OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Parte 1: Introducción

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 1: Introducción

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, Montréal, Quebec, Canada 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 1 — *Introducción*
ISBN 978-92-9265-375-0

ENMIENDAS

La publicación de enmiendas se anuncia periódicamente en los suplementos del *Catálogo de productos y servicios* de la OACI; 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 CORRIGENDOS

ENMIENDAS		
Núm.	Fecha	Anotada por

CORRIGENDOS		
Núm.	Fecha	Anotado por

ÍNDICE

1. PREÁMBULO

La labor de la OACI en materia de documentos de viaje de lectura mecánica empezó en 1968 cuando el Comité de Transporte aéreo del Consejo creó el Grupo de expertos sobre la tarjeta-pasaporte, al que se le encargó que redactara las recomendaciones para una libreta o tarjeta de pasaporte normalizada que fuera susceptible de lectura mecánica en pro de acelerar el despacho de pasajeros por los puestos de control de pasaportes. El Grupo de expertos hizo un número de recomendaciones, entre las que figura la adopción del reconocimiento óptico de caracteres (OCR) como técnica preferida para la lectura mecánica debido a su madurez, eficacia en función del costo y fiabilidad. En 1980 se publicaron las especificaciones y textos de orientación elaborados por el Grupo de expertos como primera edición del Doc 9303, con el título de *Pasaporte susceptible de lectura mecánica*, que Australia, Canadá y Estados Unidos emplearon como guía para comenzar a expedir pasaportes de lectura mecánica.

Con objeto de actualizar y refinar las especificaciones que fueron en su día redactadas por el Grupo de expertos, la OACI estableció en 1984 el *Grupo técnico asesor sobre documentos de viaje de lectura mecánica (TAG/MRTD)* compuesto por personas funcionarias gubernamentales especializadas en la expedición e inspección fronteriza de pasaportes y otros documentos de viaje. Más tarde las atribuciones de este grupo fueron ampliándose para incluir, primero la elaboración de especificaciones para visados de lectura mecánica y después para tarjetas de lectura mecánica que pudieran emplearse como documentos oficiales de viaje.

En 1998, el Grupo de trabajo sobre nuevas tecnologías del TAG/MRTD inició su labor para establecer el sistema de identificación biométrica más eficaz y los correspondientes medios de almacenamiento de datos para usar en aplicaciones MRTD, en particular en relación con la expedición de documentos y consideraciones de inmigración. La mayor parte de esta labor ya había finalizado para cuando los sucesos del 11 de septiembre de 2001 hicieron que los Estados asignaran mayor importancia a la seguridad de los documentos de viaje y a la identificación de sus titulares. La labor en cuestión fue rápidamente finalizada y apoyada por el TAG/MRTD y el Comité de Transporte aéreo.

Los informes técnicos resultantes sobre el empleo de biometría y tecnología de circuitos integrados sin contacto, estructura lógica de datos (LDS) e infraestructura de clave pública (PKI) se incorporaron en el Volumen 2 de la sexta edición del Doc 9303, Parte 1 (*Pasaportes de lectura mecánica*) en 2006, y en el Volumen 2 de la tercera edición del Doc 9303, Parte 3 (*Documentos de viaje oficiales de lectura mecánica*) en 2008.

2. ALCANCE

El Doc 9303 integra diversos documentos independientes en los cuales se agrupan especificaciones de carácter general (aplicables a todos los MRTD) así como específicas sobre el formato de esos documentos. En la sección 5.1 “Estructura del Doc 9303” figura una reseña general.

Estas especificaciones no tendrían carácter de normas para los documentos nacionales de identidad. No obstante, un Estado cuyos documentos de identidad son reconocidos por otros Estados como documentos de viaje válidos diseñará estos documentos de identidad de modo que se ajusten a las especificaciones de los Doc 9303-3, Doc 9303-4, Doc 9303-5 o Doc 9303-6.

Aunque las especificaciones que figuran en el Doc 9303-4 están concebidas para aplicarse en particular al pasaporte, dichas especificaciones se aplican igualmente a otros documentos de identidad de tamaño DV3, por ejemplo, el laissez-passer, el documento de identidad de la gente de mar y los documentos de viaje para refugiados.

El presente documento es la Parte 1. En ella se introducen las especificaciones del Doc 9303 y se describe la estructura de las trece partes del Doc 9303, se proporciona información general sobre la OACI, así como orientación relativa a la terminología y abreviaturas empleadas en dichas especificaciones.

3. CONSIDERACIONES GENERALES

3.1 Liderazgo de la OACI

La iniciativa de la OACI de redactar especificaciones normativas para pasaportes y otros documentos de viaje siguió la tradición establecida por las conferencias de la Liga de las Naciones sobre pasaportes en los años veinte, así como la labor de su sucesora, la Organización de las Naciones Unidas. El mandato de la OACI de perseverar en su función de liderazgo tiene su origen en el Convenio sobre Aviación Civil Internacional (“Convenio de Chicago”) que abarca una gama completa de requisitos para que las operaciones de aviación civil se ejerzan en forma eficiente y ordenada, lo cual comprende disposiciones para el despacho de personas por los puntos de control fronterizos, o sea:

a) el requisito de que las personas que viajen por vía aérea y las tripulaciones de aeronaves obedezcan los reglamentos de inmigración, aduanas y pasaportes (Artículo 13);

b) el requisito de que los Estados simplifiquen las formalidades para el cruce de fronteras y eviten todo retardo innecesario (Artículo 22);

c) el requisito de que los Estados colaboren en estos asuntos (Artículo 23); y

d) el requisito de que los Estados elaboren y adopten normas y procedimientos internacionales respecto a las formalidades de aduana e inmigración [Artículo 37 j)].

Siguiendo este mandato, la OACI redacta y mantiene normas internacionales en el Anexo 9 — *Facilitación,* del Convenio de Chicago, que los Estados miembros han de poner en práctica. En la elaboración de tales normas es precepto fundamental que, si las autoridades públicas han de facilitar las formalidades de inspección para la inmensa mayoría del público viajero usuario del transporte aéreo, esas mismas autoridades tengan un grado satisfactorio de confianza en la fiabilidad de los documentos de viaje y en la eficacia de los procedimientos de inspección. La creación de especificaciones estándar para los documentos de viaje y los datos contenidos en ellos está encaminada a nutrir esa confianza.

En 2004, la Asamblea de la OACI afirmó que la Organización debería emprender con carácter altamente prioritario la labor de cooperación respecto a especificaciones para reforzar la seguridad y la integridad de los documentos de viaje. Además de la Organización Internacional de Normalización (ISO), las entidades consultoras del TAG/MRTD comprenden a la Asociación del Transporte Aéreo Internacional (IATA), el Consejo Internacional de Aeropuertos (ACI), y la Organización Internacional de Policía Criminal (INTERPOL).

En 2005, los 188 Estados miembros de la OACI existentes en esa fecha aprobaron la nueva norma de que todos los Estados debían comenzar a expedir pasaportes de lectura mecánica con arreglo al Doc 9303, no más allá del año 2010. A más tardar para el año 2015 deben haber caducado todos los documentos de viaje que no son de lectura mecánica. La norma al respecto se publica en la decimotercera edición (2011) del Anexo 9 — *Facilitación*.

3.2 Costos y ventajas relativas de los documentos de viaje de lectura mecánica

La experiencia acumulada en la expedición de pasaportes de lectura mecánica, según las especificaciones establecidas en el Doc 9303, indica que el costo de producir los MRTD tal vez no sea mayor que el de imprimir los documentos tradicionales, aunque el costo será más elevado cuando se implanten la identificación biométrica y los documentos de viaje electrónicos. Según aumenta el volumen del tráfico y los Estados se concentran cada vez más en la forma de racionalizar los trámites de despachar viajeros mediante el empleo de bases de datos computadorizadas y el intercambio electrónico de estos datos, los MRTD desempeñan un papel cardinal en todo sistema moderno dedicado a ese fin. Puede que la adquisición del equipo necesario para leer documentos y acceder a las bases de datos entrañe una inversión

considerable, pero se prevé que tal inversión quede compensada con las resultantes mejoras en materia de seguridad, rapidez de despacho y confianza en la exactitud de la verificación que tales sistemas proporcionan. El uso de los MRTD en los sistemas de despacho automatizados puede permitir a los Estados prescindir de documentos en papel tales como los manifiestos de pasajeros y las tarjetas de embarque/desembarque, eliminando así los costos administrativos relacionados con los procedimientos manuales conexos.

3.3 Operaciones

El documento básico de viaje de lectura mecánica con su legibilidad por OCR, está dirigido tanto a la lectura visual como mecánica.

Los Estados miembros de la OACI han reconocido que la normalización es una necesidad y que las ventajas de adoptar los formatos normalizados del Doc 9303 para pasaportes y otros documentos de viaje trascienden las obvias ventajas para aquellos Estados que cuentan con lectores mecánicos y bases de datos para utilizar en los sistemas de despacho automático. De hecho, las características físicas y los elementos de seguridad de los datos de los propios documentos ofrecen una fuerte defensa contra alteraciones, falsificaciones o imitaciones fraudulentas. Además, la adopción del formato normalizado para la zona visual de un MRTD facilita su inspección por parte de las líneas aéreas y de los funcionarios gubernamentales, con lo cual se acelera el despacho de los pasajeros de poco riesgo, se reconocen más fácilmente los casos problemáticos y se facilita el cumplimiento de las leyes. La introducción opcional de la identificación biométrica con los datos almacenados en los circuitos integrados sin contacto brindará mayor seguridad y resistencia al fraude y, de esta forma, facilitará la obtención de visados para viaje por el titular legítimo del documento y su procesamiento a través de los sistemas de inspección fronteriza.

Nota.— Se reconoce que surgirán situaciones en que un eMRTD no interactuará correctamente con un lector en una frontera. Hay varias razones para ello, siendo la falla del eMRTD solo una de ellas. La OACI hace hincapié en que un eMRTD que no logre leerse es, no obstante, un documento válido. Sin embargo, la falla de la lectura podría ser resultado de un ataque fraudulento y el Estado receptor debería establecer sus propios procedimientos para lidiar con esta posibilidad, que deberían entrañar una inspección más estricta del documento y de quien sea su titular, pero también tener en cuenta que dicha falla podría no deberse a intenciones fraudulentas.

3.4 Aprobación de la ISO

Las secciones relativas a las especificaciones técnicas del Doc 9303 han recibido la aprobación de la Organización Internacional de Normalización con carácter de norma ISO 7501. Esta aprobación se hace posible mediante un mecanismo de enlace que permite a los fabricantes de documentos de viaje, dispositivos de lectura mecánica y otras tecnologías, proporcionar asesoramiento técnico al TAG/TRIP bajo los auspicios de la ISO. Mediante esta relación de trabajo las especificaciones de la OACI han alcanzado, y se espera que continúen recibiendo, la categoría de normas mundiales empleando un procedimiento simplificado dentro de la ISO.

