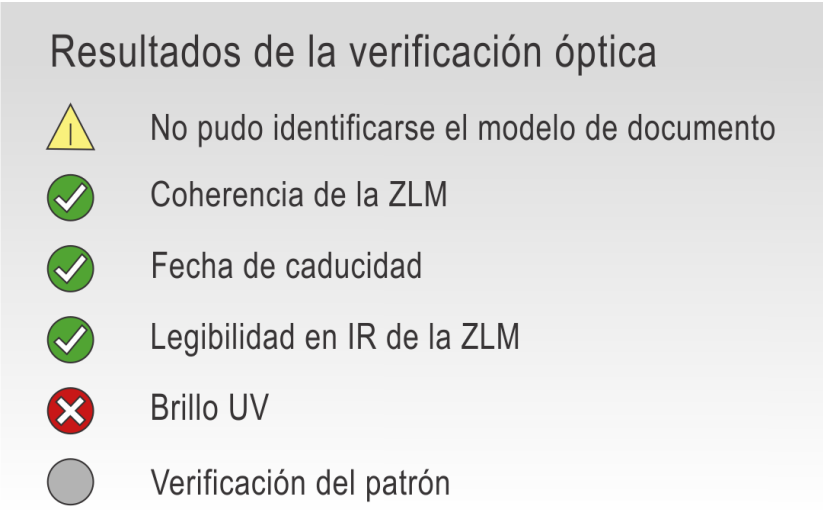

Figura C-18. Ejemplo de visualización de error: Modelo de documento y rutina de verificación negativa

c) *Información no concordante en la microplaqueta*: Cuando un dato de la ZLM no sea el mismo en la página de datos ópticos y la microplaqueta (véase la sección C.1.3), el par de datos no concordantes deberían mostrarse en rojo (con una señal de advertencia, véase la figura C-19).

d) *Dígito no concordante de verificación global*: Los errores relacionados con el dígito de verificación global (véase el Doc 9303, parte 3, capítulo 4 (“ZLM”) podrían ser la indicación de una manipulación de los dígitos de verificación, p. ej., inserción de dígitos de verificación incorrectos en la ZLM con el fin de impedir que se ejecuten los mecanismos de control de acceso (p. ej., control de acceso básico (BAC)). Para cada verificación fallida en la ZLM óptica, el dígito de verificación captado del elemento de la ZLM correspondiente debería mostrarse al lado del dígito de verificación previsto en ese caso.

C.45 **Indicación de los errores de la comparación del pasaporte y el visado/eRP**: Si al menos uno de los datos comparables de la ZLM no es el mismo en el pasaporte y el visado/eRP, esta discrepancia debería mostrarse de la siguiente manera:

a) *zona de vista general del visado/eRP*: Los datos comparables de la ZLM (apellido(s), nombre, fecha de nacimiento, sexo y nacionalidad) del pasaporte deben mostrarse en la página de vista general del visado/eRP al lado de los datos de la ZLM del visado/eRP. Todo par de datos no concordantes debería mostrarse en rojo con una señal de advertencia (véase el ejemplo de la figura C-20).

b) *zona de detalles del visado/eRP*: Cuando los datos de la ZLM no coinciden con los del visado/eRP y el pasaporte, cada par de datos no concordantes debería mostrarse en rojo (con una señal de advertencia).

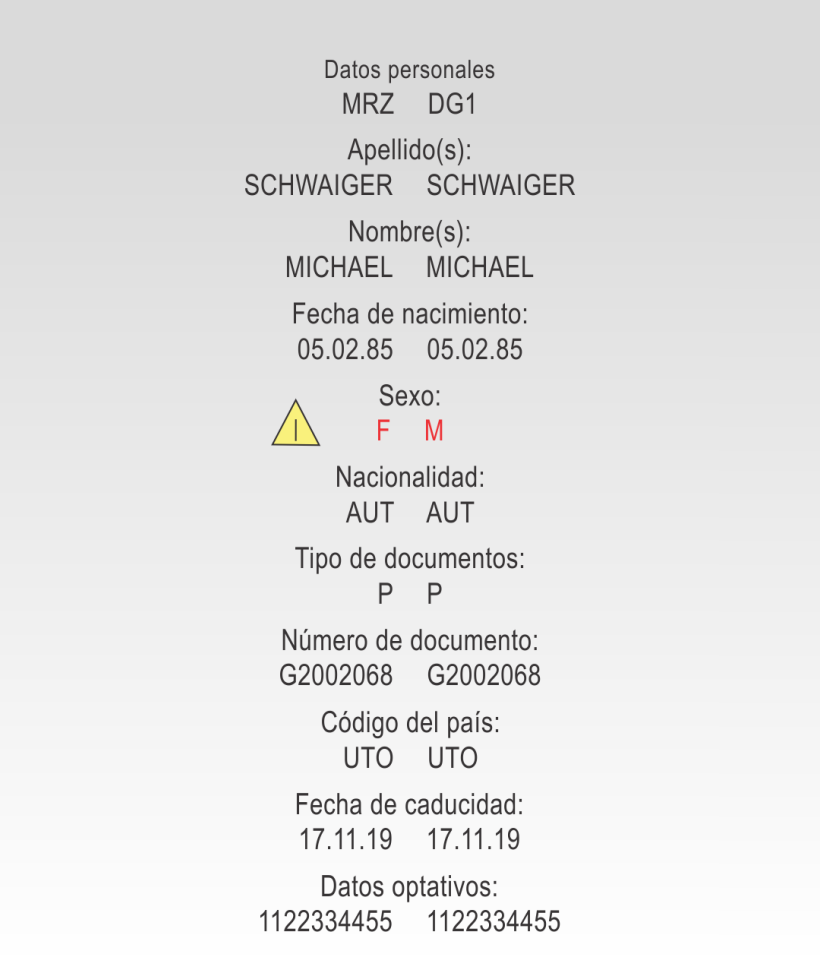

Figura C-19. Ejemplo de visualización de error: datos de la ZLM

Figura C-20. Ejemplo de comparación de los datos del visado y del pasaporte

C.4.3.5 Registro

Para el registro del proceso de autenticación óptica mecánica, son de aplicación las siguientes recomendaciones:

