TÉRMINOS DE REFERENCIA

CONTRATACIÓN DEL SERVICIO DE EMISIÓN DESCENTRALIZADA DE PASAPORTES BIOMÉTRICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES

DICIEMBRE, 2015

ÍNDICE

INTRODUCCIÓN Y ANTECEDENTES

El Ministerio de Relaciones Exteriores (MRE) requiere contar con un SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES para identificar de manera segura y fehaciente a los peruanos en el exterior; jefes y altos directivos de los Poderes del Estado y sus organismos públicos; así como a los funcionarios del Servicio Diplomático de la República, cumpliendo con el más alto nivel de seguridad y facilitando la movilidad de los mismos en los Estados receptores.

La Ley de Organización y Funciones del Ministerio de Relaciones Exteriores (MRE), Ley Nº 29357, y el Reglamento de Organización y Funciones, aprobado por Decreto Supremo Nº 135-2010-RE, establecen en su artículo 6º y 3º, respectivamente, que una de las funciones específicas de la Cancillería es administrar, expedir y revalidar pasaportes diplomáticos y especiales, así como los pasaportes comunes en el exterior. Asimismo, en el artículo 131º del mencionado reglamento, se señala que la Dirección General de Protocolo y Ceremonial del Estado se encarga de supervisar el otorgamiento y renovación de pasaportes diplomáticos y especiales a funcionarios del Estado; y, en el artículo 118º, que la Dirección de Política Consular, dependencia de la Dirección General de Comunidades Peruanas en el Exterior y Asuntos Consulares, se encarga de administrar los documentos de viaje que emite el Ministerio, así como normar, dirigir, controlar y evaluar el proceso para su expedición y revalidación, en coordinación con las áreas competentes.

CONFIDENCIALIDAD

El PROVEEDOR, resulte o no adjudicado, estará obligado a guardar confidencialidad respecto de la información que le proporcione el MRE, durante todo el proceso de selección e incluso una vez finalizado éste.

A la firma del contrato, el proveedor deberá firmar acuerdos de confidencialidad por toda la información reservada o no, del diseño de la configuración de seguridad de la solución integral, así como de las aplicaciones e información propia del MINISTERIO DE RELACIONES EXTERIORES.

En caso de incumplimiento de los acuerdos, el proveedor podrá ser penalizado e incluso se podrá efectuar la resolución del contrato.

El proveedor, sus empleados, y todos los terceros subcontratados por él, en cualquier calidad se encuentren ligados, deberán cumplir con la Ley de Protección de Datos Personales, Ley 29733 y su reglamento, respecto de los datos personales de los ciudadanos que se encuentran en las bases de datos O QUE SON TOMADOS del MINISTERIO DE RELACIONES EXTERIORES.

En caso de incumplimiento de la Ley, la MINISTERIO DE RELACIONES EXTERIORES iniciará los procesos legales correspondientes.

FINALIDAD PÚBLICA

El Ministerio de Relaciones Exteriores (MRE) requiere contar con un servicio de emisión de pasaportes biométricos Comunes, Diplomáticos y Especiales para identificar de manera segura y fehaciente a los peruanos en el exterior; jefes y altos directivos de los Poderes del Estado y sus organismos públicos; así como a los funcionarios del Servicio Diplomático de la República, cumpliendo con el más alto nivel de seguridad y facilitando la movilidad de los mismos en los Estados receptores.

OBJETIVOS DEL SERVICIO

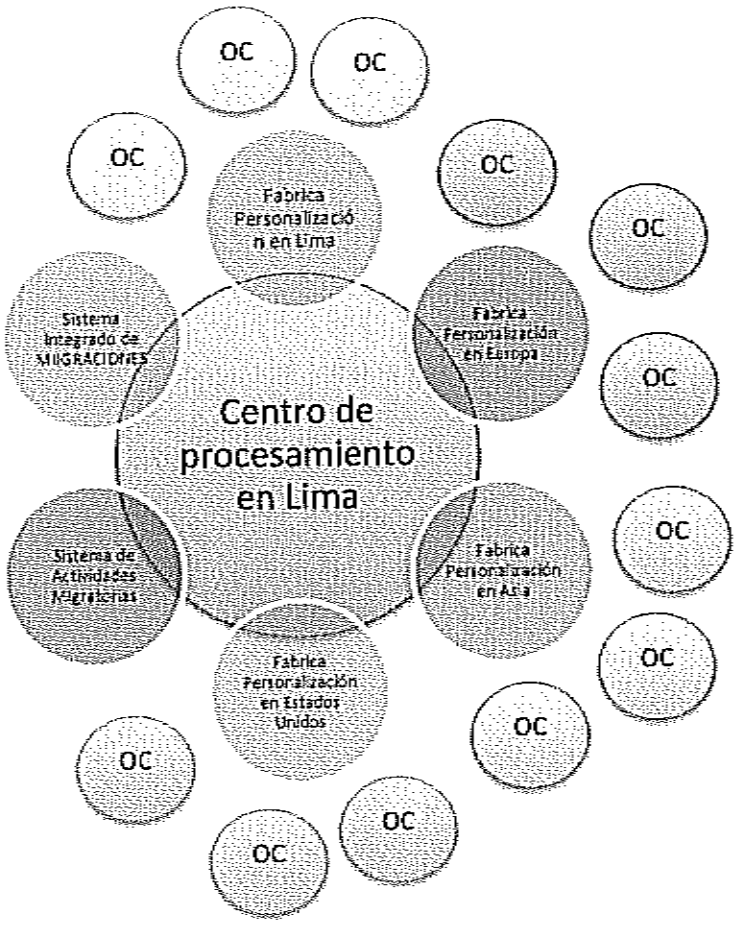
OBJETIVOS GENERALES

Los presentes términos de referencia tienen como objetivo principal proveer el SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES, fortalecer la verificación e identificación automática de la identidad de las personas, producir los nuevos pasaportes electrónicos que serán expedidos en las Oficinas Consulares a nivel mundial, cumpliendo con los estándares internacionales de uso y de seguridad de los documentos emitidos y del proceso de producción de éstos.

El PROVEEDOR deberá abastecer de CUATROCIENTOS MIL LIBROS PERSONALIZADOS DE PASAPORTES ELECTRONICOS a las Oficinas Consultares seleccionadas durante el periodo de 3 años, fabricados y personalizados en al menos 02 fábricas del PROVEEDOR, 01 localizada en Europa o Estados Unidos (en instalaciones físicas del PROVEEDOR), y 01 localizada en Lima – Perú (en instalaciones provistas por el MINISTERIO DE RELACIONES EXTERIORES).

Se deberán habilitar los sistemas de captura de datos biométricos y fotografía en todas las Oficinas Consulares seleccionadas y en la sede en Lima dispuesta por el MRE. Asimismo, se deberá implementar un sistema de

procesamiento que incluya la administración de un sistema de identificación biométrica AFIS, la PKI del MRE y que se encuentre interconectado de manera segura con canales cifrados a las fábricas de personalización, las Oficinas Consulares y la sede de expedición en Lima, conforme a la regulación permitida en cada país.



El PROVEEDOR deberá proveer todos los elementos necesarios para la operación del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES, incluyendo los insumos que sean requeridos en las fábricas de personalización de documentos, centro de datos, los almacenes, servicios de transporte, y en las demás dependencias bajo su responsabilidad, con las excepciones claramente señaladas en los presentes términos de referencia.

OBJETIVOS ESPECÍFICOS

El SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES deberá cumplir con los siguientes objetivos específicos:

a) Proveer CUATROCIENTOS MIL LIBROS PERSONALIZADOS DE PASAPORTES ELECTRONICOS a las Oficinas Consultares internacionales y sedes de expedicion seleccionadas por el MRE durante el periodo de 3 años,

la distribucion sera conforme a las proyecciones de demanda presentadas en el presente documento y solicitudes coordinadas del MRE.

b) Este servicio incluye el transporte especifico para la protección de los libros de pasaportes comunes personalizados desde las fábricas de personalizacion a las Oficinas Consulares y sedes de expedición seleccionadas por el MRE. Los pasaportes diplomáticos y especiales serán expedidos en Lima.

c) Proveer de sistemas de captura biométricos, cámaras fotográficas y lectores de firma a todas las Oficinas Consulares y sedes de expedición seleccionadas por el MRE.

d) Interconectar con canales seguros cifrados (VPN o HTTPS) las fábricas de personalizacion, el centro de procesamiento, el Sistema de Actividades Migratorias del MRE y el centro de procesamiento del Nuevo sistema de Emision de Pasaportes Electronicos de la Superintendencia Nacional de Migraciones y las Oficinas Consulares y sede de expedicion de LimaDefinidas por el proveedor . Los operadores de las Oficinas Consulares y de las fabricas de personalizacion deben autenticarse con certificados digitales o con informacion biometrica para acceder a la aplicación de gestion de pasaportes.

e) Implementar un nuevo Sistema de Emisión de Pasaportes Electrónicos que soporte los procesos de Atención a Usuarios, Servicios de Verificación de Identidad, Emisión de Documentos y que permita mantener una Base de Datos que almacene imágenes biométricas de las personas.

f) Proveer y mantener las aplicaciones operativas y de gestión del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

g) Proveer un sistema para la verificación automática de identidad mediante una comparación AFIS 1:1, de un dedo, tanto a través de una conexión en línea con el SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES como en forma autónoma utilizando el chip del pasaporte electrónico.

h) Realizar la integracion necesaria para el intercambio de consultas entre el Sistema Integrado de Migraciones y el Nuevo sistema de emision de pasaportes electrónicos del MRE, asegurando que se pueda realizar una consulta de comparacion AFIS 1:1 de la base de datos de informacion biometrica de Migraciones, siempre que medie la autorizacion respectiva por parte de dicha Entidad, para verificar que no existan intentos de suplantacion de identidad por parte de personas que inicialmente hayan obtenido sus pasaportes electronicos en el Peru y soliciten pasaportes con una identidad distinta en las Oficinas Consulares. De igual modo, el sistema debe permitir la consulta AFIS 1:1 de la base de datos biometrica del MRE por parte del sistema de emision de pasaportes de Migraciones, para verificar que no se realicen intentos de suplantacion de identidad en las solicitudes de pasaportes electronicos que hayan sido emitidos incialmente en las Oficinas Consulares.

i) Proveer un sistema para la identificación automática de las personas mediante el uso de AFIS 1:N. Asimismo, se debera realizar la integracion necesaria para el intercambio de consultas entre el Sistema Integrado de Migraciones y el Sistema de Actividades Migratorias del MRE, asegurando que se pueda realizar una consulta de comparacion AFIS 1:N de la base de datos de informacion biometrica de Migraciones, siempre que medie la autorizacion respectiva por parte de dicha Entidad para verificar que no existan intentos de suplantacion de identidad por parte de personas que inicialmente hayan obtenido sus pasaportes electronicos en el Perú y soliciten pasaportes con una identidad distinta en las Oficinas Consulares. De igual modo, el sistema debe permitir la consulta AFIS 1:N de la base de datos biométrica del MRE por parte del sistema de emisión de pasaportes de Migraciones, para verificar que no se realicen intentos de suplantación de identidad en las solicitudes de pasaportes electrónicos que hayan sido emitidos incialmente en las Oficinas Consulares.

j) El sistema deberá realizar el envío de información de registro de solicitud de un pasaporte electrónico para que pueda ser utilizado por Migraciones para realizar la anulación de los pasaportes previos expedidos.

k) Contar con un sistema web service que permita la activación y bloqueo de los pasaportes, cuyo acceso será a través de las Oficinas Consulares e Internet.

l) El provedor debera contar con al menos 2 fábricas para la personalización de pasaportes que permitan contar con los niveles de disponibilidad, rendimiento, seguridad y prevención de catástrofes requeridos, 01 localizada en los Estados Unidos de América o Europa (en las instalaciones del proveedor) y 01 localizada en Perú (en las instalaciones del MRE). Estas fábricas seran administradas y operadas por el provedor.