El mecanismo de enlace con la ISO se ha empleado con éxito no sólo para avalar nuevas especificaciones de documentos de viaje como normas ISO, sino también para aprobar enmiendas de las especificaciones. Por consiguiente, las revisiones que se hagan más adelante al Doc 9303 se tramitarán del mismo modo que antes se hacía para obtener la aprobación de la ISO.

4. DEFINICIONES Y REFERENCIAS

4.1 Acrónimos

Acrónimo	Texto completo
3DES	Triple DES
AA	Autenticación activa
ABC	Control fronterizo automatizado
AES	Norma criptográfica avanzada
AFS	Especialista antifraude
AID	Identificador de aplicación
AO	Funcionario autorizante
APDU	Unidad de datos del protocolo de aplicación
BAC	Control de acceso básico
BER	Reglas de codificación básicas
BLOB	Objeto binario grande
BSC	Certificado de firmante de código de barras
CA	Autoridad de certificación – también – Autenticación de microplaqueta
CAM	Correspondencia de autenticación de microplaqueta
CAN	Número de acceso de tarjeta
CAR	Referencia de autoridad de certificación
CBC	Cadena de bloques cifrados
CBEFF	Marco común de formatos de intercambio biométrico
CCD	Dispositivo acoplado cargado
C_{DS}	Certificado de firmante de documento
CIC	Circuito integrado sin contacto
CI	Circuito integrado
CID	Identificación de tarjeta
CMAC	Código de autenticación de mensaje basado en cifrado
CMOS	Semiconductor complementario de óxido metálico
CRL	Lista de revocación de certificados
CSCA	Autoridad de certificación de firma de país
CSD	Distancia entre la cámara y sujeto; distancia entre el plano de los ojos de una persona y el centro óptico de la lente de la cámara
CVCA	Autoridad de certificación de verificación de país

Acrónimo	Texto completo
DER	Regla de codificación distinguida
DES	Norma de cifrado de datos
DF	Fichero especializado
DG	Grupo de datos
DH	Diffie Hellmann
DN	Nombre distinguido
DO	Objeto de datos
DOVID	Dispositivo de imágenes difrangentes ópticamente variables (función con efectos de imágenes difrangentes ópticamente variables; p.ej., efectos holográficos)
DS	Firmante del documento
DSA	Algoritmo de firma digital
DTA	Autorización electrónica de viaje
DTBS	Datos que deben firmarse
DV	Verificador del documento
DV1	Documento oficial de viaje de lectura mecánica de tamaño 1
DV2	Documento oficial de viaje de lectura mecánica de tamaño 2
DV3	Documento oficial de viaje de lectura mecánica de tamaño 3
EAL	Nivel de garantía de evaluación
ECDH	Curva elíptica Diffie Hellmann
ECDSA	Algoritmo de firma digital de curva elíptica
ECKA	Acuerdo de clave de curva elíptica
EEPROM	Memoria de solo lectura programable de borrado eléctrico
EF	Fichero elemental
EM	Distancia entre el ojo y la boca
eMROTD	Documento oficial de viaje de lectura mecánica electrónico
eMRP	Pasaporte de lectura mecánica electrónico
eMRTD	Documento de viaje de lectura mecánica electrónico
eRP	Permiso de residencia electrónico
ETS	Sistema electrónico de viaje
EVZ	Zona de visibilidad de los ojos. Zona que abarca un rectángulo de una distancia V desde cualquier parte del globo ocular visible, que equivale como mínimo al 5% de la distancia de separación entre los ojos (IED).
FAR	Proporción de aceptaciones falsas
FIPS	Norma federal de procesamiento de la información

Acrónimo	Texto completo
FRR	Proporción de rechazos falsos
GM	Correspondencia genérica
HD	Ángulo de desviación horizontal; desviación máxima permitida desde la horizontal de la línea imaginaria entre la nariz de una persona y la lente de la cámara
ICC	Tarjeta de circuito integrado
IED	Distancia entre los ojos
IFD	Dispositivo de interfaz
IM	Correspondencia integrada
IR	Luz/Radiación infrarroja
IS	Sistema de inspección
IV	Vector inicial
LDS	Estructura lógica de datos
MAC	Código de autenticación de mensajes
MF	Fichero maestro
MROTD	Documento oficial de viaje de lectura mecánica en forma de tarjeta
MRP	Pasaporte de lectura mecánica
MRTD	Documento de viaje de lectura mecánica
MRV-A	Visado de lectura mecánica de tamaño normal (Formato A)
MRV-B	Visado de lectura mecánica de tamaño pequeño (Formato B)
MTF	Función de transferencia de modulación
MTF20	Máxima frecuencia espacial cuando la MTF es del 20% o mayor
NAD	Dirección de nodo
NIST	Instituto Nacional de Normas y Tecnología
NTWG	Grupo de trabajo sobre nuevas tecnologías
OACI	Organización de Aviación Civil Internacional
OCR	Reconocimiento óptico de caracteres
OCR-B	Tipo de letra para reconocimiento óptico de caracteres definido en la ISO 1073-2
OID	Identificador de objeto
OVD	Dispositivo ópticamente variable
OVF	Elemento ópticamente variable
OVI	Tinta ópticamente variable
PACE	Establecimiento de conexión autenticada por contraseña
PCD	Dispositivo de acoplamiento de proximidad
PICC	Tarjeta con circuito integrado de proximidad

Acrónimo	Texto completo
PIX	Extensión del identificador registrado/de propiedad (PIX)
PKD	Directorio de claves públicas
PKI	Infraestructura de clave pública
RID	Identificador registrado (RID)
RFID	Identificación por radiofrecuencia
RGB	Rojo-verde-azul
ROI	Región de interés
ROM	Memoria de solo lectura
RSA	Rivest, Shamir y Adleman
SFR	Respuesta de frecuencia espacial
SHA	Algoritmo de condensación (hash) seguro
SM	Construcción segura de mensajes
SNR	Radio de señal a ruido
SO_D	Objeto de seguridad de documento
SPOC	Punto de contacto único
sRGP	Espacio cromático RGB estándar creado para uso en monitores, impresoras y la Internet usando los primarios de la norma ITU-R BT.709
SSC	Contador de secuencia de envío
TA	Autenticación en la terminal
TAG/MRTD	Grupo técnico asesor sobre los documentos de viaje de lectura mecánica
TAG/TRIP	Grupo técnico asesor sobre el Programa de identificación de viajeros
TLV	Valor de longitud de rótulo
TR	Informe técnico
UID	Identificador único
UV	Luz/Radiación ultravioleta
VDS	Sello digital visible
VIS	Sistema de información de visados de la Unión Europea
VS	Firmante de visado
VVA	Autoridad de validación de visado
WSQ	Cuantificación escalar de onda pequeña
ZIV	Zona de inspección visual
ZLE	Zona de lectura efectiva
ZLM	Zona de lectura mecánica

4.2 Términos y definiciones

Término	Definición
Acceso aleatorio	Medio de almacenar datos por el cual pueden recuperarse datos específicos sin necesidad de recorrer en orden todos los datos almacenados.
Aceptación falsa	Cuando un sistema biométrico identifica incorrectamente a un individuo o verifica incorrectamente a un impostor con respecto a una pretendida identidad.
Adobe RGB	Espacio de color RGB (rojo-verde-azul) diseñado para incluir todos los colores que se obtienen con impresoras d colores CMYK (cian, magenta, amarillo y negro), pero utilizando los colores primarios RGB en un dispositivo como una pantalla de computadora.
Alcance de lectura	Distancia práctica máxima entre el CI sin contacto con su antena y la distancia de lectura.
Algoritmo	Proceso matemático especificado para computación; conjunto de reglas que, si se las aplica, darán un resultado prescrito.
Algoritmo asimétrico	Tipo de operación criptográfica que utiliza una clave para el cifrado de texto claro y otra clave para el descifrado del texto cifrado conexo. Estas dos claves se relacionan entre sí y se denominan par de claves.
Algoritmo de bloque	Véase: Cifra de bloque.
Algoritmo de condensación seguro (SHA)	Función de correspondencia especificada por el NIST y publicada como norma federal de procesamiento de información FIPS-180.
Algoritmo de firma digital (DSA)	Algoritmo asimétrico publicado por el NIST en la FIPS 186. Este algoritmo solo proporciona una función de firma digital.
Algoritmo de verificación	Componentes del soporte lógico que permiten aplicar rutinas de verificación (p.ej., buscar patrones)
Algoritmo simétrico	Tipo de operación criptográfica que utiliza la misma clave o conjunto de claves para cifrado de texto claro y descifrado del texto cifrado conexo.
Alteración fraudulenta	Alteración de un documento genuino para uso en viaje de una persona no autorizada o hacia un destino no autorizado. Los detalles personales del titular genuino, particularmente el retrato, son el objetivo principal de dicha alteración.
Asimétrico	Distintas claves necesarias en cada extremo de un enlace de comunicación.
Ataque de presentación	Presentación al subsistema de captura biométrica de un artefacto de características humanas de tal modo que, podría interferir con la política concebida para el sistema biométrico.
Autenticación	Proceso que valida la identidad alegada de un participante en una transacción electrónica.
Autenticidad	Capacidad de confirmar que la estructura lógica de datos y sus componentes fueron creados por el Estado u organización expedidores.
Autoridad de certificación (CA)	Órgano fiable que expide certificados digitales para PKI.