C.46 **Registro de los XML de conformidad con [BSI-TR-03135]**: El registro debe realizarse de conformidad con los esquemas XML definidos en [BSI-TR-03135] que contienen, además de los resultados ópticos detallados, los resultados de la verificación electrónica y combinada (óptica y electrónica) de un documento. Por ejemplo, esto permite:

a) registrar el identificador genérico de una rutina de verificación patentada (véase la sección C.3).

b) poner las rutinas de verificación en modo silencioso, i.e. se ejecuta la rutina y se registran sus resultados, pero el resultado de la verificación no se tiene en cuenta en el resultado general del proceso de autenticación. Esto reviste particular importancia cuando se evalúan nuevas rutinas de verificación, algoritmos o umbrales.

La persona operadora podría necesitar más información sobre las rutinas espectralmente selectivas para fines de evaluación y para actualizar la base de datos subyacente con el fin de garantizar unos resultados de autenticación coherentes y de alta calidad a lo largo del tiempo. Esta información es la misma para todos los documentos de un modelo específico; por ejemplo, la función de decisión, los textos explicativos sobre las rutinas de verificación y la sección de imágenes de la base de datos de referencia. Así pues, el fabricante debe proporcionar este catálogo XML en forma susceptible de lectura mecánica según el esquema XML definido en [BSI-TR-03135], que resume toda la información necesaria sobre las verificaciones espectralmente selectivas. Gracias al formato, el catálogo puede integrarse en la evaluación de los resultados.

C.47 **Registro de los datos de imágenes opcionales**: Los esquemas XML definidos en [BSI-TR-03135] permiten, aunque no reglamentan directamente, el almacenamiento del conjunto de datos reales procesados e imágenes recortadas que muestran la zona de búsqueda de las rutinas de verificación. El programa informático de autenticación debe ser capaz de almacenar los datos de imágenes mencionados en la estructura de datos XML. En la sección C.5 figuran recomendaciones para el almacenamiento de las imágenes de datos por parte de la dirección de operaciones de conformidad con la reglamentación vigente sobre la protección de datos.

C.48 **Posibilidad de anonimización**: El programa informático debería ofrecer la posibilidad de anonimizar el conjunto de datos reales directamente después de la autenticación a fin de que se puedan almacenar permanentemente las imágenes para su ulterior inspección. En la sección C.5.1 figuran recomendaciones de anonimización.

C.4.4 Fabricante de la base de datos de autenticación

Tal como se describe en las secciones C.2.1 y C.2.2, la base de datos de autenticación contiene conjuntos bien definidos de rutinas de verificación para diferentes modelos de documento. Interactúa directamente con el programa informático de autenticación proporcionándole el conjunto de rutinas de verificación correspondientes al modelo de documento identificado. Como se han establecidos modelos nuevos de documento y surgen falsificaciones constantemente, es crucial disponer de una base de datos de autenticación flexible y bien mantenida. En las siguientes secciones se resumen las recomendaciones para la base de datos relativas al proceso de actualización (véase la sección C.4.4.1) y la configurabilidad de la base de datos (véase la sección C.4.4.2).

C.4.4.1 Actualización

A continuación se brindan recomendaciones para los fabricantes de bases de datos de autenticación relativas al proceso de actualización:

D.1 **Intercambio de información sobre nuevos modelos de documento o falsificaciones**: El fabricante de la base de datos de autenticación establecerá un canal de comunicación específico con el director de operaciones para la transferencia segura de conjuntos de datos sobre los nuevos modelos de documento que deberían insertarse en la base de datos. El fabricante intercambiará información sobre los nuevos modelos de documento con quien esté a cargo de la dirección de operaciones por medio de uno de los siguientes métodos:

a) *Intercambio de información por medio de una muestra original*: En este caso debe proporcionarse una muestra original del nuevo modelo de documento o de la falsificación para que se defina y cargue el correspondiente conjunto de rutinas de verificación en la base de datos. El canal de comunicación establecido y los procesos conexos deben tener en cuenta la legislación nacional sobre la protección de datos (véase la sección C.5).

b) *Intercambio por medio del programa informático de captura*: En este caso tiene que proporcionarse a quien se encargue de la dirección de operaciones el programa informático de captura con el fin de generar un conjunto adecuado de datos reales de nuevos modelos de documento o falsificaciones. Este conjunto de datos debe contener al menos una imagen VI, UV y IR. Idealmente el programa informático de captura debería generar varias imágenes de un espectro de luz (de forma análoga a la fotografía de alto rango dinámico). El conjunto de datos se transfiere al fabricante para que se defina el correspondiente conjunto de rutinas de verificación que habrán de incluirse en la siguiente edición de la base de datos. El fabricante debe recomendar una lista de dispositivos de captura adecuados para este fin.