m) Maximizar la seguridad del proceso de traslado y custodia de los materiales e insumos que serán utilizados en la personalización de los pasaportes hasta la entrega de los documentos personalizados al MRE, minimizando en todo momento el riesgo de uso indebido.

n) Producir el pasaporte electrónico, con características avanzadas de seguridad, con imágenes digitales de alta calidad, que sea legible computacional y mecánicamente, con un sistema de personalización que minimice la intervención humana y cumpla con los estándares de la OACI DOC 9303 – Séptima edición y anexos complementarios para documentos de viaje. Respecto a los pasaportes comunes, el diseño grafico y todas las seguridades fisicas del libro , de la hoja de datos, tienen que ser identicas al 100% y de misma calidad, el contenido de la parte electronica , Inlay(antena , modulo y el chip incluyendo el mismo sistema operativo, deben ser exactamente identicos al que es utilizado para la produccion de pasaportes electronicos por parte de la Superintendencia Nacional de MIGRACIONES, a a fin de asegurar que se trata de un mismo documento para todos los ciudadanos peruanos, ya sea que radiquen en el país como en el extranjero. Respecto de los pasaportes diplomáticos y especiales, el diseño de la tapa y de la pagina de datos tiene que ser diferente del pasaporte ordinario. conforme a las aprobaciones del MRE. Respecto al diseños de las paginas de visados y otras seguridades fisicas del libro (marca de agua, parte electronica, etc) de los pasaportes diplomáticos y especiales el diseño estético tienen que ser los mismos que el pasaporte ordinario .

o) Implementar, administrar y custodiar de manera segura la infraestructura de criptografía basada en claves públicas (PKI) durante todo el periodo de contratación, para emitir y revocar Certificados Digitales que se utilizarán para firmar electrónicamente los pasaportes electrónicos, Document Signing Certificate (DSC) y para verificar pasaportes electrónicos, Document Verifying Certificate (DVC), conforme las especificaciones de la OACI.

p) Proveer y mantener las estaciones de trabajo del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES, dispuestas para la Atención de Usuarios en las Oficinas Consulares del MRE, necesarias para permitir la captura en vivo de la fotografía e impresiones dactilares.

q) Capturar por medios electrónicos y almacenar imágenes digitales de alta resolución de impresiones dactilares planas para operar con AFIS 1:1 y AFIS 1:N desde todas las Oficinas Consulares.

r) Proveer y mantener las estaciones de trabajo para el funcionamiento del Back Office del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES en las Oficinas Consulares y sedes de expedicion seleccionadas por el MRE.

s) Proveer y mantener las estaciones de trabajo y las aplicaciones de apoyo a los peritos biométricos del MRE, en tareas de verificación de identidad, utilizando AFIS (mínimo 8 estaciones de peritos).

t) Otorgar los servicios de Soporte y Mesa de Ayuda para los usuarios del SISTEMA DE EMISIÓN DE PASAPORTES.

u) Mantener y actualizar el SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES y los documentos, asegurando el cumplimiento de los niveles de servicio, la seguridad y la interoperabilidad.

v) Capacitar a los Operadores que participan en la operación y control del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

w) Capacitar al personal con conocimientosinformáticos en la administración y mantenimiento del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

x) Entregar y mantener actualizada la documentación del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

ALCANCE DE LOS SERVICIOS

SEDES DE EXPEDICIÓN DEL SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES

Se requiere que el PROVEEDOR provea pasaportes electrónicos personalizados a las Oficinas Consulares y sedes de expedición seleccionadas. Los pasaportes deben ser personalizados y distribuidos desde al menos 2 fábricas de personalizacion las cuales serán propiedad del proveedor y deberán localizarse 01 en Estados Unidos de América o Europa y 01 en Perú.

Cada fábrica proveerá los pasaportes a las Oficinas Consulares y sedes de expedición que se encuentren dentro de su área territorial o conforme a la demanda proyectada y a solicitudes coordinadas por el MRE.

Todas las Oficinas Consulares y sedes de expedición deberán ser provistas de equipos de captura de datos conforme se detalla en las siguientes secciones.

El proveedor podrá proponer implementar más fábricas de personalización de pasaportes electrónicos.

Continente	País	Oficina Consular	Dirección
Europa	Alemania	Hamburgo	Blumenstrasse 28, 22301 Hamburgo, Alemania.
Europa	Alemania	Berlín	Mohrenstrasse 42 10117 Berlín
Europa	Alemania	Frankfurt	Kaiserstrasse 74, 63065 Offenbach am Main Hessen, Alemania
Europa	Alemania	Munich	Herzog-Heinrichstrasse 23 80336 Muchen, Alemania
África, Medio Oriente y Países del Golfo	Arabia Saudita	Riad	Villa N° 7393 Ibn Younis Al-Sadafi Street, northern Maathar District Riyadh. P.O. Box 94433, Riyadh 11693
África, Medio Oriente y Países del Golfo	Argelia	Argel	2 et 4 Capitaine Salah Moghni – El Biar, 16406 Alger
América del Sur	Argentina	Buenos Aires	San Martín Nº 128-136, CP 1004, Microcentro, Capital Federal, Buenos Aires
América del Sur	Argentina	Córdoba	Calle 12 de Octubre N° 1320, Barrio Providencia, Córdoba Capital CP. 5000 Argentina
América del Sur	Argentina	Mendoza	Huarpes 629, 5ta Sección CP (5500) Mendoza, Argentina
América del Sur	Argentina	La Plata	Calle 8 Nº 862 1er. Piso, entre 49 y 50 La Plata C.P. 1900
Asia y Oceanía	Australia	Sídney	Suite 1001, 84 Pitt Street, Sydney – NSW 2000, Australia
Asia y Oceanía	Australia	Camberra	40 Brisbane Avenue, Piso 2, Oficina 1B, Barton 2600 ACT, Canberra
Europa	Austria	Viena	Mahlerstrasse 7/22, A-1010 Viena
Europa	Bélgica	Bruselas	Rue de Praetere 2-4, Código Postal 1000 Bruselas

América del Sur	Bolivia	El Alto	Av. Cívica Nº 33, casi esquina Av. Satélite – Villa Tejada Triangular, El Alto, Bolivia
América del Sur	Bolivia	Cochabamba	Av. Oquendo, E-0654, Piso 6 oficina 606/7 Entre Calle Pacciri y Pedro Borda Edificio "LasTorres Sofer I", Cochabamba, Bolivia
América del Sur	Bolivia	La Paz	Av. 6 de Agosto Nº 2455, Edificio Hilda, P-4, Oficina 402 Sopocachi, La Paz
América del Sur	Bolivia	Santa Cruz	Calle Viador Pinto Nº 84, Barrio Equipetrol, Santa Cruz de la Sierra, Bolivia
América del Sur	Brasil	Brasilia	S.E.S. Av. Das Nacoes Lote 43 Quadra 811 CEP: 70428-900 Brasilia DF
América del Sur	Brasil	Río de Janeiro	Av. Rui Barbosa, 314 2 Andar Flamengo CEP 22250 020 Rio de Janeiro
América del Sur	Brasil	Manaos	Rua Constelacao Nº 16-A Morada do Sol Bairro Aleixo, Manaus - AM Brasil CEP 69060-081
América del Sur	Brasil	Rio Branco	Rua Pernambuco N°1040 , Bosque, Rio Branco – Acre CEP 69900-421
América del Sur	Brasil	San Pablo	Alameda Campinas 646 4to. Andar, Jardim Paulista CEP 01404 - 001 San Pablo, Brasil
América del Norte	Canadá	Montreal	970-550 Sherbrooke Ouest, La Tour Ouest Montreal, Québec, H3A 1B9
América del Norte	Canadá	Toronto	10 St. Mary Street, Suite 301 Toronto, Ontario, M4Y 1P9
América del Norte	Canadá	Vancouver	260-505 Burrard Street, Vancouver, B.C. (Canadá), V7X 1M3
América del Norte	Canadá	Ottawa	Oficina Consular 1901-130 Albert Street Ottawa, Ontario K1P 5G4, Canadá
América del Sur	Chile	Arica	Av. 18 de Setiembre Nº 1554 Arica, Chile
América del Sur	Chile	Iquique	Zegers 570, 2do Piso, Casa Billinghurst, Iquique Casilla Postal: 248
América del Sur	Chile	Santiago	Calle Antonio Bellet Nº 444, Oficina 104, Providencia, Santiago, República de Chile.
América del Sur	Chile	Valparaíso	Calle Errazuriz Nº 1178, Of. 71 Edificio Olivari - Valparaíso
Asia y Oceanía	China	Hong Kong	Unit 1401, 14th Floor, China Merchants Tower 168-200 Connaught Road Central Shun Tak Centre, Sheung - Hong Kong
Asia y Oceanía	China	Shanghái	Shanghai Kerry Center, 1515 Nanjing XI Road, Piso 27, Oficina 270, Shanghai, 200040
Asia y Oceanía	China	Guangzhou	International Finance Center, 32FI, 5 Zhujiang Xi Lu, Tianhe, Guangzhou 510623
Asia y Oceanía	China	Pekín	SanLiTun Banggong Lou 1-91, Beijing 100600
América del Sur	Colombia	Bogotá	Calle 90 Nº 14 26, Of. 417 Bogotá
América del Sur	Colombia	Leticia	Calle 11 Nº 5-32, Barrio San Martín Leticia, Amazonas, Colombia
Asia y Oceanía	Corea del Sur	Seúl	Daeyungak Building, Suite 1305, 25-5, Chungmuro 1-Ka, Jung-ku, Seoul, Korea. Código Postal 100-706
América Central y Caribe	Costa Rica	San José	Del Mc Donald's de Plaza del Sol, 500 m. Sur y 175 m Este, Curridabat, San José, Costa Rica. A.P. 4248-1000 San José

América Central y Caribe	Cuba	La Habana	Calle 8 No. 307 entre 3ra. Y 5ta. , Miramar, Playa La Habana, Cuba
América del Sur	Ecuador	Macará	Calle Bolívar 48-33, Barrio Juan Montalvo, Macará
América del Sur	Ecuador	Guayaquil	Av. Francisco Orellana, Kennedy Norte Piso 14, of. 2, Edificio Centrum (Porta), Guayaquil.
América del Sur	Ecuador	Loja	Avenida Zoilo Rodríguez 03-05 y Clodoveo Carrión Ciudadela Zamora, Loja
América del Sur	Ecuador	Machala	Urbanización Unioro Manzana 14 Villa 11 Provincia de El Oro Machala.
América del Sur	Ecuador	Quito	Av. República de El Salvador N34-361, e Irlanda, Planta Baja, Quito
África, Medio Oriente y Países del Golfo	Egipto	El Cairo	41 Al - Nahda Street, 2nd Floor Maady, El Cairo.
América Central y Caribe	El Salvador	San Salvador	Avenida Masferrer Norte # 17-P, Cumbres de la Escalón, Colonia Escalón.
Asia y Oceanía	Emiratos Árabes Unidos	Dubái	25 th Floor, Al Habtoor Business Tower, Dubái Marina - Dubái Emiratos Árabes Unidos, P.O. Box: 213243
Europa	España	Barcelona	Calle Tarragona Nº 110-112, Condominio Roma 2000, Barcelona, CP 08015
Europa	España	Madrid	Paseo del Pintor Rosales Nº 30, Código Postal 28008, Madrid
Europa	España	Sevilla	Av. de María Luisa S/N, Pabellón del Perú, Sevilla, 41013
Europa	España	Valencia	Plaza Los Pinazos 2, piso 3, 46004 Valencia, España
Europa	España	Bilbao	Colón de Larreategui, 26-6°B, 48009 Bilbao
América del Norte	Estados Unidos	Nueva York	241 East 49th Street New York, NY 10017
América del Norte	Estados Unidos	Atlanta	4360 Chamblee Dunwoody RD. Suite 580 Atlanta, GA 30341
América del Norte	Estados Unidos	Boston	20 Park Plaza, Suite 511, Boston Massachusetts 02116
América del Norte	Estados Unidos	Chicago	180 North Michigan Avenue, Suite 401 Chicago, Illinois 60601
América del Norte	Estados Unidos	Dallas	13601 Preston Rd. Suite E – 650, Dallas, TX, 75240, Carillon Towers - Torre Este
América del Norte	Estados Unidos	Denver	6795 E Tennessee Ave., Suite 550, Denver, CO 80224
América del Norte	Estados Unidos	Hartford	19 High Street, Hartford, Connecticut, CT. 06103
América del Norte	Estados Unidos	Houston	5177 Richmond Avenue, Suite 695, Houston, Texas 77056
América del Norte	Estados Unidos	Los Ángeles	3450 Wilshire Boulevard, Suite 800, Los Ángeles, California CA 90010.
América del Norte	Estados Unidos	Miami	444 Brickell Avenue, Suite M-135, Miami Florida 33131
América del Norte	Estados Unidos	Paterson	100 Hamilton Plaza, Suite 1220, Paterson, NJ 0705
América del Norte	Estados Unidos	San Francisco	870 Market Street Suite 1075 San Francisco, California 94102
América del Norte	Estados Unidos	Washington	1225 23 St. N.W. Washington, DC 20037
Europa	Finlandia	Helsinki	Lönnrotinkatu 7 B 11, 00120 Helsinki, Finlandia