Término	Definición
Autoridad de registro (RA)	Persona u organización responsable de la identificación y autenticación de un solicitante de certificado digital. Esta autoridad no expide o firma certificados.
Autoridad de validación de visado (VVA)	Autoridad que valida un sello digital visible basándose en un visado ajustado a una política de validación.
Autoridad expedidora	Entidad acreditada para la expedición de un MRTD al titular legítimo.
Autorización	Procedimiento de seguridad para decidir si puede brindarse o no un servicio.
Autorización de viaje	Autorización, física o no física, expedida por el Estado receptor, mediante la cual se autoriza a la persona a viajar.
Autorización electrónica de viaje	Visado electrónico expedido y mantenido en el Estado emisor.
Base de datos de autenticación	In esta base de datos se almacenan para cada modelo de documento los algoritmos de autenticación para la aplicación de las rutinas de verificación.
Biometría	Característica física o rasgo de comportamiento personal singular y medible, utilizado para reconocer la identidad o verificar la pretendida identidad de una persona.
Bit	Dígito binario. La unidad de información más pequeña posible en un código digital.
Bloque	Cadena o grupo de bits sobre el que opera un algoritmo de bloque.
Bloque de datos del expedidor	Serie de grupos de datos escritos por el Estado expedidor u organización expedidora en la tecnología de expansión de capacidad opcional.
Bloque de datos del receptor	Serie de grupos de datos escritos por el Estado receptor u organización receptora autorizada en la tecnología de expansión de capacidad opcional.
Bloqueada (microplaqueta)	Después de la personalización, la microplaqueta DEBE bloquearse. Esto significa que se impedirá la ejecución de comandos de personalización y la escritura de datos de personalización en la microplaqueta. Sólo será posible escribir datos si se ejecuta con éxito un mecanismo de autenticación (TA). Una microplaqueta que ha sido bloqueada no podrá desbloquearse.
Byte	Secuencia de ocho bits que funciona normalmente como una unidad.
Cabina para toma de fotografías	Sistema automatizado para la captura digital de fotografías de identidad en entornos públicos o en oficinas; la persona (la/el sujeto) ingresa a un recinto de iluminación bien controlada que consta de una cámara, iluminación y dispositivos periféricos, como impresoras; tiene entrada por uno o ambos lados con cortinas reflectivas de protección contra la luz ambiental.
Captación	Método de obtener una muestra biométrica del usuario final.
Captación en vivo	Proceso de captar una muestra biométrica mediante una interacción entre el titular de un MRTD y un sistema biométrico.
Característica	Elemento de un documento adecuado para la prueba de autenticidad (p.ej.: Fotografía IR absorbente)

Término	Definición
Característica biométrica de interfuncionamiento mundial	Se refiere a la imagen facial como se establece en el Doc 9303-9.
Característica biométrica de verificación mecánica	Característica de identificación personal física y de carácter único (p. ej., imagen facial, huella digital o iris) almacenada en forma electrónica en el CI de un eMRTD.
Característica biométrica múltiple	Empleo de más de una característica biométrica.
Característica (digital) de documento	Propiedad de un documento que puede usarse para verificar el contenido del documento. Puede ser la información textual como el nombre de quien sea titular, o la fecha de expedición, o una imagen impresa de quien sea titular del documento. Una característica digital de un documento es la versión digitalizada de una característica de documento.
Casilla	Espacio concreto para un dato individual dentro de una zona.
Caso de aplicación 1:1	Proceso biométrico (algoritmo) que compara una fotografía de muestra con una muestra registrada de la identidad pretendida, también conocido como verificación.
Caso de aplicación 1:N	Proceso biométrico (algoritmo) que busca una fotografía no conocida de antemano entre N-muestras registradas en una base de datos, también conocido como identificación.
Centro del ojo	Centro de la línea que conecta la esquina interior con la esquina exterior del ojo. *Nota 1.— Los centros de los ojos son los puntos de característica 12.1 y 12.2 conforme se definen en la norma ISO/IEC 14496-2.* *Nota 2.— Las esquinas interior y exterior del ojo se definen con arreglo a la norma ISO/IEC 14496-2. Son los puntos de característica 3.12 y 3.8 del ojo derecho, y 3.11 y 3.7 del ojo izquierdo.*
Centro del rostro	Centro de la línea que conecta los dos centros de los ojos
Certificado	Fichero electrónico que confirma que un par de claves criptográficas pertenecen a la persona o a al componente de equipo o de programa lógico que se identifica en el certificado. Los certificados los expide una Autoridad de certificación. Al firmar el certificado la Autoridad de certificación aprueba la relación entre la identidad de la persona y el par de claves criptográficas o entre el componente y el par de claves criptográficas. El certificado puede ser revocado si ya no se valida dicha relación. El certificado tiene una validez limitada.
Certificado de clave pública	Información de clave pública de una entidad firmada por la autoridad de certificación y con ello hecha inolvidable.
Certificado de firmante de código de barras (BSC)	Un BSC es un certificado que contiene la clave pública del firmante del código de barras. Los certificados de firmante de código de barras se utilizan para verificar la validez de los datos que se firmaron con la clave privada del firmante del código de barras.
Certificado de firmante de visado	Certificado que contiene información que identifica a la entidad que firmó un sello digital visible en un visado, y que contiene la clave pública que corresponde a la clave pública con la cual se creó la firma.

Término	Definición
Certificado X.509 v3	Documento electrónico reconocido internacionalmente empleado para comprobar la identidad y la propiedad de la clave pública en una red de comunicación. Contiene el nombre del expedidor, la información de identidad del usuario y la firma digital del expedidor.
Cifra de bloque	Algoritmos que operan sobre texto claro en bloques (cadenas o grupos) de bits.
Cifrado	Escritura secreta basada en una clave o conjunto de reglas o símbolos predeterminados.
Cifrar	Acción de ocultar información mediante el uso de una clave para que no pueda ser comprendida por una persona no autorizada.
Circuito integrado (CI)	Componente electrónico diseñado para realizar funciones de procesamiento o memoria.
Circuito integrado sin contacto	Dispositivo semiconductor que almacena datos del MRTD y que se comunica con un lector utilizando energía de radiofrecuencia con arreglo a ISO/IEC 14443.
Clave maestra	Raíz de la cadena de derivación para claves.
Clave privada	Componente privado de un par de claves asimétricas integradas conocido solamente por el usuario, empleado en criptografía de clave pública para descifrar o firmar información.
Clave pública	Componente público de un par de claves asimétricas integradas, utilizadas para cifrar o verificar información.
Claves asimétricas	Par de claves de usuario separadas pero integradas formado por una clave pública y una clave privada. Cada clave es unidireccional, es decir, que una clave utilizada para cifrar información no puede utilizarse para descifrar la misma información.
Código de autenticación de mensaje (MAC)	Un MAC es un compendio de mensaje adjunto al propio mensaje. El MAC no puede computarse o verificarse a menos que se conozca un código secreto. Es añadido por el remitente y verificado por el receptor que puede así detectar una falsificación de mensaje.
Código de barras	Representación óptica de lectura mecánica, en una o dos dimensiones, de los datos relativos al objeto en el cual se encuentre ubicado.
Código de país	Código de dos o tres letras según se define en ISO 3166-1, utilizado para designar la autoridad expedidora de un documento o la nacionalidad del titular del documento.
Comparación	Proceso de comparar una muestra biométrica con respecto a una plantilla o plantillas almacenadas previamente (véase también “uno a muchos” y “uno a uno”).
Compuesto marcador	Compuesto de sustancias que no son de origen natural que puede añadirse a los componentes físicos de un MRTD y que constituyen normalmente una característica de nivel 3, que requiere equipo especial para su detección.
Condensación	Fórmula matemática que convierte un mensaje de cualquier longitud en una cadena de dígitos única de longitud fija conocida como “compendio de mensajes” que representa el mensaje original. La función hash es unidireccional, es decir, que es imposible invertir el proceso para determinar el mensaje original. Además, esta función no producirá el mismo compendio de mensaje a partir de dos entradas diferentes.
Conjunto de datos de referencia	Las imágenes visuales, IR, y UV de un documento de referencia definen las rutinas de verificación para un modelo de documento correspondiente.

Término	Definición
Conjunto de datos para autenticación	Conjunto específico de rutinas de verificación para un modelo de documento dentro de la base de datos de autenticación.
Conjunto de documentos de referencia	Conjunto de documentos cuyo conjunto de datos de referencia se utilizan para definir las rutinas de verificación.
Coronilla	Parte superior de la cabeza sin contar el pelo.
Cotejo/cotejar	Proceso de comparar una muestra biométrica con respecto a una plantilla almacenada previamente y medir el nivel de similitud. La decisión de aceptar o rechazar se basa luego en el hecho de que dicha medida supere o no un determinado umbral.
Criptografía	Ciencia de transformar información en una forma cifrada e ininteligible por medio de un algoritmo y una clave.
Criptografía de clave pública	Forma de cifrado asimétrico en el que todas las partes poseen un par de claves, una privada y una pública, para uso en cifrado y firma digital de datos.
Cuantificación escalar de onda pequeña (WSQ)	Medio de comprimir datos empleados en particular con relación al almacenamiento de imágenes de huellas digitales.
Datos biográficos (biodatos)	Información personal del portador del documento que aparece en forma de texto en las zonas de inspección visual y de lectura mecánica de la página de datos personales de un MRTD, o en el circuito integrado en caso de haberla.
Datos biométricos	Información extraída de la muestra biométrica y utilizada para construir una plantilla de referencia (datos de plantilla) o para comparar con respecto a alguna plantilla de referencia creada anteriormente (datos de comparación).
Datos para firmar (DTBS)	Mensaje que se entrega como entrada a un algoritmo de generación de firma de un plan de firmas.
Datos sensibles	Estos datos se consideran como más sensibles con respecto a la privacidad que los datos no sensibles. El acceso a los datos sensibles DEBERÍA ser más restringido. En el Doc 9303-11 se especifica la autenticación del terminal como un mecanismo interoperable para acceder a datos sensibles. Si no se necesita la interoperabilidad, pueden emplearse otros mecanismos.
Descifrado	Restauración de un archivo cifrado a su estado original mediante uso de una clave.
Despumado (skimming)	Lectura electrónica de los datos almacenados en el CI sin contacto sin que se haya autorizado esa lectura del documento.
Detección de ataque de presentación	Determinación automatizada de un ataque de presentación.
Directorio de claves públicas de la OACI	Base de datos central que sirve como depósito para certificados de firmante de documentos, listas maestras CSCA, certificados de enlace de CA de firma de país y listas de revocación de certificado expedida por los participantes, conjuntamente con un sistema para su distribución mundial mantenido por la OACI en nombre de los participantes a efectos de facilitar la validación de datos en los eMRTD.