D.2 **Actualización periódica de la base de datos**: La base de datos de autenticación permitirá la realización de actualizaciones programadas periódicamente (como mínimo cada 3 meses). Asimismo, permitirá la realización de actualizaciones especiales, previa solicitud especial (urgente):

a) si el fabricante obtuvo información nueva sobre documentos genuinos o falsificaciones y actualizó la base de datos de documentos sobre la base de esa información en cooperación con el director de operaciones (véase D.1 a), o

b) si la persona operadora generó un conjunto de datos reales con el programa informático de captura (documento genuino o falsificación) y lo envió al fabricante (véase D.1 b).

D.3 **Suministro de actualizaciones graduales**: Por defecto, el fabricante de la base de datos de autenticación debe suministrar a la persona operadora actualizaciones de versiones completas. Deberían distribuirse también actualizaciones graduales con el fin de ahorrar tiempo y anchura de banda.

D.4 **Entrega de documentación suficiente sobre los cambios**: Al entregar las actualizaciones, el fabricante de la base de datos de autenticación debe proporcionar suficiente documentación sobre los cambios introducidos en la base de datos.

C.4.4.2 Contenido y configurabilidad de la base de datos

En esta sección se brinda una lista de recomendaciones para los fabricantes de bases de datos de autenticación relativas al contenido y la configurabilidad de la base de datos:

D.5 **Contenido reducido**: La base de datos de autenticación debería estar disponible con diferentes alcances, pudiendo adaptarse, por tanto, a situaciones diferentes. Por ejemplo, las situaciones del entorno comercial tienen un alcance limitado y el tipo de documentos verificados suele ser muy específico (p. ej., la autenticación de documentos en las compañías de alquiler de coches). Por ello, se recomienda proporcionar bases de datos de autenticación que aborden específicamente las necesidades de las posibles situaciones comerciales por medio de una complejidad reducida. Al proporcionar una base de datos de contenido reducido, el fabricante garantiza que siga siendo eficaz en función del costo y fácil de integrar en diferentes entornos.

D.6 **Asignación de verificaciones por nivel de importancia**: Las verificaciones deberían asignarse con un nivel de importancia con el fin de que el programa informático de autenticación pueda realizar esas verificaciones por orden de importancia (véase la recomendación C.25 a) para los fabricantes de programas informáticos de autenticación mencionados en la sección C.4.3).

D.7 **Opción de modos operativos diferentes**: Las diferentes situaciones de uso requieren diferentes niveles de seguridad en cuanto a la aceptación o rechazo de un documento. Para el control fronterizo estacionario, por ejemplo, es necesario un alto grado de seguridad, mientras que las situaciones que se dan en un entorno comercial suelen centrarse más en su alta practicidad para la persona titular del documento. Así pues, la base de datos de autenticación debería proporcionar, como mínimo, dos modos operativos diferentes, para la alta seguridad y para la alta practicidad.

D.8 **Información sobre la exposición a la luz UV específica para el modelo de documento**: Como se mencionó en la sección C.4.2, a menudo modelos de documento diferentes requieren una exposición diferente a la luz UV. Por ejemplo, algunos modelos de documento requieren una iluminación UV más larga con el fin de verificar adecuadamente a la luz UV determinados elementos. Así pues, la base de datos de autenticación debería contener información sobre el reglaje del tiempo de exposición UV necesario para los modelos de documento correspondientes, para que el programa informático de autenticación pueda configurar automáticamente el lector de página completa en consecuencia (véase la sección C.4.2, párrafo B.8).

D.9 **Suministro de un entorno basado en un servidor**: Se recomienda suministrar una base de datos de autenticación que pueda funcionar también en un entorno basado en un servidor. En este caso, programas informáticos de autenticación distintos podrían acceder a una sola base de datos de autenticación. Además, dos o más bases de datos de autenticación se podrían operar como un grupo accesible a varios productos informáticos de autenticación.

C.4.5 Fabricante de la base de datos de referencia

Aun cuando la base de datos de referencia no forme parte directamente del sistema de autenticación (véase la sección C.2.1), puede utilizarse como fuente complementaria de información si no es posible determinar claramente la autenticidad de un documento por medio de la autenticación mecánica. En ese caso, la base de datos de referencia puede servir de apoyo a la persona operadora al proporcionarle información detallada sobre el modelo de documento correspondiente, p. ej., imágenes de alta calidad de las características, textos explicativos e información sobre formas comunes de falsificación (a la intención de la 2ª línea/inspección de la oficina auxiliar). Un ejemplo de una base de datos de referencia es el denominado sistema FADO (Documentos Auténticos y Falsos en Red) de la Unión Europea. El recurso homólogo del FADO, de acceso público, se llama PRADO[14] (Registro Público de Documentos Auténticos de Identidad y de Viaje en Red).

En caso de que se use, tiene algunas implicaciones prácticas que el fabricante de la base de datos de referencia debería tener en cuenta. En esta sección se abordan esas implicaciones por medio de recomendaciones:

E.1 **Suministro automático de resultados de salida**: La base de datos de referencia recibirá y procesará un enlace específico a un modelo de documento como entrada del proceso de identificación. Debería proporcionar también un conjunto de datos de referencia correspondientes a ese enlace como resultado de salida.

E.2 **Opción de selección manual del conjunto de datos**: Además de la selección automática de un conjunto de datos de referencia, una persona operadora también podrá hacer selecciones y búsquedas manuales en un conjunto de datos específicos por medio de una GUI.

E.3 **Suministro de información amplia sobre los documentos auténticos**: La base de datos de referencia contendrá información sobre documentos auténticos y podrá ir acompañada de descripciones conexas de alteraciones habituales de documentos. Las propiedades específicas de los modelos de documentos de referencia se describirán detalladamente y todo contenido irá acompañado de un texto descriptivo.