Europa	Francia	Paris	25, Rue de L'Arcade, 75008 Paris
África	Ghana	Accra	16 Plot 1st. Circular Road Cantonments Accra
Europa	Grecia	Atenas	Calle Koumbari N° 2, Tercer piso, Kolonaki C.P. 106 74, Atenas, Grecia
América Central y Caribe	Guatemala	Guatemala	15 Av. "A" 20-16, Zona 13, Guatemala, C.A. 01013
América Central y Caribe	Honduras	Tegucigalpa	Escuela Dowal Casa Nro. 3301, Calle Principal Colonia Linda Vista, Tegucigalpa, Casilla Postal 3171
Asia y Oceanía	India	Nueva Delhi	D-2/5 Vasant Vihar Nueva Delhi 110057 - India
Asia y Oceanía	Indonesia	Yakarta	Menara Rajawali, 12th floor Jl. DR Ide Anak Agung Gde Agung # 5.1 Kawasan Mega Kuningan Jakarta 12950 Indonesia
África, Medio Oriente y Países del Golfo	Israel	Tel Aviv	Medinat Hayehudim, 60, Herzliya Pituach 46766 Tel Aviv, Israel
Europa	Italia	Milán	Via Roberto Bracco No. 1, 20159, Milano
Europa	Italia	Florencia	Piazza San Firenze 3, 50122, Florencia, Italia
Europa	Italia	Génova	Piazza Della Vittoria, 15 AMM E, Génova - 16121
Europa	Italia	Roma	Via Illiria Nº 18, Escalera F, interior 2-3, 00183, Roma
Europa	Italia	Turín	Via Pastrengo 29, C.HP. 10128 Turin Italia
Asia y Oceanía	Japón	Tokio	Ichigo Gotanda Bldg. 6F, Higashi Gotanda 1-13-12, Shinagawa ku, Tokio 141-0022, Japón
Asia y Oceanía	Japón	Nagoya	ARK Shirakawa Koen Building 3F, Sakae 2-2-23, Naka-Ku, Nagoya-shi, Aichi-ken, 〒460-0008
África, Medio Oriente y Países del Golfo	Kuwait	Kuwait	Al Arabiya Tower Building, 6to. Piso, Ahmed Al Jaber Street, Distrito de Sharq, Kuwait City
Asia y Oceanía	Malasia	Kuala Lumpur	Wisma Selangor Dredging, 6th Floor, South Block, 142-A, Jalan Ampang, 50450 Kuala Lumpur. P.B. Nº 18
África, Medio Oriente y Países del Golfo	Marruecos	Rabat	16, Rue D'Ifrane, Plaza Perú, Rabat, Marruecos
América del Norte	México	México D.F.	Presidente Masarik, 29, segundo piso, Colonia Chapultepec Morales, Delegación Miguel Hidalgo, C.P. 11570 - México, D.F
América Central y Caribe	Nicaragua	Managua	Barrio Bolonia Casa No. 305, Managua
Europa	Países Bajos	Ámsterdam	Kabelweg 37, 1014 BA Amsterdam
América Central y Caribe	Panamá	Panamá	Calle Punta Darién y Punta Coronado, Edificio Torres de las Américas, Torre C, Piso 15, Oficina 1507, Punta Pacifica
América del Sur	Paraguay	Asunción	César López Moreira 812 esquina Nuestra Señora del Carmen, Asunción - Paraguay
Europa	Polonia	Varsovia	Calle Staroscinska 1/3, 02-516 Varsovia
Europa	Portugal	Lisboa	Rua Castilho 50,4º Dto. 1250 -071, Lisboa
África, Medio Oriente y Países del Golfo	Qatar	Doha	Street 835, Building 42, Lejbailat, Zone 64, P.O. Box 24062, Doha - Qatar

Europa	Reino Unido	Londres	52 Sloane Street, London SW1X9SP.
Europa	República Checa	Praga	Muchova 9, Praga 6, 16000, Dejvica 16000
América Central y Caribe	República Dominicana	Santo Domingo	Calle Mayreni N° 31 Urb. Los Cacicazgos, Santo Domingo, República Dominicana
Europa	Rumania	Bucarest	Str. Maior Gh. Şontu nr. 10-12, et. 3, ap. 10, Sector 1, 014031, Bucarest, Rumania
Europa	Rusia	Moscú	C.Sadovaya-Triumfalnaya, ed.4/10, piso 5, Moscú, Rusia 119002.
Asia y Oceania	Singapur	Singapur	390, Orchard Road Nº 12-03, Palais Renaissance Singapore 238871
África, Medio Oriente y Países del Golfo	Sudáfrica	Pretoria	200 Saint Patricks Street, Muckleneuk Hill, Pretoria 0083
Europa	Suecia	Estocolmo	Kommerdörsgatan 35 NB, 114 58, Stockholm, Suecia
Europa	Suiza	Zúrich	Lowenstrasse 69, 4to piso, 8021 Zurich
Europa	Suiza	Ginebra	17 Rue Des Pierres-Du-Niton, 1207 Ginebra
Europa	Suiza	Berna	Thunstrasse Nº 36, 3005 Berna
Asia y Oceanía	Tailandia	Bangkok	Glas Haus Building, 16 th. Floor, 1 Sukhumvit 25 Road, Klongtoey, Bangkok 10110, Tailandia
América Central y Caribe	Trinidad y Tobago	Puerto España	Bayside Towers, Office 1004 E, Western Main Road, Cocorite, Port-of-Spain
Europa	Turquía	Ankara	Resit Galip Caddesi, 70/1, 06700, Gaziosmanpasa, Ankara, Turkey
América del Sur	Uruguay	Montevideo	Obligado N° 1384, 11300 Montevideo
América del Sur	Venezuela	Caracas	4ta. Avenida entre 5ta. Y 6ta. Transversal, Quinta Perú, Urbanización Altamira, Municipio Chacao. Caracas - Venezuela.
América del Sur	Venezuela	Puerto Ordaz	Calle Roraima con esquina de Calle Aguila, Mz. 04, Casa No. 20, Urbanización Roraima, Alta Vista Sur, Puerto Ordaz, Estado Bolivar, República Bolivariana de Venezuela.
Asia y Oceanía	Vietnam	Handi	14F, Cornerstone Building 16 Phan Chu Trinch Hoan Kiem District, Ha Noi

PROYECCION DE EXPEDICIÓN DE PASAPORTES MECANIZADOS EN LAS OFICINAS CONSULARES DEL PERÚ 2016 - 2018

PERIODO			2013	2014	PROYECCIONES			
Nº	PAÍS	OFICINA CONSULAR	TOTAL 2013	TOTAL 2014	TOTAL 2015	TOTAL 2016	TOTAL 2017	TOTAL 2018
1	Alemania	Hamburgo	180	215	250	285	320	355
2	Alemania	Berlín	117	133	149	165	181	197
3	Alemania	Frankfurt	135	175	215	255	295	335
4	Alemania	Múnich	282	277	282	282	282	282
5	Arabia Saudita	Riad	5	12	19	26	33	40
6	Argelia	Argel	3	1	3	3	3	3
7	Argentina	Buenos Aires	2,849	2,247	2849	2849	2849	2849
8	Argentina	Córdoba	97	80	97	97	97	97
9	Argentina	La Plata	86	55	86	86	86	86
10	Argentina	Mendoza	72	102	132	162	192	222
11	Australia	Sídney	254	355	456	557	658	759
12	Australia	Canberra	2	5	8	11	14	17
13	Austria	Viena	102	126	150	174	198	222
14	Bélgica	Bruselas	169	166	169	169	169	169
15	Bolivia	Cochabamba	110	71	110	110	110	110
16	Bolivia	El Alto	56	59	62	65	68	71
17	Bolivia	La Paz	84	91	98	105	112	119
18	Bolivia	Santa Cruz	219	184	219	219	219	219
19	Brasil	Rio de Janeiro	140	198	256	314	372	430
20	Brasil	San Pablo	480	428	480	480	480	480
21	Brasil	Brasilia	47	45	47	47	47	47
22	Brasil	Manaos	95	78	95	95	95	95
23	Brasil	Rio Branco	7	17	27	37	47	57
24	Canadá	Toronto	131	167	203	239	275	311
25	Canadá	Montreal	280	292	304	316	328	340
26	Canadá	Ottawa	36	27	36	36	36	36
27	Canadá	Vancouver	66	132	198	264	330	396
28	Chile	Arica	20	25	30	35	40	45
29	Chile	Santiago	5,536	6,424	7312	8200	9088	9976
30	Chile	Iquique	682	1,006	1330	1654	1978	2302
31	Chile	Valparaíso	73	116	159	202	245	288
32	China	Pekín	18	17	18	18	18	18

33	China	Guangzhou	-	-	-	-	-	-	-
34	China	Hong Kong	89	82	89	89	89	89	89
35	China	Shanghái	19	42	65	88	111	134	134
36	Colombia	Bogotá	320	498	676	854	1032	1210	1210
37	Colombia	Leticia	62	55	62	62	62	62	62
38	Corea del Sur	Seúl	24	31	38	45	52	59	59
39	Costa Rica	San José	253	231	253	253	253	253	253
40	Cuba	La Habana	20	21	22	23	24	25	25
41	Ecuador	Guayaquil	200	387	574	761	948	1135	1135
42	Ecuador	Quito	199	356	513	670	827	984	984
43	Ecuador	Loja	210	132	210	210	210	210	210
44	Ecuador	Macará	1	0	1	1	1	1	1
45	Ecuador	Machala	63	55	63	63	63	63	63
46	Egipto	El Cairo	8	12	16	20	24	28	28
47	El Salvador	San Salvador	27	15	27	27	27	27	27
48	Emiratos Árabes	Dubái	26	35	44	53	62	71	71
49	España	Barcelona	5,692	4,369	5692	5692	5692	5692	5692
50	España	Bilbao	-	-	-	-	-	-	-
51	España	Madrid	6,501	6,069	6501	6501	6501	6501	6501
52	España	Sevilla	574	454	574	574	574	574	574
53	España	Valencia	626	541	626	626	626	626	626
54	Estados Unidos	Atlanta	1,233	1,097	1233	1233	1233	1233	1233
55	Estados Unidos	Boston	194	499	804	1109	1414	1719	1719
56	Estados Unidos	Chicago	1,326	1,036	1326	1326	1326	1326	1326
57	Estados Unidos	Dallas	867	730	867	867	867	867	867
58	Estados Unidos	Denver	944	789	944	944	944	944	944
59	Estados Unidos	Hartford	1,843	1,465	1843	1843	1843	1843	1843
60	Estados Unidos	Houston	889	899	909	919	929	939	939
61	Estados Unidos	Los Ángeles	3,353	3,051	3353	3353	3353	3353	3353
62	Estados Unidos	Miami	5,004	3,909	5004	5004	5004	5004	5004
63	Estados Unidos	Nueva York	5,502	4,372	5502	5502	5502	5502	5502
64	Estados Unidos	Paterson	3,939	3,336	3939	3939	3939	3939	3939
65	Estados Unidos	San Francisco	2,219	2,150	2219	2219	2219	2219	2219
66	Estados Unidos	Washington	3,776	2,875	3776	3776	3776	3776	3776
67	Finlandia	Helsinki	33	12	33	33	33	33	33
68	Francia	París	707	814	921	1028	1135	1242	1242
69	Ghana	Accra	-	-	-	-	-	-	-
70	Grecia	Atenas	15	26	37	48	59	70	70
71	Guatemala	Guatemala	46	29	46	46	46	46	46