Término	Definición
Directorio/Directorio de claves públicas (PKD)	Depósito para almacenar información. Normalmente, un directorio para una PKI particular es un depósito para certificados cifrados de clave pública expedidos por la Autoridad de certificación de esa PKI, junto con otra información sobre el cliente. El Directorio también mantiene certificados cruzados, listas de revocación de certificados y listas de revocación de autoridad.
Diseño de Guilloche	Patrón de líneas finas continuas, generalmente creadas por computadora, que forman una imagen de naturaleza única que solo puede volverse a original con exactitud si se tiene acceso al equipo, al soporte lógico y a los parámetros empleados para crear el diseño original.
Diseño de líneas negras y blancas	Diseño compuesto de líneas finas, a menudo bajo la forma de un patrón de Guilloche, empleado algunas veces como borde en los documentos de seguridad. El patrón cambia de imagen positiva a negativa a medida que va avanzando a través de la página.
Diseño doble	Diseño a base de un patrón con entrelazado de pequeñas formas irregulares, impreso en dos o más colores y que requiere una impresión del registro muy exacta a fin de preservar la integridad de la imagen.
Diseño en relieve (3-D) (medallón)	Diseño de fondo de seguridad que incluye una imagen generada para dar la impresión de estar resaltada o repujada en la superficie del sustrato.
Dispositivo de interfaz	Todo dispositivo de comunicación terminal o máquina a la que se conecte eléctricamente la ICC durante el funcionamiento.
Dispositivo difrangente ópticamente variable	Característica de seguridad que contiene una imagen holográfica o equivalente en su construcción, que cambia de apariencia según el ángulo de visión o la iluminación.
Dispositivo ópticamente variable (OVD)	Elemento de seguridad que presenta diferentes colores o apariencia de imagen según el ángulo de visión o condiciones de verificación.
Distancia entre el ojo y la boca	Distancia entre el centro de la cara M y el punto medio de la boca (punto de característica 2.3 conforme a ISO/IEC 14496-2)
Distorsión por aumento	Distorsión de la imagen cuando el grado de aumento varía en función de la distancia desde la cámara y la profundidad de la cara.
Distorsión radial	Imperfección de la imagen cuando el grado de aumento varía en función de la distancia desde el eje óptico.
Documento de identidad	Documento utilizado para identificar a su titular y expedidor, que puede contener datos requeridos para el uso previsto del documento.
Documento de viaje de lectura mecánica (MRTD)	Documento oficial, conforme a las especificaciones del Doc 9303, expedido por un Estado u organización que el titular emplea en viajes internacionales (p. ej., MRP, MRV, MROTD) y que contiene datos visuales (lectura ocular) obligatorios y un resumen de datos obligatorio por separado en formato capaz de leerse mecánicamente.
Documento de viaje de lectura mecánica electrónico (eMRTD)	MRTD (pasaporte, visado o tarjeta) que incorpora un circuito integrado sin contacto, así como la capacidad de emplearse para identificación biométrica de quien es titular del MRTD con arreglo a las normas especificadas en la Parte pertinente del Doc 9303 — *Documentos de viaje de lectura mecánica*.

Término	Definición
Documento de viaje de lectura mecánica oficial electrónico (eMROTD)	MROTD de tamaño DV1 y DV2 que se ajusta a las especificaciones del Doc 9303-5 y del Doc 9303-6 respectivamente, al que se incorpora además un circuito integrado sin contacto que incluye la capacidad de identificación biométrica de su titular.
Documento generador	Documentación empleada como prueba de identidad cuando se solicita un documento de viaje.
Documento oficial de viaje de lectura mecánica (MROTD)	Documento, normalmente en forma de tarjeta de tamaño DV1 o DV2, que se ajusta a las especificaciones del Doc 9303-5 y del Doc 9303-6 y puede utilizarse para cruzar fronteras internacionales por acuerdo entre los Estados involucrados.
Documento oficial de viaje de lectura mecánica de tamaño 1 (DV1)	Tarjeta con dimensiones nominales orientadas por las especificaciones para la tarjeta de tipo ID-1 (ISO/IEC 7810) (excluyendo el espesor).
Documento oficial de viaje de lectura mecánica de tamaño 2 (DV2)	Tarjeta o etiqueta que se ajusta a las dimensiones definidas para la tarjeta del tipo ID-2 (ISO/IEC 7810) (excluyendo el espesor).
Documentos en blanco	Documentos de viaje que no contienen datos personales del titular del documento. Normalmente los documentos en blanco constituyen el material básico a partir del cual se crean los documentos de viaje personalizados.
Elemento datos	Incorporación de información codificada en los datos del documento o estructura de la imagen, normalmente en los datos personales, especialmente el retrato.
Elemento estructura	Un elemento estructura entraña la incorporación en, o sobre, el MRTD de una estructura medible. La presencia de la estructura puede detectarse y medirse por la máquina de detección.
Elemento lenticular	Característica de seguridad en la cual se integra una estructura de lente en la superficie del documento o que se utiliza como dispositivo de verificación.
Elemento ópticamente variable (OVF)	Imagen o elemento cuya apariencia en cuanto al color o al diseño cambia según el ángulo de visión o iluminación, por ejemplo, elementos que incluyen estructuras de difracción con alta resolución (dispositivo de imágenes difrangentes ópticamente variables/DOVID), hologramas, tintas de color variable (p. ej., tinta con propiedades ópticamente variables) y otros materiales difrangentes o reflectantes.
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 a la inspección visual. La presencia del material puede detectarse mediante la presencia y magnitud de una propiedad adecuada de la sustancia añadida.
Elemento táctil	Elemento superficial que da una textura singular al documento.
Equiparación biométrica	Proceso de aplicar un algoritmo que compara plantillas obtenidas de la referencia biométrica y de los datos biométricos en vivo, y que resultan en la determinación de una correspondencia o ausencia de la misma.
Escucha furtiva	Interceptación no autorizada de comunicaciones de datos.

Término	Definición
Estado expedidor	País que expide el MRTD.
Estado receptor	País que inspecciona el MRTD del titular.
Esteganografía	Imagen o información codificada u oculta dentro de una imagen visual principal.
Estructura lógica de datos (LDS)	La estructura lógica de datos describe la forma en que se almacenan y formatean los datos en el CI sin contacto de un eMRTD.
Etiqueta	Autoadhesivo que se utiliza como página de datos en el pasaporte. En general no se recomienda esta práctica, en particular para documentos con validez prolongada.
Expedidor	Organización que expide documentos MRTD.
Extracción	Proceso de convertir en datos biométricos una muestra biométrica captada de modo que pueda compararse con una plantilla de referencia.
Factor de recorte	Relación de la diagonal de la cámara de formato completo (43,3 mm) con respecto al sensor de imagen de la cámara seleccionada. Se puede determinar la lente de la distancia focal adecuada para un campo visual equivalente a una cámara de formato completo teniendo en cuenta el factor de recorte.
Falla de adquisición	Falla de un sistema biométrico en obtener las características biométricas necesarias para inscribir una persona.
Falla de inscripción	Falla de un sistema biométrico en la inscripción de una persona.
Falsificación	Alteración fraudulenta de cualquier parte del documento genuino.
Fibras	Pequeñas partículas en forma de hilos que se incorporan a un sustrato durante su fabricación.
Filigrana	Diseño que por lo general contiene una grabación de tonalidades, que se forma en el papel o en otro sustrato durante su fabricación, se crea mediante el desplazamiento de materiales y es visible al trasluz.
Filigrana digital	Véase: Esteganografía.
Firma desplegada	Firma original escrita o reproducción de su original impresa digitalmente.
Firma digital(criptográfica)	Resultado de una operación criptográfica que permite validar información por medios electrónicos. Esta firma NO es la firma presentada del titular del MRTD expresada en forma digital.
Firma exhibida	Firma escrita original o reproducción del original impresa en forma digital.
Firmante de lista maestra	Entidad que firma en forma digital una lista maestra de certificados CSCA. El firmante de lista maestra está autorizado por su CSCA nacional para ejecutar esa función mediante la expedición de un certificado de firmante de lista maestra.
Firmante de lista de desviaciones	Entidad que firma en forma digital una lista de desviaciones. El firmante de lista de desviaciones está autorizado por su CSCA nacional para desempeñar esta función mediante la expedición de un certificado de firmante de lista de desviaciones.
Firmante del código de barras	Un firmante de código de barras firma digitalmente los datos (encabezamiento y mensaje) codificados en el código de barras. La firma también se almacena en el código de barras.

Término	Definición
Firmante del documento	Órgano que expide un documento biométrico y certifica que los datos almacenados en él son genuinos de forma que permitirá la detección de alteraciones fraudulentas.
Firmante del visado (VS)	La autoridad que recibe los datos de un Sistema de personalización de visados y que utiliza un certificado VS y la clave privada correspondiente para cifrar y firmar el sello digital visible
Fuera de banda	Se refiere a las comunicaciones que tienen lugar fuera de un método o canal de comunicación previamente establecido.
Fuerza bruta (ataque)	Probar con todas las claves posibles y verificar si el texto claro resultante tiene sentido.
Galería	Base de datos de plantilla biométricas de personas inscritas previamente, que puede explorarse para encontrar una prueba.
Gestión de claves	Proceso por el cual se proporcionan claves criptográficas para uso entre partes comunicantes autorizadas.
Grabado láser	Proceso mediante el cual los datos personalizados se “queman” con láser dentro del sustrato. Los datos pueden contar de texto, imágenes de retrato y otros elementos de seguridad.
Grupo de datos	Serie de elementos de datos conexos agrupados dentro de la estructura lógica de datos.
Hilo de seguridad	Tira delgada de plástico o de otro material total o parcialmente incorporada en el sustrato durante el proceso de fabricación del papel. La tira puede estar metalizada o parcialmente desmetalizada.
Hoja	Cada pieza de sustrato en un pasaporte que contiene más de una página de pasaporte.
Huellas digitales	Una o más representaciones visuales de la superficie de las yemas de los dedos del titular.
Identidad	Conjunto colectivo de características personales y físicas distintivas, datos y cualidades que permiten que se identifique definitivamente a una persona con respecto a otras. En un sistema biométrico, la identidad se establece normalmente cuando la persona se registra en el sistema mediante el uso de los denominados “documentos generadores” como el certificado de nacimiento y el certificado de ciudadanía.
Identificación biométrica	Medios de identificar o confirmar la identidad del titular de un MRTD, mediante la medición y validación de una o más propiedades singulares de la persona del titular.
Identificación/identificar	Proceso de uno a varios de cotejar una muestra biométrica presentada con todas las plantillas de referencia biométrica almacenadas para determinar si se corresponde con alguna de éstas y, de ser así, la identidad del portador del eMRTD cuya plantilla corresponde. El sistema biométrico que utiliza el enfoque de uno a varios procura encontrar una identidad dentro de una base de datos en vez de verificar una pretendida identidad. Compárese con “Verificación”.
Identificador	Cadena unívoca de datos empleada como clave en el sistema biométrico para nombrar la identidad de una persona y sus atributos conexos. Un ejemplo de identificador sería el número del MRTD.
Identificador de aplicación (AID)	Elemento de datos que identifica una aplicación. Las aplicaciones de eMRTD utilizan un AID estándar que corresponde a una de cuatro categorías de AID. Consiste de un identificador de proveedor de aplicación registrado (RID) y una extensión de identificador de aplicación de propiedad (PIX).