En este contexto, cabe mencionar que una base de datos como EDISON-TD también puede tomarse en consideración. Pueden usarse los mecanismos que se describen en la recomendación D.1 para incrementar el uso de las bases de datos comerciales.

C.4.6 Director de operaciones

Se denomina *director de operaciones* a la organización encargada de la administración y la gestión de todos los procesos relacionados con el funcionamiento de una infraestructura de autenticación. Estas organizaciones son miembros del personal de dirección de operaciones que interactúa directamente con el sistema de autenticación.

14. http://prado.consilium.europa.eu/en/homeindex.html

La realización concreta de la operación prevista depende de la situación de inspección. Ejemplos de posibles situaciones son:

- **Control fronterizo estacionario** (abreviatura SBC): En este caso, la dirección de las operaciones corresponde a las autoridades gubernamentales para el control fronterizo estacionario (p. ej., policía fronteriza). En este entorno las personas operadoras suelen estar muy familiarizadas con la verificación óptica de documentos. El alcance de la inspección es inmenso debido al elevado número y diversidad de los documentos verificados. Además, el sistema requiere una amplia interacción y la evaluación de las personas operadoras que interactúan directamente con el sistema y la persona titular del documento.

- **Control fronterizo automatizado por medio de las puertas ABC** (abreviatura ABC): En este tipo de situación las autoridades gubernamentales para las puertas ABC también asumen la dirección de las operaciones, que a menudo se centra más en la autenticación rápida de los documentos que en una autenticación amplia de los documentos. En este caso las personas operadoras son guardias de frontera, que poseen la instrucción adecuada y suelen supervisar un conjunto de puertas ABC respetando la visualización minimalista. Al revés que en el caso del control fronterizo estacionario, este sistema lo usa el público viajero, por lo que es necesario facilitarle una amplia orientación, que queda fuera del alcance de este manual.

- **Autenticación de documentos para fines comerciales** (abreviatura CP): En este caso, la dirección de las operaciones corresponde a las entidades comerciales (p. ej., en los bancos). Al revés que en las situaciones mencionadas previamente, las personas operadoras no suelen estar familiarizadas con la verificación óptica de los documentos y el alcance de la inspección suele ser más reducido que el del control fronterizo.

Las capacidades de los componentes adquiridos deben responder a las necesidades de quien se encarga de la dirección de operaciones y de los requisitos de la situación de implementación. En esta sección, las recomendaciones para los fabricantes de lectores de página completa (véase la sección C.4.2), de programas informáticos de autenticación (véase la sección C.4.3), de bases de datos de autenticación (véase la sección C.4.4) y de bases de datos de referencia (véase la sección C.4.5) se adaptan a las situaciones de uso. En la sección C.5 se formulan recomendaciones para una vigilancia conforme a la reglamentación sobre la protección de datos.

La tabla C-4 que figura a continuación resume, para cada situación, el uso razonable de las recomendaciones para el fabricante de lectores de página completa.

Tabla C 4. Recomendaciones para los lectores de página completa clasificadas por situación de inspección

Fabricante de lectores de página completa				
Nº.	*Descripción breve*	*Situación de uso*		
		SBC	ABC	CP
B.1	Longitudes de onda adecuadas del espectro de luz	X	X	X
B.2	Garantía de una resolución mínima	X	X	X
B.3	Presentación de un formato estándar de las imágenes	X	X	X
B.4	Captura de un tamaño de hasta ID-3	X	X	X
B.5	Captura de todas las superficies con la misma calidad	X	X	X
B.6	Tiempo de respuesta breve e intensidad constante	X	X	X
B.7	Calidad de la imagen constante	X	X	
B.8	Ajuste de la exposición de la luz UV por medio del programa informático de autenticación	X	X	
B.9	Captura de múltiples imágenes UV	X		
B.10	Imágenes sin reflejos	X	X	
B.11	Mecanismo para presionar el documento y que quede plano en la zona de captura	X	X	X
B.12	Funcionamiento con una sola mano	X	X	X
B.13	Orientación interactiva para el público usuario		X	X[15]
B.14	Equipo informático con un alto grado de solidez	X	X	X

15. La forma de entender “orientación al usuario” depende considerablemente del caso de uso comercial.

La tabla C-5 que figura a continuación resume, para cada situación, el uso razonable de las recomendaciones para el fabricante de productos informáticos de autenticación.

Tabla C 5. Recomendaciones para los productos informáticos de autenticación clasificadas por situación de inspección

Fabricante de programas informáticos de autenticación				
Nº	*Descripción breve*	*Situación de uso*		
		SBC	ABC	CP
C.1	Procesamiento de imágenes previamente grabadas[16]	X		
C.2	Procesamiento de imágenes de diferentes fuentes de equipo informático	X	X	X
C.3	Abstracción de la GUI (interfaz gráfica de usuario) del programa y equipo informáticos de autenticación	X	X	X
Detección de documentos				
C.4	Detección automática y manual de documentos	X	X[17]	
C.5	Compensación de la rotación y consiguiente recorte de la página de datos captada	X	X	X
C.6	Detección del documento sobre la base de su presencia óptica	X	X	X
Identificación				
C.7	Identificación del modelo de documento	X	X	X
C.8	Identificación rápida por medio de la ZLM	X	X	X
C.9	Opción de reserva en caso de que la ZLM no sea legible a la luz IR	X	X	X
C.10	Modelo de documento inequívoco	X		
C.11	Posibilidad de identificación parcial	X		
C.12	Posibilidad de identificación manual posible	X		
C.13	Identificación de las tarjetas ID por ambos lados	X	X	X
C.14	Identificación de los documentos de muestra	X	X	X

16. Esta recomendación es importante para la evaluación de los productos informáticos de autenticación.
17. La detección manual de documentos no es aplicable a la situación de control fronterizo automático.