72	Honduras	Tegucigalpa	7	41	75	109	143	177
73	India	Nueva Delhi	35	7	35	35	35	35
74	Indonesia	Yakarta	11	10	11	11	11	11
75	Israel	Tel Aviv	82	71	82	82	82	82
76	Italia	Milán	6,059	6,698	7337	7976	8615	9254
77	Italia	Roma	2,166	2,001	2166	2166	2166	2166
78	Italia	Génova	265	371	477	583	689	795
79	Italia	Turín	1,098	1,051	1098	1098	1098	1098
80	Italia	Florencia	781	917	1053	1189	1325	1461
81	Japón	Tokio	1,743	1,629	1743	1743	1743	1743
82	Japón	Nagoya	1,504	1,223	1504	1504	1504	1504
83	Kuwait	Kuwait	0	1	2	3	4	5
84	Malasia	Kuala Lumpur	21	16	21	21	21	21
85	Marruecos	Rabat	4	9	14	19	24	29
86	México	México	506	519	532	545	558	571
87	Nicaragua	Managua	13	20	27	34	41	48
88	Países Bajos	Ámsterdam	176	155	176	176	176	176
89	Panamá	Panamá	266	326	386	446	506	566
90	Paraguay	Asunción	97	135	173	211	249	287
91	Polonia	Varsovia	13	12	13	13	13	13
92	Portugal	Lisboa	11	13	15	17	19	21
93	Qatar	Doha	11	14	17	20	23	26
94	Reino Unido	Londres	257	237	257	257	257	257
95	Republica Checa	Praga	11	13	15	17	19	21
96	República Dominicana	Santo Domingo	211	148	211	211	211	211
97	Rumania	Bucarest	10	8	10	10	10	10
98	Rusia	Moscú	59	47	59	59	59	59
99	Singapur	Singapur	8	30	52	74	96	118
100	Sudáfrica	Pretoria	41	44	47	50	53	56
101	Suecia	Estocolmo	224	322	420	518	616	714
102	Suiza	Zúrich	222	238	254	270	286	302
103	Suiza	Berna	78	52	78	78	78	78
104	Suiza	Ginebra	295	310	325	340	355	370
105	Turquía	Ankara	4	4	4	4	4	4
106	Tailandia	Bangkok	23	39	55	71	87	103

107	*Trinidad y Tobago*	Puerto España	-	-	-	-	-	-
108	*Uruguay*	Montevideo	35	33	35	35	35	35
109	*Venezuela*	Caracas	2,725	2,056	2725	2725	2725	2725
110	*Venezuela*	Puerto Ordaz	577	553	577	577	577	577
111	*Vietnam*	Hanói	-	0	-	-	-	-
					0			0
TOTAL			**78,886**	**73,173**	**86,732**	**90,655**	**94,578**	**98,501**
TOTAL POR 3 AÑOS (2016 – 2018)					**283,734**			
MARGEN DE PROTECCION 20%					**340,481**			

Los pasaportes diplómaticos y especiales deberán ser entregados al MRE desde la fábrica de personalizacion localizada en el Perú, la cual sera habilitada dentro en un ambiente provisto por el Ministerio de Relaciones Exteriores.

EMISIÓN DE PASAPORTES DIPLOMÁTICOS Y ESPECIALES 2016 - 2018

EMISIÓN DE PASAPORTES DIPLOMÁTICOS	2015	2016	2017	2018	2016 - 2018	2016 - 2018 (20%)
ENERO	110	121	134	147	402	482
FEBRERO	143	157	173	190	521	625
MARZO	137	150	165	182	498	597
ABRIL	88	97	107	118	322	386
MAYO	65	71	78	86	235	283
JUNIO	51	56	62	68	186	223
JULIO	48	52	58	63	174	208
AGOSTO	49	54	60	66	180	216
SETIEMBRE	44	48	53	59	160	192
OCTUBRE	27	29	32	35	97	117
NOVIEMBRE	54	59	65	72	197	236
DICIEMBRE	32	35	38	42	115	138
TOTAL	847	932	1,025	1,128	3,085	3,702

EMISIÓN DE PASAPORTES ESPECIALES	2015	2016	2017	2018	2016 - 2018	2016 - 2018 (20%)
ENERO	308	339	373	410	1,121	1,346
FEBRERO	120	132	146	160	438	526
MARZO	138	152	167	184	504	604
ABRIL	175	192	211	232	636	763
MAYO	253	278	306	337	921	1,105
JUNIO	175	193	212	233	638	766
JULIO	376	414	455	500	1,369	1,643
AGOSTO	162	178	196	215	589	706
SETIEMBRE	205	226	248	273	746	896
OCTUBRE	278	306	336	370	1,012	1,215
NOVIEMBRE	179	197	217	238	652	782
DICIEMBRE	54	59	65	71	195	234
TOTAL	2,423	2,665	2,932	3,225	8,822	10,587

TOTAL AÑO	3,270	3,597	3,957	4,353	11,907	14,289

FRECUENCIA DE DISTRIBUCION DE PASAPORTES

Oficinas Consulares	Frecuencia de Distribucion	Responsable
Demanda mayor a 1000 pasaportes al año proyectados para el 2018	Semanal, en caso exista demanda.	PROVEEDOR
Demanda mayor a 500 y menor o igual a 1000 pasaportes al año proyectados para el 2018	Quincenal, en caso exista demanda.	PROVEEDOR
Demanda mayor a 50 y menor o igual a 500 pasaportes al año proyectados para el 2018	Mensual, en caso exista demanda.	PROVEEDOR
Demanda menor a 50 pasaportes al año proyectados para el 2018	Mensual, en caso exista demanda.	Ministerio de Relaciones Exteriores

INSTALACIÓN DE LOS EQUIPOS DE CAPTURA EN LAS SEDES DE EXPEDICION

Oficinas Consulares	Periodo de instalación	Modalidad de Instalación	Modalidad de Capacitación en el uso de los equipos de captura
Consulados que se encuentran localizados en países que pertenecen a la Unión Europea	Dentro de los primeros cuatro meses luego de la firma del contrato.	Presencial. El proveedor deberá enviar un técnico encargado de la instalacion.	Presencial. El proveedor deberá enviar un técnico encargado de la capacitación.
Consulados que se encuentran localizados fuera de la Unión Europea y que tienen una demanda anual proyectada para el 2018 mayor a 200 pasaportes	Dentro de los primeros seis meses luego de la firma del contrato.	Presencial. El proveedor deberá enviar un técnico encargado de la instalacion.	Presencial. El proveedor deberá enviar un técnico encargado de la capacitación.
Consulados que se encuentran localizados fuera de la Unión Europea y que tienen una demanda anual proyectada para el 2018, menor o igual a 200 pasaportes	Dentro de los primeros seis meses luego de la firma del contrato.	Guiada de manera remota. El proveedor deberá entregar un manual de instalación y prestará soporte remoto al personal técnico asignado por el MRE o la Oficina Consular para realizar la instalación de los sistemas.	El proveedor deberá entregar un manual de operación de los equipos de captura a cada Oficina Consular y al MRE Capacitación para el despliegue de los sistemas de enrolamiento al personal técnico del MRE en Lima.

SERVICIOS QUE DEBE ENTREGAR EL PROVEEDOR

a) Proveer CUATROCIENTOS MIL LIBROS PERSONALIZADOS DE PASAPORTES ELECTRONICOS a las Oficinas Consultares y sedes de expedición seleccionadas por el MRE durante el periodo de 3 años, conforme a las caracteristicas descritas en el presente documento. La distribucion será conforme a las proyecciones de demanda presentadas en el presente documento y solicitudes coordinadas del MRE.

b) Los sistemas de captura para 111 Oficinas Consulares a nivel mundial y una sede de expedición en Lima – Perú designada por el MRE.

c) Entregar 24 kits móviles de captura (1 por cada sede de mayor consumo y 2 para la sede de expedición que se implementará en Lima).

d) Interconectar con canales cifrados con certificados digitales (VPN o HTTPS) las fábricas de personalización, el centro de procesamiento, el Sistema de Actividades Migratorias y el centro de procesamiento del Nuevo sistema de Emision de Pasaportes Electronicos de la Superintendencia Nacional de Migraciones, y las Oficinas Consulares y sedes de expedición seleccionadas por el MRE. Todas las comunicaciones deben ser cifradas para evitar exponer la informacion de datos personales de los ciudadanos.

e) Interconectar con canales de alta velocidad el centro de procesamiento, el Sistema de Actividades Migratorias y el centro de procesamiento del Nuevo sistema de Emision de Pasaportes Electrónicos de la Superintendencia Nacional de Migraciones.

f) La aplicación central debe estar sobre una arquitectura web para la administración automatizada del sistema de captura de datos y control de producción de pasaportes asegurando una transmisión de datos con bajo consumo de ancho de banda con un consumo máximo de ancho de banda de 256 kbps para las Oficinas Consulares, bajo la aprobación del MRE.

g) Respecto a los pasaportes comunes, el diseño grafico y todas las seguridades fisicas del libro , de la hoja de datos, tienen que ser identicas al 100% y de misma calidad, el contenido de la parte electronica , Inlay(antena , modulo y el chip incluyendo el mismo sistema operativo, deben ser exactamente identicos al que es utilizado para la produccion de pasaportes electronicos por parte de la Superintendencia Nacional de MIGRACIONES, a a fin de asegurar que se trata de un mismo documento para todos los ciudadanos peruanos, ya sea que radiquen en el país como en el extranjero. Respecto de los pasaportes diplomáticos y especiales, el diseño de la tapa y de la pagina de datos tiene que ser diferente del pasaporte ordinario. conforme a las aprobaciones del MRE. Respecto al diseños de las paginas de visados y otras seguridades fisicas del libro (marca de agua, parte electronica, ...) s de los pasaportes diplomáticos y especiales el diseño estético tienen que ser los mismos que el pasaporte ordinario .

h) Las cámaras y/o dispositivos de captura de fotos y lectores de huella para todas las Oficinas Consulares especificadas en el presente documento, y su correspondiente garantía técnica durante un período de 3 años de la operación, más 2 años de garantía extendida, para casos de fallas del fabricante y daños por uso apropiado conforme a la información especificada por el fabricante.

i) Los traslados, fletes y seguros e instalación de los repuestos de los equipos de captura hasta ser entregados en las Oficinas Consulares y la sede de expedición de Lima.

j) El proveedor deberá brindar el servicio de transporte específico para la protección de los libros de pasaportes personalizados desde las fábricas de personalización hasta las Oficinas Consulares. El proveedor deberá implementar y acordar un procedimiento para la entrega segura y oportuna de los libros personalizados, a fin de cumplir con los plazos de entrega conforme a la demanda.

k) Provisión y gestión de los equipos de cómputo, servidores necesarios para la expedición, lo cual incluye mantenimiento y la actualización del sistema operativo y software necesario para su operación incluido el software de base de datos por el período del servicio.