Término	Definición
Iluminante normalizado D65 de la CIE	Iluminante común normalizado definido por la Comisión Internacional de Iluminación (CIE) que forma parte de la serie D de iluminantes que tratan de reproducir condiciones de iluminación estándar al aire libre en diferentes partes del mundo.
Imagen	Representación de una característica biométrica captada normalmente mediante un dispositivo vídeo, fotográfico o escáner. Para fines de biometría se almacena en forma digital.
Imagen fantasma	Véase: Imagen sombreada.
Imagen frontal completa (del rostro)	Retrato del titular del MRTD, producido con arreglo a las especificaciones establecidas en el Doc 9303.
Imagen incorporada	Imagen o información codificada u oculta dentro de una imagen visual primaria. Véase también: Esteganografía.
Imagen láser variable	Elemento generado mediante grabado o perforación láser que exhibe información e imágenes que cambian según el ángulo de observación.
Imagen latente	Imagen oculta formada dentro de una imagen en relieve que se compone de estructuras de líneas que varían en cuanto a su dirección y perfil, originando una imagen oculta que aparece en ángulos de observación predeterminados, lo cual se logra comúnmente mediante impresión calcográfica.
Imagen secundaria	Reproducción, por el método que sea, del retrato del titular que se repite en otra parte del documento.
Imagen simbólica	Retrato del titular del MRTD, normalmente una imagen de frente completa, que se ha ajustado en tamaño para asegurar una distancia fija entre los ojos. También puede haberse girado ligeramente para asegurar que una línea horizontal imaginaria trazada entre los centros de los ojos es paralela al borde superior del rectángulo del retrato si esto no ha sido logrado cuando se tomó o captó el retrato original.
Imagen sombreada	Se utiliza como sinónimo de imagen fantasma: segunda representación del retrato del titular en el documento, reducida en contraste o saturación o tamaño.
Imitación fraudulenta	Copia o reproducción no autorizada de un documento de seguridad genuino hecha por el medio que sea.
Impostor	Persona que solicita y obtiene un documento asumiendo un nombre e identidad falsos o persona que modifica su apariencia física para hacerse pasar por otra con objeto de utilizar el documento de esa otra persona.
Impresión arco iris (iris o tintero compartido)	Técnica por medio de la cual se imprimen simultáneamente, en una prensa, dos o más colores de tinta mediante la misma unidad para crear una fusión controlada de colores semejantes al efecto que se observa en un arco iris. También se denomina impresión prismática o impresión iris.
Impresión calcográfica	Proceso de impresión utilizado en la producción de documentos de seguridad en el cual se utilizan placas de grabado, altas presiones de impresión y tintas especiales para crear una imagen en relieve sensible al tacto en la superficie del documento.

Término	Definición
Infraestructura de clave pública (PKI)	Conjunto de políticas, procesos y tecnologías utilizado para verificar, enrolar y certificar usuarios de una aplicación de seguridad. Una PKI utiliza criptografía de clave pública y prácticas de certificación de claves para asegurar las comunicaciones.
Inicialización (de una tarjeta inteligente)	Proceso de poblar la memoria persistente (EEPROM, etc.) con datos comunes a un gran número de tarjetas incluyendo una cantidad mínima de elementos únicos de la tarjeta (p. ej., número de serie ICC y claves de personalización).
Inscripción	Proceso de recoger muestras biométricas de una persona o su siguiente preparación y almacenamiento de plantillas de referencia biométrica que representan la identidad de dicha persona.
Inscrito	Ser humano, es decir, persona natural a la que un Estado u organismo expedidor asigna un MRTD.
Inspección	Acción de un Estado u organización que examina un MRTD que representa a un viajero (titular del MRTD) y verificar su autenticidad.
Inspección de nivel 1	Examen superficial para la rápida inspección en el punto de uso (características visuales o táctiles fácilmente identificables).
Inspección de nivel 2	Examen por inspectores capacitados con equipo sencillo.
Inspección de nivel 3	Inspección por especialistas forenses.
Integración de sistemas	Proceso por el cual se integran entre sí los sistemas para titulares de tarjetas, internos y para asociados y sus aplicaciones.
Integridad	Capacidad de confirmar que la estructura lógica de datos y sus componentes no han sido alterados con respecto a los creados por el Estado u organización expedidor.
Intercambio de claves	Proceso de otorgar claves de sesión a los participantes en una comunicación.
Interfaz	Definición técnica normalizada de la conexión entre dos componentes.
Interfuncionamiento	Capacidad de varios sistemas independientes o componentes de subsistemas para trabajar juntos.
Interfuncionamiento mundial	Capacidad de los sistemas de inspección (manuales o automáticos) en diferentes Estados de todo el mundo para obtener e intercambiar datos, procesar datos recibidos de sistemas de otros Estados y utilizar dichos datos en las operaciones de inspección en sus respectivos Estados. El interfuncionamiento mundial es un objetivo principal de las especificaciones normalizadas para la colocación de datos de lectura visual y de lectura mecánica en todos los eMRTD.
Iris (impresión)	Véase: Impresión arco iris.
JPEG y JPEG2000	Normas para la compresión de datos de imágenes, utilizada en particular para el almacenamiento de imágenes faciales.
Laissez-passer (salvoconducto)	Documento, en general equivalente a un pasaporte, expedido bajo los auspicios de una entidad supranacional (p. ej., las Naciones Unidas).

Término	Definición
Laminado	Material transparente que puede tener elementos de seguridad, como propiedades ópticamente variables, diseñado para unirse firmemente a la página de datos personales o a otra página del documento.
Laminado o recubrimiento del dispositivo difrangente de imágenes ópticamente variables (DOVID)	Laminado o recubrimiento que contiene una DOVID y cubre un área completa o está emplazado para proteger datos clave en el documento.
Laminado sellado térmicamente	Laminado concebido para unirse a la página de datos personales de la libreta pasaporte mediante la aplicación de calor y presión.
Leyenda	Palabra o frase que se imprime para identificar un campo. En circunstancias excepcionales, cuando en el campo de datos no hay suficiente espacio para diferentes idiomas oficiales, pueden utilizarse números. Estos números deben ir acompañados por un texto explicativo en otro lugar del MRP.
Lista de desviaciones	Lista firmada expedida por un Estado expedidor en que se especifican los casos de no cumplimiento en documentos de viaje o claves y certificados.
Lista de revocación de certificados (CRL)	Lista de certificados que se han revocado. Por consiguiente, los documentos asociados a (firmados por) un certificado contenido en una CRL dejan de ser fiables.
Lista maestra	Una lista maestra es una lista, firmada digitalmente, de certificados CSCA en los que “confía” el Estado receptor que la utiliza (véase el Doc 9303-12).
Marca habitual	Símbolo que sustituye la firma escrita del titular en caso de que éste no esté en condiciones de firmar.
Marcas de cotejo	Véase: Marcas de referencia.
Marcas de referencia	Estas marcas se imprimen sobre el borde exterior de cada página en orden consecutivo a partir de la parte superior de la primera página hasta una posición inferior en la página siguiente y así sucesivamente. La marca de registro de la última página aparece al pie de la misma. Este método de impresión hace que aparezca una banda continua sobre el borde del pasaporte. Toda página que se haya extraído se registrará como una brecha o espacio vacío. Cuando se imprime en color UV, la franja es visible solamente con radiación UV. También se denominan marcas de cotejo.
Marco común de formatos de intercambio biométrico (CBEFF)	Formato de fichero común que facilita el intercambio y el interfuncionamiento de los datos biométricos.
Medida	Número en una escala de bajo a elevado, que mide el grado de correspondencia de un registro de prueba biométrica (la persona que se investiga) y un registro de galería particular (una persona inscrita previamente).
Memoria de acceso aleatorio (RAM)	Memoria volátil de acceso aleatorio utilizada en el CI y que requiere alimentación eléctrica para mantener los datos.

Término	Definición
Memoria de solo lectura (ROM)	Memoria no volátil que se escribe una vez, normalmente durante la producción del CI. Se utiliza para almacenar sistemas y algoritmos operacionales empleados por el semiconductor en una tarjeta de circuito integrado durante transacciones.
Memoria de solo lectura programable de borrado eléctrico (EEPROM)	Tecnología de memoria no volátil en que los datos pueden borrarse eléctricamente y volverse a escribir.
Memoria no volátil	Memoria de semiconductor que conceda su contenido cuando se quita la alimentación eléctrica (p. ej., ROM, EEPROM).
Mensaje	Menor conjunto significativo posible de información transmitida de remitente a receptor. Esta información puede consistir en una o más transacciones de tarjeta o información relacionada con transacciones de tarjetas.
Mensaje asegurado	Mensaje protegido contra alteración o creación ilegal.
Mentón	Prominencia central de la mandíbula inferior.
Microimpresión	Texto o símbolos impresos de tamaño inferior a 0,25 mm/0,7 puntos pica.
Modelo de documento	El documento modelo abarca la serie de documentos de una nación, que tienen la misma apariencia óptica (p.ej.: (D, P, 1, 2005), (D, P, 2, 2007) y (D, P, 3, 2010). Una nación puede tener en circulación en un momento dado múltiples modelos de documento válidos [p.ej.: (GBR, P, 1, 2008) y (GBR, P, 2, 2010)].
MP	Longitud lateral del patrón de medición: Las zonas de medición tienen forma de cuadrados y su tamaño equivale al 30% de la distancia entre los ojos; se utilizan para medir la intensidad de la luz en las mejillas, la frente y el mentón.
MROTD electrónico	MROTD de tamaños DV1 o DV2 que se ajusta a las especificaciones del Doc 9303-5 o Doc 9303-6, respectivamente, y que además incorpora un circuito integrado sin contacto que incluye capacidad de identificación biométrica del titular.
Muestra biométrica	Datos brutos captados como valor discreto, inequívoco, único y lingüísticamente neutro que representa una característica biométrica de una persona inscrita captada por un sistema biométrico (por ejemplo, las muestras biométricas pueden comprender la imagen de una huella digital así como sus derivados para fines de autenticación).
Norma de cifrado de datos (DES)	Método de cifrado de datos especificado en FIPS 46-3.
Número de control	Número asignado a un documento en el momento de su fabricación para mantenimiento de registro y fines de seguridad.
Número de documento	Número que identifica unívocamente un documento. Se recomienda que el número de documento y el número de control sean idénticos.
Número de identificación personal (NIP)	Código de seguridad numérico utilizado como mecanismo para la verificación local uno a uno a efectos de determinar si el titular de la tarjeta es realmente la persona natural autorizada para acceder o utilizar un servicio específico como el derecho de liberar cierta información en la tarjeta.