Fabricante de programas informáticos de autenticación				
Nº	*Descripción breve*	*Situación de uso*		
		SBC	ABC	CP
Verificación				
C.15	Realización de un número mínimo de verificaciones espectralmente selectivas	X	X	X
C.16	Verificación de la coherencia de la ZLM	X	X	X
C.17	Realización de verificaciones en todas las categorías	X	X	X
C.18	Verificación de la presencia de microplaquetas	X	X	X
C.19	Verificación de patrones dinámicos	X	X	X
C.20	Combinación de rutinas de verificación en caso necesario	X	X	X
C.21	Realización de rutinas de verificación redundantes en múltiples posiciones	X		X
C.22	Rutinas de verificación redundantes en múltiples colores bajo la luz UV	X		
C.23	Vinculación y verificación de ambas páginas de una tarjeta ID	X	X	X
C.24	Verificación cruzada en múltiples páginas de los datos personales	X	X	X
C.25	Realización de rutinas de verificación en función de su importancia	X	X	X
C.26	Consideración de la degradación de las características	X	X	X
C.27	Detección de ataques genéricos	X	X	X
Visualización				
C.28	Presentación de todas las verificaciones del documento en una GUI	X	X	X
C.29	Visibilidad obligada de la *zona de resumen del proceso*	X	X	X
C.30	Muestra de la *zona de vista general óptica* en la página de inicio	X		
C.31	Selección de más detalles mediante un clic	X	X	
C.32	Presentación de los resultados con los colores del semáforo	X	X	X
C.33	Correspondencia de los resultados acorde con [BSI-TR-03135]	X	X	X
C.34	Correspondencia minimalista para los resultados	X	X	X

Fabricante de programas informáticos de autenticación				
Nº	*Descripción breve*	*Situación de uso*		
		SBC	ABC	CP
C.35	Presentación de la información detallada en una *zona de detalles ópticos* específica	X		
C.36	Orientación al público usuario durante la lectura del documento	X	X	X
C.37	Presentación de la información de bases de datos centrales	X		
C.38	Configuración homogénea de los MRTD	X		X
C.39	Orientación a la persona operadora a lo largo del proceso de verificación multipáginas	X		
C.40	Comparación del contenido del pasaporte y el visado/permiso de residencia electrónico (eRP)	X		
C.41	Destacado únicamente de las irregularidades	X	X	X
C.42	Presentación de errores en la zona de resumen del proceso	X	X	X
C.43	Presentación de errores en la zona de vista general óptica	X		
C.44	Indicación de errores en la zona de detalles ópticos	X		
C.45	Indicación de los errores de la comparación del pasaporte y el visado/eRP	X		
Registro				
C.46	Registro de los XML de conformidad con [BSI-TR-03135]	X	X	X
C.47	Registro de los datos de imágenes opcionales	X	X	X
C.48	Posibilidad de anonimización	X	X	X

La tabla C-6 que figura a continuación resume, para cada situación, el uso razonable de las recomendaciones para el fabricante de bases de datos de autenticación.

Tabla C 6. Recomendaciones para las bases de datos de autenticación clasificadas por situación de inspección

Fabricante de bases de datos de autenticación				
Nº	*Descripción breve*	*Situación de uso*		
		SBC	ABC	CP
D.1	Intercambio de información sobre nuevos modelos de documento o falsificaciones	X	X	
D.2	Actualización periódica de la base de datos	X	X	X
D.3	Suministro de actualizaciones graduales	X	X	X
D.4	Entrega de documentación suficiente sobre los cambios	X	X	X
D.5	Contenido reducido			X
D.6	Asignación de verificaciones por nivel de importancia	X	X	X
D.7	Opción de modos operativos diferentes	X	X	X
D.8	Información sobre la exposición a la luz UV específica para el modelo de documento	X	X	X
D.9	Suministro de un entorno basado en un servidor	X	X	X

La tabla C-7 que figura a continuación resume, para cada situación, el uso razonable de las recomendaciones para el fabricante de bases de datos de referencia.

Tabla C 7. Recomendaciones para las bases de datos de referencia clasificadas por situación de inspección

Fabricante de bases de datos de referencia				
Nº	*Descripción breve*	*Situación de uso*		
		SBC	ABC	CP
E.1	Suministro automático de resultados de salida	X		
E.2	Opción de selección manual del conjunto de datos	X		X[18]
E.3	Suministro de información amplia sobre los documentos auténticos	X		X[18]

18. Considerando los CP, es importante ajustar el nivel de conocimientos, en función del caso de uso.

C.5 VIGILANCIA CONFORME A LA PROTECCIÓN DE DATOS

Un proceso de autenticación óptica puede dar lugar a un resultado inesperado debido a una de las siguientes razones:

- Se ha detectado un documento falsificado.
- Se ha clasificado un documento falsificado como auténtico.
- Se ha clasificado un documento auténtico como falsificado.
- Se ha producido un error de manejo del lector de página completa, p. ej., se ha retirado el documento del lector durante la autenticación.
- No se pudo identificar el modelo de documento.