l) Realizar la integración necesaria para el intercambio de consultas entre el Sistema Integrado de Migraciones y el Nuevo sistema de emisión de pasaportes del MRE, asegurando que se pueda realizar una consulta de comparacion AFIS 1:1 de la base de datos de informacion biométrica de Migraciones, siempre que medie la autorización respectiva por parte de dicha Entidad, para verificar que no existan intentos de suplantación de identidad por parte de personas que inicialmente hayan obtenido sus pasaportes electrónicos en el Perú y soliciten pasaportes con una identidad distinta en las Oficinas Consulares. De igual modo, el sistema debe permitir la consulta AFIS 1:1 de la base de datos biométrica del MRE por parte del sistema de emisión de pasaportes de Migraciones, para verificar que no se realicen intentos de suplantación de identidad en las solicitudes de pasaportes electrónicos que hayan sido emitidos incialmente en las Oficinas Consulares.

m) Proveer un sistema para la identificación automática de las personas mediante el uso de AFIS 1:N. Asimismo, se debera realizar la integracion necesaria para el intercambio de consultas entre el Sistema Integrado de Migraciones y el Nuevo Sistema de emision de pasaportes electronicos del MRE, asegurando que se pueda realizar una consulta de comparacion AFIS 1:N de la base de datos de informacion biometrica de Migraciones, siempre que medie la autorizacion respectiva por parte de dicha Entidad para verificar que no existan intentos de suplantacion de identidad por parte de personas que inicialmente hayan obtenido sus pasaportes electronicos en el Peru y soliciten pasaportes con una identidad distinta en las Oficinas Consulares. De igual modo, el sistema debe permitir la consulta AFIS 1:N de la base de datos biometrica del MRE por parte del sistema de emision de pasaportes de Migraciones, para verificar que no se realicen intentos de suplantacion de identidad en las solicitudes de pasaportes electronicos que hayan sido emitidos incialmente en las Oficinas Consulares.

y) Producir el pasaporte electrónico, con las mismas caracteristicas de seguridad que MIGRACIONES Respecto a los pasaportes comunes, el diseño grafico y todas las seguridades fisicas del libro , de la hoja de datos, tienen que ser identicas al 100% y de misma calidad, el contenido de la parte electronica , Inlay(antena , modulo y el chip incluyendo el mismo sistema operativo, deben ser exactamente identicos al que es utilizado para la produccion de pasaportes electronicos por parte de la Superintendencia Nacional de MIGRACIONES, a a fin de asegurar que se trata de un mismo documento para todos los ciudadanos peruanos, ya sea que radiquen en el país como en el extranjero. Respecto de los pasaportes diplomáticos y especiales, el diseño de la tapa y de la pagina de datos tiene que ser diferente del pasaporte ordinario. conforme a las aprobaciones del MRE. Respecto al diseños de las paginas de visados y otras seguridades fisicas del libro (marca de agua, parte electronica, ...) s de los pasaportes diplomáticos y especiales el diseño estético tienen que ser los mismos que el pasaporte ordinario .

n) Implementar, administrar y custodiar de manera segura la infraestructura de criptografía basada en claves públicas (PKI) durante todo el periodo de contratacion, para emitir y revocar Certificados Digitales que se utilizarán para firmar electrónicamente los pasaportes electrónicos, Document Signing Certificate (DSC) y para verificar pasaportes electrónicos, Document Verifying Certificate (DVC), conforme las especificaciones de la OACI. El PROVEEDOR deberá actuar como intermediario en la gestión del Certificado de Firma País frente a la Superintendencia Nacional de Migraciones, facilitando todas las operaciones de generación de certificados digitales y listas de revocación, configuración de equipos y realización de ceremonias de claves conforme a las políticas de certificación, las cuales serán también elaboradas por el proveedor.

o) Servicio de mantenimiento preventivo de todos los equipos de captura e intercambio de piezas por uso natural de acuerdo al plan de mantenimiento establecido por el fabricante de los equipos provistos para brindar el servicio en todas las Oficinas Consulares y la sede de expedición en Lima.

p) Soporte y garantía por los 3 años de operación para el sistema contratado, incluyendo sistemas de cómputo, servidores, personalización y captura.

q) Garantía extendida adicional por 2 años para el sistema contratado, incluyendo sistemas de cómputo, servidores y captura.

r) Administración, mantenimiento y licenciamiento de la plataforma tecnológica que sostiene la Solución Integral del Servicio de Emisión de Pasaportes Electrónicos, durante el período contratado. La administración incluye el control y reporte de los indicadores de producción, incidentes y proyecciones futuras de consumo de insumos y pasaportes, a fin de brindar las alarmas necesarias para que el MRE pueda adoptar las medidas de corrección y previsión correspondientes.

s) Sistema para la verificación de la relación entre la huella dactilar del solicitante y la huella registrada en el chip del pasaporte electrónico, el cual deberá ser provisto para todas la Oficinas Consulares seleccionadas y la sede de expedición del MRE.

t) Software de aplicación para la gestión y registro de pasaportes personalizados y su distribución a nivel internacional. La aplicación deberá permitir el registro de pasaportes personalizados perdidos, dañados y robados en todas la Oficinas consulares seleccionadas y la sede de expedición del MRE.

u) Equipos servidores (arquitectura x64) en redundancia para la aplicación central integrada de gestión de pasaportes (Proveedor- El MRE) y la base de datos de pasaportes emitidos.

v) Aplicación para la generación y administración del ciclo de vida de los Certificados digitales de firma de contenido del pasaporte, así como el Repositorio CRL.

w) Aplicación para la verificación de la firma digital del contenido del chip.

x) Entrenamiento del personal encargado de la supervisión de la Aplicación central de procesamiento y firma digital.

y) Entrenamiento del personal encargado de la captura de datos de solicitudes de pasaporte a nivel internacional.

z) Entrenamiento para el personal de informática en la supervision y control del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

aa) Acompañamiento al personal del MRE durante 6 meses al inicio de la producción en Lima.

bb) Las licencias para los equipos como sistema operativo servidor y desktop, gestor de base de datos o cualquier otro que se requiera para brindar el sistema.

cc) Servicio de mantenimiento correctivo de los sistemas incluidos en el alcance durante el plazo del contrato. Para el soporte a cambios en los sistemas que soportan el proceso de producción de pasaportes electrónicos del MRE, como por ejemplo cambios en la solicitud, cambios en los campos de personalización, etc., el PROVEEDOR dará una bolsa de mil quinientas horas de desarrollo para este punto.

dd) Los componentes de software que forman parte de la interfaz entre la Solución Integral Implementada y los componentes de software del MRE, las bases de datos del MRE y las bases de datos de consulta, así como aquellas herramientas que sirvan de interfase y permitan la corrección de errores, realización de modificaciones de los procedimientos de emisión del pasaporte electrónico, conexión a nuevas bases de datos de consulta, y todo aquello que permita mantener funcionando la aplicación luego de terminado el contrato con el PROVEEDOR deberán ser desarrollados a medida, conforme a los requerimientos funcionales del MRE y su código fuente deberá ser entregado a el MRE al culminar el período de contratación, conforme a la sección "Transición de salida" del presente documento. Los algoritmos propietarios que no sean afectos por esta definición podrán ser mantenidos como propiedad intelectual del proveedor. La entrega del código fuente sólo es aplicable a los módulos o componentes de software que sean desarrollados o personalizados a medida y no a software licenciado. El lenguaje de programación debe ser C# o Java y el gestor de base de datos SQL Server.

ee) Las soluciones que sean hechas a medida o desarrollo específico pasarán a ser propiedad del MRE y el código fuente deberá ser entregado al culminar el período de contratación.

ff) Los instaladores, DLL's, paquetes u otros de los componentes que no sean parte de las interfaces entre el actual el Sistema de Actividades Migratorias del MRE (SAM) y la Solución Integral Implementada, pasarán a ser propiedad del MRE al culminar el período de contratación.

gg) El licenciamiento correspondiente a todos los componentes de software adquiridos como parte de la Solución Integral Implementada deberá ser de uso perpetuo.

hh) Se deberá proporcionar la garantía extendida a 2 años adicionales al período de contratación al software de la aplicación central de procesamiento y firma digital.

ii) Habilitación y dotación del mobiliario, cableado eléctrico y de datos conforme sea necesario en la sede de expedición de Lima, cuyo local será dispuesto por el MRE. Cuyas dimensiones no serán mayores de 5 x 5m.

jj) Habilitación y dotación del mobiliario y equipamiento necesario para el centro de monitoreo localizado Lima, cuyo local será dispuesto por el MRE. Cuyas dimensiones no serán mayores de 5 x 5m. Este centro deberá ser dotado de al menos 3 pantallas LED de un tamaño de al menos 50", 3 computadores de escritorio. El centro de monitoreo permitirá la visualización y control de la producción y entrega de pasaportes a nivel internacional.

REQUERIMIENTOS TÉCNICOS

ESTÁNDARES, CERTIFICACIONES Y BUENAS PRÁCTICAS

El PROVEEDOR debe cumplir en todos los puntos que corresponda en su propuesta, los estándares internacionales, las normas de distinto rango y las buenas prácticas que formalizan el apoyo a los procesos por las tecnologías de la información y comunicaciones. El PROVEEDOR debe cumplir con la normativa mencionada a continuación o la más reciente a la fecha de presentación de su propuesta.

Sistemas de Información

En los casos que corresponda, la Propuesta Técnica debe cumplir con lo siguiente:

a) Usabilidad según la norma ISO 9126 y sus actualizaciones mas recientes (comprensión, aprendizaje, operación, atractivo, conformidad de usabilidad)

b) Administración y seguridad de información biométrica según la norma ANSI X9.84

c) Control del ciclo de vida de las claves (PKI) según la norma ISO 15782 Cifrado Simétrico, gestión de claves y ciclo de vida (PKI) según norma ISO 11568-2:2005

d) Gestión de los procesos de seguridad de los documentos de valor, según la norma ISO 14298-2013.

El cumplimiento de la norma ISO 9126 requeridos, en relación con el desarrollo de software que deba realizarse para la adaptación del SISTEMA DE EMISIÓN DE PASAPORTES y para su integración con otros sistemas de información, tanto de el Ministerio de Relaciones Exteriores como de externos.

Prácticas de Seguridad

En los casos que corresponda, la Propuesta Técnica debe cumplir con las siguientes normativas:

a) Política de Seguridad de la Información de el Ministerio de Relaciones Exteriores

b) Ley sobre Protección de la Vida Privada: Artículo 2.5, 2.6, 2.7 y 97 de la Constitución, Ley de Transparencia y Acceso a la Información Pública - Ley 27806, Ley de Protección de Datos Personales - Ley 29733.

c) Ley sobre Documentos Electrónicos, Firma Electrónica y servicios de certificación de dicha firma: Ley de Firmas y Certificados Digitales - Ley 27269.

d) Disposiciones relativas a la Modernización del Estado y Gobierno Electrónico: Ley Marco de Modernización de la Gestión del Estado - Ley 27658, Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013-2017, DECRETO SUPREMO Nº 081-2013-PCM.

Puestos de Trabajo

En los casos que corresponda, la Propuesta Técnica debe cumplir con las siguientes normativas:

a) Normas de ergonomía para trabajos de oficina con pantallas de visualización de datos Energy Star 4.0 en eficiencia en el consumo de energía eléctrica, para estaciones de trabajo de escritorio.

b) Las estaciones de trabajo de escritorio deberán estar dotadas de monitores LED o superior, de al menos 18.5 pulgadas y una resolución de 1366x768 pixeles.

Interoperabilidad

En los casos que corresponda, la Propuesta Técnica debe cumplir con las siguientes normativas:

a) Interna: SOA, XML, BPM, Web services sincrónicos o similar que aseguren el rendimiento, control y seguridad de las transacciones

b) Externa: SOA, XML, BPM, Web services seguros, bus de servicios empresariales, monitores de actividad

Formato de Imágenes

En los casos que corresponda, la Propuesta Técnica debe cumplir con las siguientes normativas:

a) Fotografía digital: Token Frontal Image Type, JPEG-2000, ICAO 2D, ISO/IEC FCD 19794-5

b) Patrones faciales: ANSI-INCITS 385-2004.

c) Impresiones dactilares: WSQ, ISO/IEC FCD 19794-4

d) Minucias de impresiones dactilares: ANSI-INCITS 378-2004

Dispositivos de Captura de Imágenes y de Lectura de Documentos

En los casos que corresponda, la Propuesta Técnica debe cumplir con las siguientes normativas:

a) Escáner de impresión dactilar plana (flat), certificación norma IAFIS, calidad de imagen para escáner FBI CJIS-RS-0010 de 500 ppi o superior.

b) Escáner de impresiones decadactilares planas (flat), del tipo tres palmadas (three slap), certificación norma IAFIS, calidad de imagen para escáner FBI CJIS-RS-0010 de 500 ppi o superior.