Término	Definición
Organización expedidora	Entidad autorizada a expedir MRTD oficiales [p. ej., la Organización de las Naciones Unidas, expedidora del laissez-passer (salvoconducto)].
Organización receptora autorizada	Organización autorizada para procesar un documento oficial de viaje (p. ej., un explotador de aeronave) y, como tal, potencialmente admisible en el futuro para registrar detalles en la tecnología de expansión de capacidad opcional.
Página de datos	Página de la libreta pasaporte, de preferencia la segunda o penúltima página, que contiene los datos biográficos del titular del documento. Véase: Datos biográficos.
Página de datos del MRP	Página de dimensión fija dentro del MRP donde se presentan en formato estándar datos visuales y de lectura mecánica.
Par de claves	Par de claves digitales — una pública y una privada — utilizado para cifrar y firmar información digital.
Paralaje	Desplazamiento o diferencia de la posición aparente de un objeto observado desde dos líneas visuales distintas, medido por el ángulo o semiángulo de inclinación entre esas dos líneas
Participante en el PKD	Estado miembro de la OACI u otra entidad que expida o prevea expedir eMRTD que siga las disposiciones para participar en el PKD de la OACI.
Pasaporte de lectura mecánica (MRP)	Pasaporte que cumple las especificaciones contenidas en el Doc 9303-4. Normalmente está elaborado en forma de libreta de tamaño DV3 con páginas que contienen información sobre el titular y el Estado u organización expedidores y páginas para visados y otras anotaciones. La información de lectura mecánica está comprendida en dos líneas de texto OCR-B, de 44 caracteres cada una.
Pasaporte de lectura mecánica electrónico (eMRP)	MRTD de tamaño DV3 que se ajusta a las especificaciones del Doc 9303-4 y que además incorpora un circuito integrado sin contacto que incluye la capacidad de identificación biométrica del titular. Normalmente se conoce como “Pasaporte-e”.
Pasaporte-e	Nombre comúnmente utilizado con referencia a un eMRP. Véase: Pasaporte de lectura mecánica electrónico (eMRP).
Patrón antiescáner	Imagen generalmente construida a base de líneas finas con desplazamiento angular variable e incorporada al diseño del fondo de seguridad. Cuando se observa en condiciones normales, no es posible distinguir la imagen del resto del fondo de seguridad, pero cuando el original se escanea o fotocopia, la imagen incorporada se hace visible.
Patrón de muaré	Error de observación que se asemeja a un patrón ondulado causado al fotografiar una escena o un objeto que contiene detalles repetitivos (p.ej., líneas, puntos, etc.) que exceden la resolución sensora de la cámara.
Perforación con láser	Proceso mediante el cual se crean números, letras o imágenes mediante perforación del substrato con láser.
Personalización	Proceso mediante el cual se aplican al documento el retrato, la firma y los datos personales.

Término	Definición
Plan de firmas (criptográficas) digitales	Un conjunto de tres algoritmos. El algoritmo de generación de clave toma como entrada un parámetro de seguridad y saca un par de claves, una privada y una pública. El algoritmo de firma toma como entrada una clave privada y un mensaje, y saca una firma criptográfica. El algoritmo de verificación toma como entrada una clave pública, un mensaje y una firma; si la firma se generó usando el algoritmo generador de firma con la clave privada del par de claves y el mensaje como entrada, éste arroja un resultado de “válida”, de no ser así, arroja el resultado de “inválida”.
Plantilla biométrica	Datos extraídos y comprimidos tomados de una muestra biométrica.
Plantilla de referencia biométrica	Conjunto de datos que define la medición biométrica de una persona y que se utiliza como base para comparación respecto de muestras biométricas presentadas posteriormente.
Plantilla/Plantilla de referencia	Datos que representan la medición biométrica de una persona y que se utilizan como base para comparación respecto de muestras biométricas presentadas posteriormente
Política de seguridad del sistema	Conjunto de leyes, reglas y prácticas que regulan la forma en que la información sensible y otros recursos se gestionan, protegen y distribuyen dentro de un sistema específico.
Proporción de aceptaciones falsas (FAR)	Probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o no logre rechazar a un impostor. La proporción obtenida supone normalmente intentos pasivos por el impostor. La proporción de aceptaciones falsas puede calcularse como FAR = NFA/NIIA o FAR = NFA/NIVA donde FAR es la proporción de aceptaciones falsas, NFA es el número de aceptaciones falsas, NIIA es el número de intentos de identificación por el impostor y NIVA es el número de intentos de verificación por el impostor.
Proporción de correspondencias falsas	Alternativa a “proporción de aceptaciones falsas”; utilizada para evitar confusiones en aplicaciones que rechazan a las/los titulares si sus datos biométricos corresponden a los de un inscrito. En esas aplicaciones, se invierten los conceptos de aceptación y rechazo, invirtiéndose así el significado de “aceptación falsa” y “rechazo falso”.
Proporción de desacuerdos falsos	Alternativa a “proporción de rechazos falsos”; utilizada para evitar confusiones en aplicaciones que a las/los titulares si sus datos biométricos corresponden a los de alguien inscrito. En esas aplicaciones, se invierten los conceptos de aceptación y rechazo, invirtiéndose así el significado de “aceptación falsa” y “rechazo falso”.
Proporción de rechazos falsos (FRR)	Probabilidad de que un sistema biométrico no logre identificar a un inscrito o verificar la identidad legítima de un inscrito. La proporción de rechazos falsos puede calcularse como sigue: FRR = NFR/NEIA o FRR = NFR/NEVA donde FRR es la proporción de rechazos falsos, NFR es el número de rechazos falsos, NEIA es el número de intentos de identificación por el inscrito y NEVA es el número de intentos de verificación por el inscrito. Este cálculo supone que los intentos de identificación o verificación por el inscrito representan la población entera de inscritos. La proporción de rechazos falsos normalmente excluye los errores de “falla de adquisición”.
Prueba	Muestra biométrica del inscrito cuya identidad se procura establecer.
Puerta ABC	Puerta de control fronterizo automatizada para documentos de viaje de lectura mecánica.
Puesto para toma de fotografías	Sistema semiautomatizado para la captura digital de fotografías de identidad en un entorno tipo mostrador; consiste en una cámara e iluminación que habitualmente tiene un panel separador ubicado detrás del sujeto para proporcionar el fondo requerido, pero el resto está abierto.

Término	**Definición**
Punto de confianza	En los sistemas criptográficos de estructura jerárquica es una entidad autorizada para la cual la confianza se presupone y no se infiere.
Rechazo falso	Cuando un sistema biométrico no logra identificar a un inscrito o verificar la identidad legítima de un inscrito.
Recubrimiento	Película o capa protectora muy delgada que puede pegarse a la superficie de un documento en lugar de un laminado.
Registro	Proceso de hacer conocer la identidad de una persona a un sistema biométrico, asociando un identificador unívoco a dicha entidad y recogiendo y registrando los atributos pertinentes de la persona en el sistema.
Registro anverso-reverso (transparente)	Diseño que se imprime en ambas caras del documento o en una página interior que, cuando la página se ve al trasluz, permite que se forme una imagen entrelazada.
Registro transparente (anverso reverso)	Véase: Registro anverso reverso.
Relleno	Añadido de bits adicionales a cada lado de una cadena de datos hasta una longitud predefinida.
Remuestreo (autosuficiente)	Método para ensayar la fiabilidad de un conjunto de datos.
Resistencia a la manipulación indebida	Capacidad de los componentes de un documento de rechazar alteraciones.
Respuesta	Mensaje devuelto por el dispositivo esclavo al maestro después del procesamiento de una orden recibida por el esclavo.
Retrato	Representación visual de la imagen facial de quien es titular del MRTD en forma impresa y almacenada electrónicamente.
Rivest, Shamir y Adleman (RSA)	Algoritmo asimétrico inventado por Ron Rivest, Adi Shamir y Len Adleman. Se utiliza en criptografía de clave pública y se basa en el hecho de que resulta fácil multiplicar entre ellos dos grandes números enteros, pero que es difícil factorizarlos a partir del producto.
Rótulo (característica)	Un byte que identifica de manera única una característica de documento. La correspondencia entre rótulos de característica y las características debe especificarse en un perfil.
Rutina de verificación	Procedimiento de prueba de una propiedad específica de la característica (p.ej.: examen sobre la presencia de la fotografía bajo luz IR).
Seguridad física	Gama de medidas de seguridad que se aplican durante la producción y personalización para evitar el robo y el acceso no autorizado al proceso.
Sello digital	Forma abreviada de sello digital visible
Sello digital visible (VDS)	Estructura de datos firmada criptográficamente que contiene características de documento, codificada como código de barras en 2D e impresa en un documento.

Término	Definición
Sensibilizadores químicos	Reactivos de seguridad para proteger contra intentos de alteraciones fraudulentas mediante borraduras con productos químicos, de manera que aparezcan colores irreversibles cuando el documento entra en contacto con agentes blanqueadores o disolventes.
Simbología del código de barras	La correspondencia entre mensajes y códigos de barra se denomina simbología. Dicha correspondencia se define en la especificación del código de barras e incluye la codificación de dígitos o caracteres individuales, el tamaño de la llamada zona silenciosa en torno al código de barras, así como el cómputo de las sumas de comprobación para corrección de errores.
Sintético	Material no basado en papel utilizado para la página o tarjetas de datos personales. El término “sintético” es sinónimo de “plástico” en este contexto, y comprende materiales como policarbonato, PET y otros similares y combinaciones de los mismos.
Sistema	Instalación TI específica, con finalidad y entorno operacional particulares.
Sistema biométrico	Sistema automático capaz de: 1. captar una muestra biométrica de un usuario final para un MRP; 2. extraer datos biométricos de dicha muestra biométrica; 3. comparar esos datos biométricos específicos con los que figuran en una o más plantillas de referencia; 4. decidir cuan bien se corresponden los datos, es decir, ejecutar un proceso de equiparación basado en reglas específico de los requisitos para la identificación inequívoca y la autenticación de la persona del titular con respecto a la transacción involucrada; y 5. indicar si se ha logrado o no una identificación o verificación de identidad.
Sistema de clave pública	Método criptográfico que emplea pares de claves, una de las cuales es privada y la otra es pública. Si el cifrado se hace utilizando la clave pública, el descifrado requiere aplicación de la clave privada correspondiente y vice versa.
Sistema de inspección	Sistema utilizado para inspeccionar MRTD por cualquier entidad pública o privada que necesite validar el MRTD y utilizar este documento para verificación de identidad, p. ej., autoridad de control fronterizo, líneas aéreas y otros explotadores de transporte, instituciones financieras.
Sistema operacional	Programa que gestiona los diferentes programas de aplicaciones utilizados por una computadora.
Spoofing (simulación)	Falsear la dirección del remitente de una transmisión para entrar ilegalmente a un sistema fuente. *Nota.— La suplantación, el enmascaramiento, el* piggybacking *(acceso sin autorización) y la imitación, entre otros, son formas de* Spoofing *(simulación).*
Sujeto	Persona que ha de figurar en el retrato; se refiere a quien debe ser titular del MRTD.
Sustitución de la fotografía	Tipo de falsificación en la que el retrato del documento ya expedido es sustituido por otro.
Sustrato opaco a la luz UV	Sustrato que no revela ninguna fluorescencia detectable cuando se ilumina con radiación UV.