En estos casos, es crucial que quien se encarga de la dirección operativa pueda analizar por qué motivo se tomó la decisión equivocada. Así, debe registrarse y analizarse la información obtenida en el procedimiento de autenticación, la cual, de ser posible, ha de incluir la información personal. Esto plantea directamente problemas de protección de datos porque no está permitido almacenar los datos personales, ni siquiera cifrados, sin el consentimiento de la persona titular del documento o por una razón determinada. A continuación se brindan recomendaciones para la dirección operativa:

F.1 **Registro de la información notificada de autenticación**: La información obtenida del procedimiento de autenticación sin datos personales (p. ej., modelo de documento identificado, resultados de la autenticación, resultados de la rutina de verificación, etc.) debe registrarse de conformidad con [BSI-TR-03135]. Así pues, el conjunto de datos reales, la ZLM y la ZIV quedan excluidos del registro. Este tipo de información no se necesita de forma urgente y puede usarse para análisis estadísticos.

F.2 **Establecimiento de un sistema de retroalimentación al fabricante**: Puede recurrirse a la retroalimentación regular procedente del nivel operacional para optimizar el programa informático de autenticación. Así pues, la información notificada explicada en F.1 debería transmitirse al fabricante del programa informático de autenticación regularmente.

F.3 **Almacenamiento del conjunto de datos reales inalterados si existe la posibilidad**: La mejor forma de analizar los errores es haciéndolo en el mismo conjunto de datos reales que se ha proporcionado para su autenticación. Por ello, se recomienda almacenar los conjuntos de datos reales inalterados en el esquema XML definido en [BSI-TR-03135] si existe la posibilidad de hacerlo con consentimiento respecto a las preocupaciones relativas a la privacidad de los datos. Existen las siguientes posibilidades de registro con inclusión de imágenes:

a) *Almacenamiento del conjunto de datos reales con el consentimiento de la persona titular del documento*: Si la situación lo permite, puede almacenarse el conjunto de datos reales utilizado para la autenticación obteniendo primeramente el consentimiento por escrito de la persona titular del documento. Solo es razonable optar por esta modalidad en situaciones que permiten la comunicación con la persona titular del documento, como las/os pilota/os por ejemplo, y no de forma permanente. Además, hay que eliminar los conjuntos de datos reales irreversiblemente después de un período de tiempo definido contractualmente.

b) *Almacenamiento del conjunto de datos reales en caso de error*: Se permite almacenar los datos personales durante un período de tiempo definido contractualmente si existe una razón concreta para ello, p. ej., que se haya producido un error durante la autenticación. Si la situación lo permite, este período de tiempo puede utilizarse para el análisis de errores del conjunto de datos reales inalterados, que después tiene que eliminarse irreversiblemente.

c) *Registro de regiones favorables a la privacidad*: Para evitar las preocupaciones relativas a la privacidad de los datos y, al mismo tiempo, preservar las posibilidades de análisis aproximados, solo pueden registrarse las imágenes recortadas “favorables a la privacidad” que muestren la zona de búsqueda de las rutinas de verificación. Esas regiones de interés no deben contener la imagen facial completa, ni la ZLM o la ZIV, y pueden almacenarse para todos los procesos de autenticación sin limitación temporal en el esquema XML definido en [BSI-TR-03135].

F.4 **Anonimidad de las imágenes si existe la posibilidad**: Otra propuesta para evitar las preocupaciones relativas a la privacidad de los datos y poder, aun así, almacenar el conjunto de datos reales completo sin limitación temporal, consiste en anonimizar los datos personales en el conjunto de datos reales. Con este método las zonas que contienen datos personales son difíciles de analizar, mientras que las partes de datos no personales del documento son perfectamente analizables.

Nota.— Aclaración de las preocupaciones relativas a la privacidad de los datos: *Las preocupaciones relativas a la privacidad de los datos mencionadas en las recomendaciones F.1 a F.4 deben ser aclaradas por quien se encargue de la dirección operativa, p. ej., por medio de un concepto de privacidad de los datos. Pueden combinarse las recomendaciones para almacenar conjuntos de datos reales formuladas en F.3 y F.4, p. ej., el almacenamiento de las regiones favorables a la privacidad.*

C.6 BIBLIOGRAFÍA

[BSI-TR-03135] BSI, Machine Authentication for Public Sector Applications (Autenticación mecánica para las aplicaciones del sector público), TR-03135, 2017.
url: https://www.bsi.bund.de/tr03135/

[FRONTEX-ABC] FRONTEX: Best Practice Technical Guidelines for Automated Border Control (ABC) Systems (Directrices técnicas de buenas prácticas relativas a los sistemas de control fronterizo automatizado), 2012

— — — — — — — —

APÉNDICE D DE LA PARTE 2 — PREVENCIÓN DE FRAUDES RELACIONADOS CON EL PROCESO DE EXPEDICIÓN (INFORMATIVO)

D.1 ALCANCE

En el presente apéndice se describen los riesgos de fraude relacionados con el proceso de solicitud y expedición de MRTD. Estos peligros son consecuencia de las ventajas que pueden obtenerse con la posesión de un MRTD que pueda utilizarse para confirmar la identidad y ciudadanía de la persona titular. En el apéndice se recomiendan precauciones que los Estados expedidores puedan adoptar para evitar dichos fraudes.

D.2 EL FRAUDE Y SU PREVENCIÓN

Los fraudes perpetrados como parte del proceso de expedición pueden ser de varios tipos principales:

- robo del MRTD genuino en blanco y llenado de los mismos para hacerlos parecer válidos;
- solicitud de MRTD bajo una identidad falsa utilizando pruebas genuinas de nacionalidad o de identidad robadas de otro individuo, u obtenidas ilegalmente;
- solicitud de MRTD bajo una identidad falsa utilizando pruebas falsificadas de nacionalidad o de identidad;
- uso de MRTD falsamente declarados, o no declarados, como extraviados o robados que pueden facilitarse a personas para uso fraudulento por parecido físico con la persona titular o con repetidas sustituciones de fotografía; y
- recurso a empleados del departamento de MRTD para obtener del sistema un MRTD expedido fuera de las reglas.