Pasaporte Electrónico

En los casos que corresponda, la Propuesta Técnica debe cumplir con las siguientes normativas:

a) ICAO Documento 9303 Parte 1, para MRTD (Machine Readable Travel Documents), sexta edición o superior

b) ISO 7810 Tarjetas de identificación – Características físicas formato ID-3

c) ANSI NCITS 322-2002 Métodos de pruebas de durabilidad de tarjetas
d) ICAO Suplemento al Documento 9303 para pasaportes electrónicos con capacidad de identificación biométrica.
e) ICAO NTWG TAG-MRTD/17-WP/15 Reporte técnico de durabilidad de pasaportes de lectura mecánica.
f) ISO 7816-1 Tarjetas de identificación – Tarjeta con circuitos integrados – Parte 1: Características físicas.
g) ISO 10373-6 Tarjetas de identificación – Métodos de pruebas para tarjetas con chip – Parte 6 Lectura sin contacto.
h) ISO 14443-4 Tarjetas de identificación – Tarjetas de circuitos integrados sin contacto – Parte 4 Protocolo de transmisión.
i) ISO 10373-1 Tarjetas de identificación – Métodos de pruebas – Parte 1:Características generales.

Además se debe garantizar el cumplimiento funcional del chip del pasaporte electrónico de acuerdo al modelo de capas ISO/OSI:

ISO/OSI Layer	Estándar	Ámbito
1-4	ISO 14443, Identification cards – Contact less integrated circuit(s) cards – Proximity cards	Hardware
6	ISO/IEC 7816-4:2005, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange ISO/IEC 7816-8:2004, Identifications cards – Integrated circuit cards – Part 8: Commands for security operations	Software Sistema Operativo
7	ICAO Application: ICAO NTWG, Development of a LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 May 2004 ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, October 01, 2004	Software de Aplicación

Formato de Documentos de Productividad Personal

En los casos que corresponda, la Propuesta Técnica deberá cumplir con uno de los siguientes estándares para formato de documentos electrónicos:

a) OpenDocument, ODF, ISO/IEC 26300:2006 o su versión más reciente
b) Office Open XML, OOXML u Open XML, ISO 29500:2008 o su version más reciente

NIVELES DE SERVICIO

El PROVEEDOR deberá cumplir los niveles de servicio de funcionamiento y de rendimiento, establecidos en esta sección y deberá implementar un sistema de administración de los niveles de servicio para que el MRE tenga acceso en todo momento a verificar el cumplimiento.

Este sistema debe constar de un sistema automático de monitoreo y control remoto "remote control and monitoring system (RCMS)" que monitoree todas las operaciones y estados criticos del sistema con señales de alertas y fallas.

El proveedor deberá realizar el monitoreo continuo de los niveles de servicio y cualquier incidente de severidad 2 y 3 deberá ser detectado y solucionado por el proveedor dentro del período establecido en la sección "Niveles de servicio".

El personal asignado por el MRE debera tener acceso de visualización al sistema automático de monitoreo y control de acceso para realizar el monitoreo continuo de cumplimiento de los niveles de servicio.

Funcionamiento

El incumplimiento de estos niveles de servicio dará lugar a la aplicación de las penalidades detalladas en los presentes términos de referencia.

Por el incumplimiento del SLA de cualquiera de los servicios, se aplicará una penalidad del 2% del monto que corresponda facturar en el período y/o mes.

El proveedor deberá elaborar y entregar informes de medición de todos los niveles de servicio, establecidos en el presente documento, los incidentes y el tiempo de solución, así como el control de cambios de manera mensual; dicho informe deberá ser entregado dentro de los 10 primeros días del mes siguiente al mes de medición.

Sistema Central de Identificación

El Sistema Central de Identificación, deberá tener una disponibilidad no menor a la señalada en régimen de funcionamiento de 7x24, todos los días del año, para cada uno de los servicios que se detallan a continuación:

Disponibilidad de la solución integral	99,95%	Mensual	Incluye el funcionamiento conjunto de ambos centros de datos (principal y de contingencia)
Disponibilidad de funcionamiento del sistema de pasaportes (ejecutable y base de datos)	99,95%	Mensual	Incluye la disponibilidad del hardware y software (servidores, SAN, librerías, etc.)
Disponibilidad de funcionamiento del sistema de firma digital	99,95%	Mensual	

Disponibilidad de funcionamiento de equipos de captura y entrega (equipo de cómputo desktop, lectores de huella, lectores de pasaporte, lectores de tarjetas inteligentes)	Lima: 99,5% 22 Oficinas Consulares con mayor demanda: 95% 89 Oficinas Consulares: 90%	Mensual	
Copia de respaldo del sistema de pasaportes (De acuerdo a la política establecida)	100%	Mensual	Respaldo diario
Entrega de los pasaportes comunes personalizados en las 111 Oficinas Consulares	Retraso máximo EEUU: 05 días Europa: 05 días América: 05 días Japón: 05 días Asia, África y Oceanía: 05 días	Variable	A los 20 días los pasaportes se declaran perdidos
Entrega de los pasaportes diplomáticos y especiales personalizados en Perú	Retraso máximo: 2 horas	Entrega diaria	La entrega de pasaportes electrónicos diplomáticos y especiales deberá realizarse con una frecuencia diaria (a excepción de los días declarados no laborables) entre las 8:00 y 16:30 horas
Porcentaje de desviación del plazo de implementación de mantenimientos correctivos	10%	Mensual	
Porcentaje de desviación del plazo de planificación de mantenimientos correctivos	10%	Mensual	

Cobertura mínima de prueba de casos de uso en mantenimiento correctivos	80%	Mensual	

En caso de retrasos en la entrega de pasaportes se aplicará una penalidad de 50 USD (Cincuenta Dólares Americanos) por pasaporte que se entregue fuera del tiempo establecido.

En caso de daños durante el transporte o entrega de pasaportes fallidos por causas ajenas al proveedor, el PROVEEDOR deberá reeponer los pasaportes, y deberá registrar los pasaportes fallados en la base de datos de stock y producción como corresponda.

En caso de pérdidas de pasaportes personalizados o de libros de pasaportes pre-personalizados, se aplicará una penalidad de 150 USD (Ciento Cincuenta Dólares Americanos) por pasaporte o libro perdido.

En caso de pérdidas acumuladas mayores a 1000 pasaportes durante el periodo del contrato, el MRE podrá rescindir el contrato.

Estaciones de Trabajo

El PROVEEDOR deberá garantizar que los equipos y aplicaciones permitan que las estaciones de trabajo del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES, considerando cada uno de sus componentes, puedan funcionar conforme al siguiente horario:

Oficinas	Lunes a Viernes	Sábado	Domingos y feriados
MRE	8:00 a 16:00 horas	8:00 a 13:00 horas	-
Oficinas Consulares	8:00 a 16:00 horas	8:00 a 13:00 horas	-

Las estaciones de trabajo podrán estar fuera de servicio de acuerdo a los siguientes casos:

El tiempo máximo de inoperatividad (total para las 111 Oficinas Consulares) por incidentes, fallos de equipos, reemplazo en cada sede de expedición será del 5% anual.

El tiempo máximo de inoperatividad por mantenimientos planificados de la solución integral será de 0,5% anual.

El tiempo máximo de inoperatividad por incidentes, fallos de equipos, reemplazo en el centro de procesamiento será de 0,2% anual.

En caso que la notificación de la falla se produzca en días y/u horas no contempladas en el régimen de funcionamiento, los tiempos máximos de fallas comenzarán a contabilizarse desde el día y hora de funcionamiento más próximo.

En el caso del equipamiento que conforma las estaciones de trabajo instaladas en las Oficinas Consulares y la sede del Ministerio de Relaciones Exteriores, el PROVEEDOR deberá cumplir con el tiempo de solución de falla

establecido, contado desde la fecha y hora de aviso informando de la indisponibilidad del equipamiento instalado.

Durante la vigencia del contrato, el Proveedor deberá solucionar la falla a su costo, ya sea mediante reparación, mantención de repuestos en sedes consulares y en Lima, recambio o reemplazo de equipos.

Las fechas de mantenimiento e inoperatividad programada deben ser definidas en los meses de menor demanda según las estadísticas registradas en la base de datos de el Ministerio de Relaciones Exteriores.

El mantenimiento en los centros de procesamiento y fábricas de personalización se deberán realizar como mínimo una vez al año.

Infraestructura Tecnológica

La disponibilidad mensual del funcionamiento de la Infraestructura Tecnológica del Servicio de Emisión de Pasaporte (incluye la disponibilidad del hardware y software, servidores, SAN, librerías,etc.), será del 99,95%

RENDIMIENTO

Sistemas de Atención a Usuarios, BackOffice, Bloqueo de Documentos

Para las transacciones de negocio originadas por los Sistemas de Atención a Usuarios, Backoffice central y Bloqueo de documentos, el tiempo de respuesta del sistema central, incluyendo a todos los servidores que conformen la arquitectura de software y de base de datos (sin considerar sistemas externos), no debe superar los diez (10) segundos, para el 95% de las transacciones que se realicen.

Esta restricción operacional regirá mientras el nivel de carga de estos sistemas, no sobrepase las veinte (20) transacciones de negocio por segundo (TNPS), durante los días lunes a sábado entre las 8:00 y las 20:00 hrs., exceptuando los días festivos.

Las transacciones de negocio por segundo (TNPS) a considerar en esta medición corresponden a:

a) Inserción de una persona en la base de datos

c) Actualización de parte o de toda la información de una persona

e) Actualización de parte o de toda la información de un pasaporte electrónico

Atención de Solicitudes de Pasaportes Electrónicos

Durante la etapa de pruebas se medirá el tiempo total del Sistema de Atención de Usuarios el cual no deberá superar los cinco (05) minutos para el 90% de las atenciones durante toda la vigencia del contrato.

El tiempo será medido desde que el operador ingresa el número de identificación personal (DNI) al sistema de atención de usuarios y huella dactilar hasta que la solicitud ha sido aceptada.

SOPORTE Y MESA DE AYUDA



Los tiempos máximos de solución de reportes de fallas, desde la notificación que realice cualquier funcionario del Ministerio de Relaciones Exteriores a la Mesa de Ayuda, serán los siguientes:

Provisión de Insumos	Perú	Europa	Otros
Reemplazo de piezas por fallas de equipos en Oficinas Consulares y la sede de expedición en Lima	24 horas	72 horas	7 días

Control de cambios	Lima
Cambios en la configuración de la aplicación de personalización, procesamiento y firma digital	**96 horas**
Cambios en la configuración de la base de datos de pasaportes emitidos, control de insumos e inventario	**96 horas**

Tiempos de solución de incidentes (horas)

Severidad	Lima	Europa	Otros
Severidad 1	16 horas	36 horas	72 horas
Severidad 2	8 horas	36 horas	48 horas
Severidad 3	4 horas	24 horas	24 horas

La medición se realiza de forma mensual y para el cálculo se utiliza el promedio simple de los tickets de incidentes por severidad del período.

a. Severidad 1: Sólo (un) 1 módulo del sistema se encuentra inoperativo
b. Severidad 2: Más de (un) 1 módulo del sistema se encuentra inoperativo, aún se pueden operar algunos módulos del sistema.
c. Severidad 3: El sistema está completamente inoperativo

La severidad la determina la persona que coloca el ticket de atención del incidente. Para la medición del tiempo de atención se debe considerar desde que el ticket se registró (mediante un sistema de mesa de ayuda, correo electrónico o llamada telefónica) hasta que el incidente está completamente solucionado.