Término	Definición
Tamaño de plantilla	Volumen de memoria de computadora ocupado por los datos biométricos.
Tarjeta	Medio ajustado a ISO/IEC 7810, ISO/IEC 7811, ISO 7812 utilizado para transportar información.
Tarjeta de circuito integrado (tarjeta CI, ICC)	Tarjeta en la que se ha insertado uno o más CI.
Tarjeta de identificación (tarjeta ID)	Tarjeta utilizada como documento de identidad.
Tinta de color cambiante	Tinta que cambia sus características visuales dependiendo del ángulo de visión o de la calidad de una fuente estimulante (luminosa).
Tinta de numeración penetrante	Tinta que contiene un componente de color que penetra profundamente en el substrato.
Tinta fluorescente	Tinta que contiene un material que brilla cuando se expone a la luz a una longitud de onda específica, normalmente UV.
Tinta fosforescente	Tinta que contiene un instrumento que brilla al exponerlo a una luz de determinada longitud de onda; el brillo reactivo permanece visible y luego se desvanece cuando se quita la fuente de luz.
Tinta fotocrómica	Tinta que sufre un cambio reversible de color cuando se expone a la luz de una longitud de onda especificada.
Tinta infrarroja	Tinta visible en la región infrarroja del espectro.
Tinta invisible en la región infrarroja	Tinta que forma una imagen visible cuando se ilumina con luz en la parte visible del espectro pero que no puede detectarse cuando se ilumina en la región infrarroja.
Tinta marcada	Tinta que contiene compuestos de sustancias que no son de origen natural y que puede detectarse empleando equipo especial.
Tinta metálica	Tinta de apariencia metálica.
Tinta termocrómica	Tinta que sufre un cambio reversible de color cuando la imagen impresa se expone a un cambio específico de temperatura.
Tintas metaméricas	Par de tintas formulado para que éstas parezcan tener el mismo color cuando se ven en determinadas condiciones, normalmente a la luz del día, pero que se diferencian al exponerlas a otras longitudes de onda.
Tintas reactivas	Tintas que contienen reactivos de seguridad para ofrecer protección contra intentos de falsificación que entrañan borraduras con productos químicos (supresión), de manera que se produce una reacción detectable cuando agentes blanqueadores o disolventes entran en contacto con el documento.
Titular	Persona que posee un MRTD y presenta una muestra biométrica para verificación o identificación al reclamar una identidad legítima o falsa. Persona que interactúa con un sistema biométrico para inscribirse o para que se verifique su identidad.

Término	Definición
Transformación por fusión de imágenes (morphing)	Técnica de manipulación de la imagen mediante la cual dos o más caras de sujetos se transforman o fusionan para formar una sola cara en una fotografía.
Umbral	La comparación del valor de los resultados de una rutina de verificación con un umbral de correspondencia lleva a una decisión de aprobación/reprobación.
Uno a muchos	Sinónimo de “Identificación”.
Uno a pocos	Híbrido de identificación uno a muchos y verificación uno a uno. Normalmente el proceso de uno a pocos involucra la comparación de una muestra biométrica presentada respecto de un pequeño número de plantillas de referencia biométrica en el fichero. Se utiliza normalmente para cotejar con una “lista de vigilancia” de personas que merecen una investigación de identidad detallada o son conocidos delincuentes, terroristas, etc.
Uno a uno	Sinónimo de “Verificación”.
Usuario final	Persona que interactúa con un sistema biométrico para inscribirse o para la verificación de su identidad.
Validación	Proceso de demostrar que el sistema en consideración satisface en todos sus aspectos las especificaciones para ese sistema.
Valor de exposición (EV)	Número que representa la combinación de la velocidad de obturación y el número f de la cámara, por lo que todas las combinaciones que dan la misma exposición tienen el mismo EV.
Ventana transparente	Elemento de seguridad creado por la construcción del sustrato, donde parte de éste se elimina o sustituye por material transparente, que puede incorporar elementos de seguridad adicionales como lentes o elementos táctiles.
Verificación biométrica	Medio de identificar o confirmar la identidad del titular de un MRTD mediante medición y validación de una o más propiedades singulares de la persona del titular.
Verificación de documento con ayuda de máquina	Proceso que utiliza un dispositivo para ayudar en la verificación de la autenticidad de un documento con respecto a los datos o a la seguridad.
Verificación/verificar	En biometría: se refiere al proceso de comparación de una muestra biométrica presentada con respecto a la plantilla de referencia biométrica de un único inscrito cuya identidad se reclama para determinar si se corresponde con la plantilla del inscrito. Compárese con “Identificación”. En autenticación mecánica: se refiere a la aplicación de una rutina de verificación a un conjunto de datos del modelo de documento que está en proceso de ser verificado. El resultado de una verificación a menudo se presenta como un valor numérico.
Visado de lectura mecánica (MRV)	Visado que se ajusta a las especificaciones que figuran en el Doc 9303-7. Por lo común, el MRV se adjunta a una página de visado del pasaporte.
Visado de lectura mecánica de tamaño normal (Formato-A) (MRV-A)	Un MRV que se ajusta a las dimensiones especificadas en el Doc 9303-7, cuyo tamaño cubre por completo la página de visados del pasaporte.

Término	Definición
Visado de lectura mecánica de tamaño pequeño (Formato-B) (MRV-B)	Un MRV que se ajusta a las dimensiones especificadas en el Doc 9303-7, y cuyo tamaño permite mantener un espacio en blanco en la página de visado del pasaporte.
Visado físico	Documento de viaje tipo hoja colocada dentro del pasaporte de la persona que viaja.
Zona	Área que contiene un agrupamiento lógico de datos en el MRTD. Para los MRTD se definen siete (7) zonas.
Zona de inspección visual (ZIV)	Partes del MRTD (página de datos en el caso del MRP) diseñadas para inspección visual, es decir, anverso y reverso (cuando corresponda), y no definida como ZLM.
Zona de lectura efectiva (ZLE)	Área de dimensiones fijas común a todos los MRTD, en la que los datos de lectura mecánica en la ZLM pueden ser leídos por dispositivos de lectura de documentos.
Zona de lectura mecánica (ZLM)	Área de dimensiones fijas situada en la página de datos del MRTD que contiene los datos obligatorios y opcionales ordenados de forma que puedan ser leídos mecánicamente con métodos OCR.

4.3 Palabras clave

Se utilizan palabras clave para señalar los requisitos.

Las palabras clave “DEBE”, “NO DEBE”, “SE EXIGE”, “DEBERÍA”, “NO DEBERÍA”, “SE RECOMIENDA”, “PUEDE” y “OPCIONAL”, así como el uso del futuro afirmativo y negativo, en letras mayúsculas en el Doc 9303, deben interpretarse como se describen en [RFC 2119]:

DEBE	Esta palabra, o los términos “SE EXIGE” o el uso del futuro afirmativo, significa que la definición es un requisito absoluto de la especificación.
NO DEBE	Esta frase, o el uso del futuro negativo, significa que la definición es una prohibición absoluta de la especificación.
DEBERÍA	Esta palabra, o la frase “SE RECOMIENDA”, significa que pueden existir razones válidas en circunstancias particulares para ignorar un punto en particular, pero que las consecuencias completas deben comprenderse y ponderarse cuidadosamente antes de optar por un curso diferente.
NO DEBERÍA	Esta frase, o la frase “NO SE RECOMIENDA”, significa que pueden existir razones válidas en circunstancias particulares en que el comportamiento particular es aceptable o incluso útil, pero que las consecuencias completas deben comprenderse y el caso ponderarse cuidadosamente antes de aplicar cualquier comportamiento descrito con esta etiqueta.
PUEDE	Esta palabra, o el adjetivo “OPCIONAL”, significa que un artículo es verdaderamente opcional. Un usuario puede optar por incluirlo debido a que una aplicación particular lo exige o porque el usuario opina que mejora la aplicación, mientras que otro usuario puede omitir el mismo artículo. Una aplicación que no incluya una opción particular DEBE prepararse para que interfuncione con otra aplicación que incluya la opción, aunque quizás con funcionalidad reducida. Del mismo modo, una aplicación que incluya una opción particular DEBE prepararse para que interfuncione con otra aplicación que no incluya la opción (excepto, por supuesto, la característica que la opción proporciona).

CONDICIONAL	El uso de un artículo depende del uso de otros artículos. Por consiguiente, se especifica bajo qué condiciones el artículo se EXIGE o se RECOMIENDA. Esta es una palabra clave adicional empleada en el Doc 9303 (no es parte de RFC 2119).

Orientación para el uso. Los imperativos del tipo definido aquí deben utilizarse con cuidado y raras veces. En particular, DEBEN utilizarse solamente cuando se requiera realmente para el interfuncionamiento o para limitar el comportamiento que pueda provocar daños (p. ej., limitación de las retransmisiones). Por ejemplo, no deben utilizarse para tratar de imponer un método particular en quienes se encargarán de la implantación cuando dicho método no se requiera para interfuncionamiento.

Consideraciones de seguridad. Estos términos se utilizan frecuentemente para especificar comportamientos con consecuencias para la seguridad. Los efectos sobre la seguridad de no implantar un DEBE o DEBERÍA, o hacer algo que la especificación dice que NO DEBE o NO DEBERÍA hacerse, pueden ser muy sutiles. Los autores de los documentos deberían dedicar tiempo a ampliar las consecuencias para la seguridad de no seguir las recomendaciones o requisitos dado que la mayoría de las personas encargadas de la implantación no habrán tenido el beneficio de la experiencia y los debates que han producido la especificación.

En el caso de aplicarse características OPCIONALES, DEBEN aplicarse como se describe en el Doc 9303.

En el Doc 9303, los apéndices son informativos. Si se indica cumplimiento con un apéndice (informativo), las palabras clave utilizadas en ese apéndice DEBEN respetarse según se especifica.