Hay dos categorías adicionales en las cuales la persona solicitante se presenta con su propia identidad con intención de ser cómplice en el uso fraudulento ulterior del MRTD mediante:

- alteración de un documento genuinamente expedido para adecuarlo a un portador que no es la persona a la que se expidió el MRTD; y
- solicitud de un MRTD con intención de darlo o venderlo a alguien que se asemeje a la persona titular genuina.

D.3 MEDIDAS RECOMENDADAS CONTRA EL FRAUDE

Para combatir las amenazas mencionadas, se recomienda que la autoridad encargada de expedir el MRTD del Estado adopte las medidas siguientes, si cuenta con los recursos adecuados para su implantación.

Debería designarse a una persona idónea como Jefe de seguridad que responda directamente al Director General de la autoridad expedidora. El Jefe de seguridad debería ser responsable de garantizar que los procedimientos de seguridad se establecen, observan y actualizan según sea necesario.

En cada lugar en que se expidan MRTD debería haber un Gerente de seguridad designado, responsable de la implantación y actualización de los procedimientos de seguridad que responda directamente al Jefe de seguridad.

Deberían establecerse procedimientos de control y examen para asegurar que el personal se contrata solamente después de haberse verificado su identidad, establecido que no tienen antecedentes delictivos, y verificado que su situación financiera es sólida. También deberían realizarse verificaciones de seguimiento regulares para establecer si hay miembros del personal cuya situación haya cambiado y que ello los haga susceptibles a tentaciones de emprender actividades fraudulentas.

Debería alentarse a todo el personal de la autoridad expedidora de MRTD a que adopten una actitud positiva con respecto a los asuntos de seguridad, debería existir un sistema de recompensas para todo miembro del personal que notifique incidentes o identifique medidas para impedir fraudes.

Deberían establecerse controles para vigilar componentes fundamentales como las libretas en blanco y los laminados de seguridad. Cada uno de estos artículos debería tener un número de serie único y se les debería conservar bajo llave en un lugar adecuadamente seguro. A comienzo de cada día o turno de trabajo debería entregarse para procesamiento solamente la cantidad requerida. Debería efectuarse un recuento de los artículos y verificarse los resultados por dos miembros del personal quienes también deberían registrar los números propios de cada artículo. La persona a la que se les entreguen, debe responder por todos los artículos al final del turno, ya sea en forma de documentos personalizados o de productos defectuosos. Todos los artículos deberían devolverse al almacenamiento seguro al final del período de trabajo, siendo contados también por dos personas que registren los números propios de cada uno. Los registros deberían conservarse como mínimo durante toda la vida útil del MRTD expedido.

Los productos o los materiales defectuosos deberían destruirse en condiciones controladas registrándose también los números propios de cada uno.

El proceso de expedición debería dividirse en operaciones separadas que se realicen en lugares separados dentro de la instalación. La finalidad de esto es asegurar que nadie puede realizar la totalidad del proceso de expedición sin pasar por una o más áreas a las que la persona no está autorizada a ingresar.

D.4 PROCEDIMIENTOS PARA COMBATIR SOLICITUDES FRAUDULENTAS

Se recomiendan los procedimientos siguientes para impedir la expedición de un MRTD genuino como resultado de la recepción de una solicitud fraudulenta.

La oficina expedidora de MRTD debería designar un número apropiado de especialistas antifraude (AFS) que haya recibido un elevado nivel de capacitación en la detección de todos los tipos de fraude utilizados en las solicitudes de MRTD. Debería haber por lo menos un especialista antifraude presente en cada lugar en que se procesan las solicitudes y solicitantes de MRTD. Un especialista antifraude debería estar presente en todo momento para apoyar a los encargados de procesar solicitudes [funcionarios de autorización (AO)] y brindar asistencia en el tratamiento de solicitudes sospechosas. El personal de especialistas antifraude debería proporcionar capacitación con carácter regular a los funcionarios de autorización a efectos de aumentar su conocimiento de posibles riesgos de fraude.

La autoridad expedidora de MRTD debería establecer una estrecha relación con los expedidores de “documentos generadores” como los certificados de nacimiento y matrimonio y los permisos de conductor. El acceso a una base de datos de certificado de defunción ayuda a prevenir el fraude cuando se presenta una solicitud de MRTD en nombre de

una persona fallecida. El Estado debería asegurarse de que los departamentos que conservan registros de nacimientos, matrimonios y fallecimientos los mantienen cotejados y al día y los datos se almacenan en una base de datos a la que la oficina expedidora de MRTD debería tener acceso seguro. La finalidad es facilitar la verificación rápida de que los documentos generadores presentados son genuinos y que, por ejemplo, no se presenta una solicitud en el nombre de una persona fallecida. Debería exigirse que la persona que solicite un MRTD por primera vez se presente ante una oficina expedidora de MRTD con los documentos generadores de apoyo para una entrevista con un funcionario de autorización y, cuando sea necesario, con un especialista antifraude.

También puede utilizarse una entrevista para aplicar al procesamiento de solicitudes de un MRTD para sustituir un MRTD caducado. Como alternativa, siempre que la oficina expedidora de MRTD cuente con una base de datos de información personal adecuada, incluyendo retratos, la solicitud de reemplazo podría procesarse mediante presentación de la documentación, incluyendo un nuevo retrato, por correo. En tales casos, es conveniente que la solicitud y el nuevo retrato sean avalados por una persona responsable. Debería exigirse con la nueva solicitud la devolución del MRTD que expire.