El ticket puede ser colocado por los funcionarios desde las Oficinas Consulares y el personal del MRE tendrá acceso a los reportes estadísticos de la aplicación de Mesa de Ayuda del PROVEEDOR para contabilizar las horas mensuales de incidentes.

Los tickets se realizarán directamente en la Mesa de Ayuda del PROVEEDOR.

Para el caso de incidencia severidad 3: el proveedor deberá realizar el análisis causa raíz correspondiente con la finalidad de determinar la causa precisa de porqué ocurrio el incidente y debe elaborar un informe al respecto, debiendo presentarlo como máximo a 7 días de cerrado el ticket del incidente.

SISTEMA DE EMISIÓN DE PASAPORTES ELECTRÓNICOS

El Sistema de Emisión de Pasaportes Electrónicos se compone de:

a) Base de Datos de Identificación
b) Plataforma tecnológica central
c) Fábricas para la personalización de documentos
d) Servicio de Mesa de Ayuda
e) Interoperabilidad interna y externa
f) BackOffice Central
g) Bloqueo de Documentos
h) Sistema de Gestión de Información
i) Sistemas Biométricos AFIS
j) Servicios de Información al Usuario
k) Sistema de atención al usuario
l) Aplicación central de procesamiento y firma digital
m) Firma Digital y PKI
n) Sistema de gestión de insumos e inventario
o) Módulo de Seguridad y Auditoria
p) Registro de Pagos
q) Sistema de peritos biométricos

La Base de Datos de Identificación, mantiene información de todos las personas que alguna vez han solicitado un pasaporte. Esta información comprende el número de identificación personal (DNI), fotografías digitales, firmas manuscritas digitalizadas, diez impresiones dactilares planas y minucias de las impresiones dactilares. Cada vez que una persona solicita un nuevo pasaporte se verifica la existencias en la base de datos de sus diez impresiones dactilares, en caso de existir éstas, se registra la huella dactilar de verificación y se actualiza su información e imágenes, conservando el historial de documentos emitidos.

Las impresiones decadactilares se obtienen en la primera filiación de la persona y en algunos casos en las expediciones de nuevos documentos.

El PROVEEDOR deberá realizar a su costo la conexión del Centro de Procesamiento del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES del MRE con el Centro de Datos del MRE y con el Centro de Procesamiento del nuevo pasaporte electrónico de Migraciones, durante el periodo del contrato; esta conexión debe incluir su mantención y soporte. La comunicación entre el Centro de Procesamiento y las Fábricas de Personalización deberá ser mediante canales seguros cifrados.

REQUERIMIENTOS DE SOFTWARE

El software requerido debe propender a la integración de procesos transversales, evitando la duplicidad de funciones, mejorando el control, seguimiento y la automatización de los flujos de trabajo. De esta forma, los aplicativos del SERVICIO DE EMISIÓN CENTRALIZADO DE PASAPORTES debe proveer la usabilidad necesaria, seguridad de la información, auditoría, prevención y detección de fraudes y continuidad operacional. Además,

para una gestión moderna acorde con el gobierno electrónico se debe proveer herramientas para la inteligencia de negocios, la interoperabilidad, el manejo de documentos y la firma electrónica todo esto orientado en mejorar continuamente la Atención a Usuarios y la operación del MRE.

De esta forma, los sistemas deben cumplir al menos con los siguientes requerimientos:

a) Idioma español para todas las aplicaciones de usuario (pantallas, reportes e informes) que se implementen dentro de la solución propuesta, así como también los mensajes de ayuda y error.

b) Idioma inglés o español para aquellas aplicaciones de administración especializadas, configuración, centro de datos y fábricas de documentos

c) Sistemas Web desarrollados en base a la arquitectura *N* capas, lenguaje de programación C# o java.

d) Sistema de información basado en automatización de procesos de negocios y flujos de trabajo flexibles.

e) Los operadores del sistema deberán utilizar autenticación por huella dactilar o certificado digital.

f) Generación y almacenamiento de reportes seguros.

g) Aplicaciones para la generación de reportes no estructurados.

h) Definición y control de registros de auditoría y trazabilidad.

i) Integración con centro de contactos multicanal (Internet y presencial).

j) Modulo de administración de usuarios (operadores)

k) Gestión de Roles del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES

l) Gestión de Control de acceso del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES

BASE DE DATOS CENTRAL DE IDENTIFICACIÓN

El PROVEEDOR debe considerar una Base de Datos capaz de recibir y almacenar en línea los datos e imágenes que se capturan durante los procesos de primera filiación y emisión de un nuevo pasaporte electrónico.

El PROVEEDOR deberá efectuar la consulta de todos los datos almacenados en la Base de Datos de Identificación, incluyendo la información relativa a las personas (datos e imágenes), solicitudes y documentos emitidos, al momento que se efectúa una solicitud de pasaporte.

Requisitos Mínimos

El Sistema de Gestión de Base de Datos debe cumplir al menos con los siguientes requisitos:

a) Almacenamiento de imágenes (objetos binarios) directamente en la base de datos

b) Administración de la Disponibilidad

c) Administración de la Seguridad

d) Administración de las Operaciones (incluyendo logs y trazabilidad de los eventos de operaciones)

e) Aplicaciones, herramientas y conectores para Gestión de Información e Inteligencia de Negocios

f) Replicación y/o creación de Vistas Indexadas

g) Incluir el middleware necesario para la explotación del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS de acuerdo a los niveles de servicio requeridos

i) Integración con el Sistema de Respaldo y Recuperación de Información para operar en línea, con la base de datos operativa.

Información que se Almacena por cada Persona

El SISTEMA DE EMISIÓN DE PASAPORTES deberá almacenar en su Base de Datos de Identificación y mantener en línea, para cada persona que haya realizado su primera filiación civil o que haya renovado sus documentos, al menos la siguiente información:

a) Numero de Identificación personal DNI

b) Nombre completo que se consignará en el documento

c) Fotografía digital

d) Imágenes de una (1) impresión dactilar plana de verificación.

e) Imágenes de las diez (10) impresiones dactilares planas.

f) Minucias de impresiones dactilares planas para AFIS 1:1 y para AFIS 1:N

g) La historia de todas las solicitudes de documentos presentadas por la persona. Esto debe incluir al menos el número de serie, la fecha de emisión del documento, fecha de vencimiento, sede en la que se presentó la solicitud, causa declarada (vencimiento, pérdida, robo), eventual condición de bloqueo e identificación de los funcionario que intervinieron y/o que procesaron la solicitud.

h) La historia de todas las solicitudes de bloqueos de pasaportes

Para emitir el pasaporte, los datos del ciudadano seran capturados mediante la lectura automática OCR del DNI o de forma manual. Los datos "Profesión", "Estatura", "color de ojos" y "Teléfono", serán ingresados por el Operador en forma manual, para consolidar los datos a ser impresos en la hoja de datos del pasaporte y los datos a ser grabados en el chip, generando registros de auditoria de las transacciones realizadas.

El administrador del sistema no debe tener acceso a la modificación de esta información. Cada vez que una persona obtiene un nuevo pasaporte se captura su fotografía y al menos una impresión dactilar plana para verificación AFIS 1:1; las cuales deben incorporarse a la Base de Datos de Identificación. Si las correspondientes imágenes ya existían en dicha base de datos, solo se deberá almacenar la huella de verificación; de este modo siempre se dispone en línea de la información reciente e histórica de cada persona. Tratándose de primeras filiaciones se debe capturar diez (10) impresiones dactilares planas, capturadas en tres palmadas (4-4-2).

Interoperabilidad con Otros Sistemas de Información

El SERVICIO DE EMISIÓN DE PASAPORTES deberá interactuar permanentemente con el Sistema Integrado de Migraciones, con el sistema del RENIEC, y con sistemas de información externos.

El SISTEMA DE EMISION DE PASAPORTES debe proveer y utilizar los servicios necesarios para implementar la interacción con sistemas internos y externos.

Interoperabilidad con el Sistema de Actividades Migratorias del MRE (SAM) del Ministerio de Relaciones Exteriores

El Sistema Central de Identificación deberá consultar y actualizar el estado de la información que esté almacenada en el SAM del Ministerio de Relaciones Exteriores, a fin de evitar que se emitan diferentes pasaportes a un mismo solicitante.

Esta consulta y/o actualización se debe hacer en forma transparente para los usuarios, para fines de funcionamiento o eficiencia de acceso, manteniendo rigurosamente la integridad y coherencia de los datos.

Durante el periodo del contrato, si el MRE pone en produccion el sistema de Autoadhesivos Consulares que reemplazará al SAM, el PROVEEDOR deberá realizar la integración del nuevo Sistema de Emisión de Pasaportes con este nuevo sistema de Autoadhesivos Consulares.

Interoperabilidad con el Sistema Integrado de MIGRACIONES (SIM)

El Sistema Central de Identificación deberá consultar el estado de la información que esté almacenada en el SIM de Superintendencia Nacional de Migraciones. Permitiendo asimismo, que MIGRACIONES pueda consultar al Sistema Central de Identificacion.

Esta consulta se debe hacer en forma transparente para los usuarios, para fines de funcionamiento o eficiencia de acceso, manteniendo rigurosamente la integridad y coherencia de los datos.

Interoperabilidad con Sistemas Externos

El Sistema de Emisión de Pasaportes electrónicos deberá tener la capacidad de interactuar permanentemente con el sistema del RENIEC para la verificacion de datos de las personas.

Plataforma Tecnológica Central

El PROVEEDOR deberá proveer todo el equipamiento de hardware, software, licencias, instalaciones, infraestructura de red, infraestructura de seguridad y herramientas de administración para implementar una plataforma de tecnologías de información y comunicaciones que dará sustento al Sistema Central de Identificación.

Las bases de datos y el sistema de firma digital de los datos biográficos contenidos en el chip del pasaporte, deberán brindarse de manera centralizada desde los centros de procesamiento en Lima, tanto el dispuesto por el Ministerio de Relaciones Exteriores, como el centro de procesamientos principal. El PROVEEDOR podrá proporcionar otras alternativas que serán aprobadas por el MRE

Equipamiento del Centro de procesamiento

El proveedor deberá entregar e instalar todos los servidores necesarios para soportar la solución integral en un centro de datos principal y un centro de datos de contingencia que podrá estar en modalidad activo-pasivo. En la configuración activo-pasivo, la configuración deberá mantener actualizada en tiempo real los datos en ambos centros de datos (principal y de contingencia).

En el centro de procesamiento principal se requiere de:

- Servidores en alta disponibilidad para la aplicación central de procesamiento.
- 2 Equipos HSM en alta disponibilidad con FIPS 140-2 nivel 3 para la firma digital del contenido de los pasaportes.
- Servidores con balanceo de carga, en redundancia y alta disponibilidad modo activo-pasivo para la Base de datos de pasaportes emitidos.
- Servidor para la base de datos de insumos e inventario.
- Servidores de alta disponibilidad para el sistema AFIS.
- El centro de datos de contingencia debe ofrecer la posibilidad de asegurar la continuidad del servicio.

Los servidores deberán ser instalados en el Centro de Procesamiento provistos por el PROVEEDOR (principal y contingencia).

El dimensionamiento y capacidades de los servidores deben estar conformes con los niveles de servicio establecidos en el presente documento. Las especificaciones técnicas son descritas en el Anexo 2 del presente documento.

Infraestructura de seguridad de la plataforma tecnológica

El proveedor deberá proporcionar una solución que considere la seguridad transversal como prioritaria en cuanto a:

- Confidencialidad de los datos mediante encriptación
- Control de acceso por políticas de gestión de las autorizaciones
- Trazabilidad
- Protección de los puestos de trabajo
- Autenticación de todos los tipos de usuarios que acceden al sistema
- Confidencialidad de los intercambios de datos
- Protección de los accesos físicos

Licenciamiento de sistemas operativos y base de datos

El proveedor deberá proporcionar el licenciamiento de los sistemas operativos Windows necesarios para la operación de las estaciones de trabajo, servidores y de las aplicaciones actualmente en producción.