4.4 Identificadores de objetos

En las Partes 9303-10, 9303-11 y 9303-12 se especifican los identificadores de objeto de la OACI. En este párrafo se enumeran dichos identificadores de objeto reales de la OACI:

```
-- Marco de seguridad de la OACI
id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136)}

id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}

id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}

-- Objeto de seguridad de LDS
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 1}

-- Lista maestra de CSCA
id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 2}

id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 3}

-- Protocolo de autenticación activa
id-icao-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 5}

-- Cambio de nombre de CSCA
id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}

id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icao-mrtd-
security-extensions 1}
```

```
-- Lista de tipos de documento, véase TR "LDS y mantenimiento de PKI"
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-
icao-mrtd-security-extensions 2}

-- Lista de desviaciones Identificadores de objetos básicos
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 7}

id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 8}

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}

id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 1}

id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 2}

id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 3}

id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-
Deviation-CertOrKey 4}

id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}

id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}

id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 3}

id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}

id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}

id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}

-- Identificadores de objeto de LDS2
id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 8}

id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}

id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}

id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}
```

```
id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}

id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 1}

id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 3}

id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}

id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
visaRecords 1}

id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-visaRecords
3}
id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}

id-icao-lds2- additionalBiometrics-application OBJECT IDENTIFIER ::= { id-icao-
lds2- additionalBiometrics 1}

id-icao-lds2- additionalBiometrics-access OBJECT IDENTIFIER ::= { id-icao-lds2-
additionalBiometrics 3}

-- Identificadores de objeto SPOC
id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}

id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}

id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}

-- Identificadores de objeto VDS
id-icao-vds OBJECT IDENTIFIER ::= { id-icao-mrtd-security 11}

-- Identificadores de objeto DTC
id-icao-dtc OBJECT IDENTIFIER ::= { id-icao-mrtd-security 12}

id-icao-dtcSigner OBJECT IDENTIFIER ::= {id-icao-dtc 1}

id-icao-dtcAttributes OBJECT IDENTIFIER ::= {id-icao-dtc 2}

id-icao-dtcCapabilitiesInfo OBJECT IDENTIFIER ::= {id-icao-dtcAttributes 1}

-- Identificadores de objeto EF.DIR
id-EFDIR OBJECT IDENTIFIER ::= { id-icao-mrtd-security 13}
```

4.5 Empleo de notas

Aunque en las normas ISO/IEC las notas tienen carácter informativo, las notas del Doc 9303 son parte del texto normativo y se emplean para enfatizar requisitos o información adicional.

5. ORIENTACIÓN SOBRE EL USO DEL DOC 9303

5.1 Estructura del Doc 9303

El Doc 9303 consta de trece partes. Cada una de ellas describe un aspecto específico del MRTD. Las partes del Doc 9303 están integradas de tal forma que el expedidor de MRTD puede construir un conjunto completo de especificaciones pertinentes, relativas a un tipo específico de MRTD (formato). La relación entre estos formatos y las partes del Doc 9303 se describe en la Sección 5.2 de esta Parte 1.

Las partes siguientes constituyen las especificaciones completas del Doc 9303 para documentos de viaje de lectura mecánica:

Parte 1 — Introducción
El presente documento es la Parte 1.

Parte 2 — Especificaciones para la seguridad del diseño, la fabricación y la expedición de MRTD
En la Parte 2 se proporcionan especificaciones obligatorias y opcionales para las precauciones que han de adoptar las autoridades expedidoras del documento de viaje a efectos de asegurar que sus MRTD y los medios de personalización y de expedición a las personas titulares legítimas del documento 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 MRTD, así como la inspección y control del personal que participa en tales operaciones.

Parte 3 — Especificaciones comunes a todos los MRTD
En la Parte 3 se definen especificaciones comunes a los documentos de viaje de lectura mecánica (MRTD) de tamaños DV1, DV2 y DV3, incluyendo las necesarias para el interfuncionamiento mundial empleando inspección visual y medios de lectura mecánica (reconocimiento óptico de caracteres). En el Doc 9303, Partes 4 a 7 se presentan especificaciones detalladas aplicables a cada tipo de documento.

Parte 4 — Especificaciones para pasaportes de lectura mecánica (MRP) y otros MRTD de tamaño DV3
En la Parte 4 se definen especificaciones exclusivas para los pasaportes de lectura mecánica (MRP) de tamaño DV3 y otros documentos de viaje de lectura mecánica (MRTD) de tamaño DV3. A efectos de brevedad del texto, el término MRP se ha utilizado en toda la Parte 4 y, excepto mención en contrario, todas las especificaciones de esta parte se aplicarán igualmente a todos los otros MRTD de tamaño DV3.

Parte 5 — Especificaciones para documentos oficiales de viaje de lectura mecánica (MROTD) de tamaño DV1
En la Parte 5 se definen especificaciones exclusivas de los documentos oficiales de viaje de lectura mecánica (MROTD) de tamaño DV1.

Parte 6 — Especificaciones para documentos oficiales de viaje de lectura mecánica (MROTD) de tamaño DV2
En la Parte 6 se definen especificaciones exclusivas de los documentos oficiales de viaje de lectura mecánica (MROTD) de tamaño DV2.

Parte 7 — Visados de lectura mecánica
En la Parte 7 se definen las especificaciones a las que deben ajustarse los visados de lectura mecánica (MRV) para que sean compatibles e intercambiables mundialmente empleando medios tanto visuales (lectura ocular) como de lectura mecánica. Las especificaciones para visados, al ser expedidos por un Estado y aceptados por otro Estado receptor, pueden emplearse para fines de viaje. Los MRV contendrán, como mínimo, los datos especificados de modo que sean legibles tanto visualmente como con los métodos de reconocimiento óptico de caracteres, según se presenta en la Parte 7.

La Parte 7 contiene especificaciones para los tipos de visado de Formato-A y de Formato-B y se basa en la tercera edición del Doc 9303, Parte 2, *Visados de lectura mecánica* (2005).

Parte 8 — Documentos de viaje de emergencia
En la Parte 8 se proporciona un texto de orientación y especificaciones sobre los Documentos de viaje de emergencia (ETD). El propósito de este texto de orientación es promover un enfoque coherente con relación a la emisión de los ETD a fin de mejorar la seguridad del documento, proteger a las personas, promover una mayor confianza entre el personal fronterizo en relación con el tratamiento de los ETD en puertos de acceso y abordar las vulnerabilidades debidas a prácticas y características de seguridad incoherentes. En la Parte 8 también se especifica el uso de los sellos digitales visibles.

Parte 9 — Empleo de identificación biométrica y almacenamiento electrónico de datos en los eMRTD
En la Parte 9 se definen las especificaciones, complementarias de las presentadas para el MRTD básico en las Partes 3, 4, 5, 6 y 7 del Doc 9303, que han de aplicar los Estados que deciden expedir un documento de viaje de lectura mecánica electrónico (eMRTD) que pueda utilizarse por cualquier Estado receptor debidamente equipado para leer del documento un volumen considerable de datos relativos al propio eMRTD y su titular. Esto comprende datos biométricos obligatorios de interfuncionamiento mundial que puedan utilizarse como entrada para los sistemas de reconocimiento del rostro y, como opción, a los sistemas de reconocimiento de huellas digitales o del iris. Las especificaciones exigen que los datos biométricos de interfuncionamiento mundial se almacenen en forma de imágenes de alta resolución.

Parte 10 — Estructura lógica de datos (LDS) para el almacenamiento de datos biométricos y de otro tipo en el circuito integrado (CI) sin contacto
En la Parte 10 se define una estructura lógica de datos (LDS) para eMRTD necesaria para el interfuncionamiento mundial. La tecnología de ampliación de capacidad de circuitos integrados sin contacto contenida en un eMRTD seleccionado por un Estado expedidor u organización expedidora DEBE permitir que los Estados receptores tengan acceso a los datos. En la Parte 10 se definen las especificaciones para la organización normalizada de esos datos. Esto exige la identificación de todos los datos obligatorios y opcionales y un ordenamiento o agrupamiento establecido de los datos que DEBE seguirse para lograr el interfuncionamiento mundial de la lectura de detalles (datos) registrados en la tecnología de ampliación de la capacidad incluida con carácter opcional en un MRTD (eMRTD).

Parte 11 — Mecanismos de seguridad para los MRTD
En la Parte 11 se proporcionan especificaciones para permitir que los Estados y proveedores implanten características de seguridad criptográficas para documentos de viaje de lectura mecánica electrónicos (eMRTD) con acceso ICC de solo lectura.

En la Parte 11 se especifican protocolos criptográficos para:

- impedir el despumado (skimming) de datos del CI sin contacto;
- impedir la escucha furtiva de la comunicación entre el CI y el lector;
- proporcionar la autenticación de los datos almacenados en el CI basada en la PKI que se describe en la Parte 12, así como la autenticación del propio CI.

Parte 12 — Infraestructura de clave pública para los MRTD
En la Parte 12 se define la infraestructura de clave pública (PKI) para la aplicación eMRTD. Se especifican los requisitos a los que deben ajustarse los Estados u organizaciones expedidores, incluyendo el funcionamiento de una autoridad de certificación (CA) que expida certificados y listas de revocación de certificados (CRL). También se especifican los requisitos a los que deben ajustarse los Estados receptores y sus sistemas de inspección que validan dichos certificados y CRL.

Parte 13 — Sellos digitales visible para documentos no electrónicos
En la Parte 13 se especifica un sello digital para garantizar la autenticidad e integridad de los documentos no electrónicos de una manera comparativamente poco costosa pero altamente segura empleando criptografía asimétrica. La información contenida en el documento no electrónico se firma criptográficamente y se codifica la firma como código de barras bidimensional y se imprime en el mismo documento.

5.2 Relación entre los formatos de MRTD y Partes pertinentes del Doc 9303

En la Tabla 1-1 se describen las Partes del Doc 9303 que son pertinentes a cada tipo de MRTD (formato).

Tabla 1-1. Tabla de referencia de formatos

	Parte del Doc 9303												
	1	2	3	4	5	6	7	8	9	10	11	12	13
MRTD de tamaño DV3 (MRP)	√	√	√	√									
eMRTD de tamaño DV3 (eMRP)	√	√	√	√					√	√	√	√	
MROTD de tamaño DV1	√	√	√		√								
eMROTD de tamaño DV1	√	√	√		√				√	√	√	√	
MROTD de tamaño DV2	√	√	√			√							
eMROTD de tamaño DV2	√	√	√			√			√	√	√	√	
MRV	√	√	√				√						√
ETD	√	√	√					√					√

6. REFERENCIAS (NORMATIVA)

Ciertas disposiciones de las normas internacionales, a que se hace referencia en este texto, constituyen disposiciones del Doc 9303. Cuando existan diferencias entre las especificaciones contenidas en el Doc 9303 y las normas de referencia, a efectos de hacer lugar a los requisitos de construcción específicos de los documentos de viaje de lectura mecánica, incluyendo visados de lectura mecánica, tendrán precedencia las especificaciones contenidas en este texto.

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

RFC 2119 RFC 2119, S. Bradner, “Key Words for Use in RFCs to Indicate Requirement Levels”, BCP 14, RFC2119, marzo de 1997.

— FIN —

ISBN 978-92-9265-375-0