La oficina expedidora de MRTD debería iniciar procedimientos que impidan la expedición fraudulenta de más de un MRTD a un individuo que pueda haber intentado asumir más de una identidad. En este proceso pueden utilizarse verificaciones por computadora de la base de datos de retratos almacenados utilizando reconocimiento del rostro y, cuando estén disponibles, las huellas digitales.

Los procedimientos de la oficina expedidora de MRTD deberían impedir que el solicitante escoja el funcionario de autorización con quien tratar. Inversamente, el régimen de trabajo debería impedir al personal empleado seleccionar las solicitudes que debe procesar.

La expedición de un MRTD a un niño pequeño debería exigir la presencia en la oficina expedidora de MRTD de preferiblemente ambos padres y el niño. Esto contribuye a reducir el riesgo de secuestro de un niño por uno de los padres.

La sustitución de un MRTD cuyo extravío o robo se haya denunciado debería efectuarse sólo después de exhaustivas verificaciones que incluyan una entrevista personal con el solicitante.

Se recomienda proporcionar a la base de datos de INTERPOL los detalles, en particular los números de documentos, de los MRTD extraviados o robados. Esta base de datos está disponible a todos los países participantes y puede utilizarse en la elaboración de listas de vigilancia.

D.5 CONTROL DE LAS INSTALACIONES EXPEDIDORAS

Los Estados deberían considerar la expedición de todos los MRTD desde uno o, como máximo, dos centros. Esto reduce el número de lugares en que se almacenan los documentos en blanco y otros componentes de seguridad. El control de una instalación central puede ser mucho más riguroso que si existieran varios centros de expedición. Si se adopta la expedición central, habrá que establecer centros para entrevistas con los solicitantes. Además, dado que los MRTD normales no pueden expedirse instantáneamente, debería establecerse un sistema para la expedición de MRTD de emergencia.

— — — — — — — —

APÉNDICE E DE LA PARTE 2 — CONSIDERACIONES FUNDAMENTALES SOBRE LA ASF/SLTD (INFORMATIVO)

Requisitos legislativos	Antes de que los Estados puedan iniciar la carga de información en la ASF/SLTD de INTERPOL, deben explorar su propia legislación para determinar si cuentan con la autoridad o mandato para proporcionar acceso internacional a elementos de la información que figura en el documento de viaje de sus ciudadanos. En caso de que se requiera enmendar la legislación, los Estados deberían cerciorarse de que se cubren adecuadamente los aspectos siguientes: 1. recolección y almacenamiento de datos; 2. disposiciones sobre privacidad (incluyendo seguridad); 3. autorización para difundir datos a la comunidad internacional; y 4. ciclo de vida de los datos y no repudio.
Elementos de datos	Se ha elaborado un conjunto de datos estándar que se concentra en los detalles del documento más que en el titular del mismo para intercambiar información sobre documentos de viaje extraviados, robados y revocados. Los Estados deben satisfacer los siguientes campos de datos requeridos cuando carguen o suban datos a esta base de datos: 1. número de identificación del documento de viaje*; 2. tipo de documento (pasaporte u otro); 3. código de la OACI del Estado expedidor; 4. estado del documento (es decir, robado en blanco); y 5. país donde se perpetró el robo (solo obligatorio para documentos de viaje en blanco robados). *Cuando el documento de viaje ha sido personalizado se trata del número que figura en la ZLM; si es una libreta en blanco, este número debería ser el número de serie, si los números no son iguales.
Recolección de información	Los Estados deberían cerciorarse de que los mecanismos utilizados para recoger información sobre documentos de viaje extraviados y robados (es decir, entrevistas telefónicas, formularios en línea) son completos y conducen a la recolección segura de toda la información requerida para llenar el informe de ASF/SLTD.
Suministro oportuno y exacto de los datos	La fuerza de la base ASF/SLTD de INTERPOL se basa en la información oportuna y exacta. Por consiguiente, los Estados deberían cerciorarse de que cuentan con sistemas y procesos para compartir información en la forma más oportuna a efectos de interceptar intentos de utilizar documentos de viaje extravíados, robados o revocados en el puesto de control fronterizo. Los Estados deberían tratar de compartir esta información diariamente. En general, una vez recibida la información de que el documento de viaje ha dejado de estar en

	posesión de la persona titular legítima o que ha sido revocado, la autoridad expedidora debería registrar oficialmente la información en su base de datos nacional (si tiene y mantiene una) y en la ASF/SLTD. Los Estados también deberían tratar continuamente de asegurar que sus datos son exactos y fiables. Debe ejercerse cautela para evitar errores en entradas y anotaciones y proporcionar todos los datos requeridos sobre el documento, dado que la notificación precisa es responsabilidad de la autoridad expedidora. Los errores en la notificación pueden perjudicar o interrumpir los viajes y resultar costosos tanto para el viajero como para el Estado expedidor. Por consiguiente, los Estados deben adoptar las medidas necesarias para asegurar el registro y notificación exactos de los documentos de viaje extraviados, robados y revocados. Los Estados deberían contar con una instalación de respuesta de funcionamiento continuo para tratar rápidamente peticiones de más información a INTERPOL en nombre de los Estados interesados.
Fortalecimiento de las bases de datos nacionales sobre documentos de viaje extraviados, robados y revocados	Los Estados que mantienen bases de datos nacionales sobre documentos de viaje extraviados, robados y revocados deberían considerar el uso de medios automáticos para transmitir esta información a INTERPOL a efectos de potenciar sus actividades.

— FIN —

ISBN 978-92-9265-508-2