Asimismo, el proveedor deberá proporcionar el licenciamiento completo necesario para la base de datos de la Solución Integral las mismas que deben ser SQL Server 2014 Enterprise como mínimo NL Gobierno.

Licenciamiento antivirus

El proveedor deberá entregar el licenciamiento antivirus para protección de todos los servidores, el sistema antivirus deberá actualizarse y garantizar la disponibilidad de los servicios especificados en la sección "Niveles de servicio" del presente documento.

La herramienta centralizada de gestión de antivirus debe permitir:

- Gestión de grupos a través del Directorio Activo
- Instalación remota de agentes antivirus
- Administración centralizada de cuarentena
- Gestión de políticas
- Gestión de notificaciones de incidentes, notificación vía correo, SNMP y entradas de registro

Requisitos Mínimos

La Plataforma Tecnológica Central del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES, deberá cumplir al menos con los siguientes requisitos:

a) Virtualización en servidores, almacenamiento y conectividad para los centros de datos principal y secundario

b) Arquitectura Activo/Pasivo de alta disponibilidad, distribuida en los centros de datos principal y secundario.

c) Sistema de almacenamiento en alta disponibilidad, con capacidad para las bases de datos de producción y de consulta, las cuales se deberán mantener replicadas en ambos centros de datos en forma sincrónica/asincrónica.

d) Administración de Niveles de Servicio

e) Administración de la Capacidad

f) Administración de Servicios de Continuidad Operacional

g) Administración de la Disponibilidad

h) Administración de la Seguridad

i) Administración de las Operaciones (incluyendo logs y trazabilidad de los eventos de operaciones)

j) Sistema de Respaldo y Recuperación de Información

El Plan de Contingencia y los procedimientos de recuperación ante falla, caso fortuito o fuerza mayor, deberán ser probados por el PROVEEDOR y constatados por el MRE al menos una (1) vez al año.

Producción y Personalización de Documentos

La producción de los documentos será de responsabilidad del PROVEEDOR, el cual deberá contar con al menos 2 fábricas de personalización 01 localizada en Europa o Estados Unidos de América, y 01 Lima-Perú desde las cuales se realizará la distribución de los pasaportes personalizados a las 111 Oficinas Consulares a nivel internacional, y a la sede de expedición del MRE en Lima. Las fábricas deberán contar con controles de seguridad físicos, lógicos y procedimentales necesarios para proteger los sistemas de personalización y los insumos contra uso no autorizado, y asegurar la disponibilidad de los servicios de producción de pasaportes conforme a los Niveles de Servicio establecidos en el presente documento:

- Seguridad de acceso físico
- Perímetros de seguridad
- Cámaras de video vigilancia
- Controles de seguridad en la separación de roles
- Controles en la selección y capacitación del personal
- Seguridad en el cableado eléctrico y estabilización de energía
- Seguridad en el cableado de datos
- Seguridad en las redes de datos
- Controles de la operación
- Protección de datos personales

Anualmente, el MRE designara a dos miembros de su personal y/o auditores externos que realicen una inspección y auditoria de las fábricas. El costo de la contratación de los auditores y el transporte y estadía en cada fábrica será cubierto por el PROVEEDOR.

El PROVEEDOR deberá implementar un plan de contingencia y un reporte de evaluación de riesgos que permita asegurar la disponibilidad de los servicios.

Control de Stock

El PROVEEDOR deberá gestionar y registrar los materiales e insumos utilizados en un sistema en línea y en tiempo real de control de stock de materiales en todas las fábricas de personalización, mediante el cual el PROVEEDOR deberá realizar lo siguiente:

a) Mantener un stock de todos los materiales, insumos y consumibles utilizados en el proceso de personalización.

b) Contar con un sistema de alerta temprana de niveles de stock crítico

d) Registrar los insumos perdidos, robados, deteriorados, eliminados, etc.

e) Establecer roles de seguimiento, administración y control de insumos.

f) La aplicación debe generar logs de auditoría de los registros de ingreso, transferencia y eliminación de insumos, indicando el operador, la fecha y la agencia correspondiente.

g) La aplicación deberá registrar pistas de auditoría completa que incluya el conteo y la conciliación de todos los materiales (usados, no usados, defectuosos o estropeados) y registros certificados de los mismos.

h) Registrar datos de todos los documentos de viajes en blanco perdidos o robados.

i) La aplicación debe ser licenciada y con soporte durante el tiempo que dure la prestación del servicio.

El proveedor deberá presentar al MRE un informe semestral del control de todos los materiales, insumos y consumibles utilizados en el proceso de personalización, los insumos perdidos, robados, deteriorados, eliminados, los documentos de viajes en blanco perdidos o robados.

Para efectos de auditoria, el MRE deberá poder visualizar los registros de la aplicación respecto del control de insumos perdidos, robados, deteriorados, eliminados, los documentos de viajes en blanco perdidos o robados. Esta visualización debe poder realizarse desde el Centro de Monitoreo implementado para el MRE.

Control de Producción

El PROVEEDOR deberá gestionar y registrar la producción en un Sistema de Control de Producción que garantice:

a) Cuadratura entre órdenes de producción, materiales y documentos de acuerdo a los lotes de producción. La supervisión de esta cuadratura deberá realizarse por al menos dos personas.

b) Que todos los documentos rechazados y que no serán considerados como válidamente emitidos, sean inutilizados antes de ser eliminados.

c) El control de producción deberá ser a su vez auditable y deberá contar con mecanismos de seguimiento.

d) Este sistema de control de producción debe permitir registrar y contabilizar los pasaportes entregados a los ciudadanos en las Oficinas Consulares, así como casos de daño, perdida o no entrega de pasaportes en las Oficinas Consulares.

El PROVEEDOR deberá presentar al MRE en Lima un informe bimestral del control de la producción en todas las Oficinas Consulares y la sede de expedición en Lima, indicando las solicitudes recibidas, pasaportes entregados a las Oficinas Consulares, pasaportes entregados a los ciudadanos, perdidos, dañados, indicando fechas de entrega y proyecciones futuras a fin de controlar la demanda de pasaportes.

El MRE se reserva el derecho de pedir al PROVEEDOR en cualquier momento un informe adicional al bimestral

Para efectos de auditoria, el MRE deberá poder visualizar los registros de la aplicación respecto del control de producción. Esta visualización debe poder realizarse desde el Centro de Monitoreo implementado para el MRE.

Control de Desechos

El PROVEEDOR deberá implementar un Sistema de Control que asegure que todos los desechos sean separados de acuerdo al tipo de material e inutilizados antes de ser eliminados.

En el caso de los desechos químicos o que representen algún peligro para la salud de las personas o para el medio ambiente, deberán ser previamente tratados siguiendo estrictamente la legislación vigente en esta materia del país donde se encuentre localizada la fábrica.

Para efectos de auditoria, el MRE deberá poder visualizar los registros de la aplicación respecto del control de desechos. Esta visualización debe poder realizarse desde el Centro de Monitoreo implementado para el MRE.

Control de Calidad de Materiales

El PROVEEDOR deberá implementar mecanismos de control de calidad de los materiales destinados a la personalización y obtención de los pasaportes terminados que cumplan con los requerimientos establecidos en el Documento 9303 Séptima Edición o superior y las ediciones que se actualicen durante el tiempo de vigencia del contrato.

A fin de reducir los casos de falsificación de pasaporte, las impresoras e insumos (tintas, láminas, hologramas) empleados para los procesos de personalización de pasaportes deben ser exclusivos para este fin, es decir, no deben ser comercializados a terceras Entidades no autorizadas por sus respectivos países para producir documentos de identidad. Los insumos deben de ser idénticos a los utilizados por la Superintendencia Nacional de Migraciones a fin de tener un documento con características de seguridad idénticas, en los tres niveles de verificación, para todos los ciudadanos peruanos.

Control de Calidad a los Documentos Terminados

Los documentos terminados serán sometidos a controles de calidad, que verifiquen aspectos como la calidad de la impresión, la legibilidad mecánica y computacional, las medidas de seguridad, la durabilidad, la personalización electrónica de los pasaportes y la coherencia en la impresión de los datos de personalización. Se efectuará un control de calidad al mes, sin perjuicio que el Ministerio de Relaciones Exteriores efectúe controles adicionales.

Para implementar este control de calidad mensual, el MRE inyectará solicitudes de documentos con datos de prueba para Pasaportes Electrónicos, los cuales deberán ser impresos y marcados como "inutilizados". Estas muestras serán enviadas a laboratorios especializados seleccionados por el MRE, a costo del PROVEEDOR, cuyos análisis y resultados deben incluirse en los informes de avance y estado del proyecto correspondientes, como también las medidas que se requieran tomar para solucionar las deficiencias que se hubiesen detectado.

Servicio de Mesa de Ayuda

El PROVEEDOR deberá habilitar a su costo una Mesa de Ayuda, que deberá otorgar servicios a todos los usuarios del SERVICIO DE EMISIÓN DE PASAPORTES, funcionar como un punto único de contacto, mantener el

control de los niveles de servicio comprometidos y dar cumplimiento a las certificaciones definidas en este documento.

Los usuarios de la Mesa de Ayuda serán los funcionarios de las Oficinas Consulares y operadores del MRE.

La Mesa de Ayuda de nivel 1, 2 y 3, podrá estar ubicada fuera de las dependencias del MRE y deberá ser accesible mediante un número telefónico único sin costo de llamadas para el MRE, así como correo electrónico y formularios web.

La Mesa de Ayuda deberá tener al menos las siguientes funcionalidades:

a) Atender y registrar todas las solicitudes efectuadas por los usuarios del SERVICIO DE EMISIÓN DE PASAPORTES, a través de llamadas telefónicas, correo electrónico y formularios Web.
b) Categorizar casos en forma automatizada.
c) Responder a las solicitudes de los usuarios con la información apropiada y en el tiempo comprometido
d) Dirigir los casos hacia los grupos de soporte apropiados
e) Informar a quienes corresponda sobre los casos que generen impacto en sus actividades.
f) Cerrar los casos resueltos, sólo una vez que ha obtenido la aprobación del usuario correspondiente (firmó la boleta de servicio o registró su conformidad directamente en el sistema)

La Mesa de Ayuda deberá contar con un conjunto de herramientas cuyo fin es agilizar la atención y aumentar la calidad de servicio, para la mejora continua de sus procesos, entre estos sistemas, se deberá contar al menos con los siguientes:

g) Sistema de gestión de llamadas (número de llamadas, tasa de abandono, tiempos de atención, etc.)
h) Base de conocimiento (scripts de atención, alternativas de solución de problemas, etc.)
i) Sistema de registro, control y monitoreo de niveles de servicio
j) Sistema de consulta y seguimiento de casos

El funcionamiento de la Mesa de Ayuda deberá ser durante las 24 horas todos los días del año.

El PROVEEDOR podrá considerar el uso de un sistema de centro de contactos para clasificar las llamadas dirigidas a la Mesa de Ayuda.

El PROVEEDOR deberá entregar mensualmente, dentro de los diez (10) primeros días corridos, un informe sobre la calidad de los servicios otorgados por la Mesa de Ayuda y el cumplimiento de todos los niveles de servicio prestados durante el mes inmediatamente anterior.

Módulo de administración de usuarios (operadores)

El proveedor deberá implementar controles apropiados para proteger contra el fraude interno todos los sistemas de producción, los sistemas AFIS, mediante;

- Separación de roles
- Monitoreo de las actividades críticas en la gestión del ciclo de vida de los pasaportes: ingreso y retiro en los almacenes, personalización, fallos y entregas, solicitud y autorización de emisión.
- Registro de auditoría de las actividades del personal según roles asignados
- Control de asignación y permisos de acceso según roles.
- Los roles y permisos de acceso deben poder gestionarse considerando:
  a) Suspensiones del personal
  b) Retiro de la entidad

c) Vacaciones
d) Rotación o cambio de área de trabajo.

- El proveedor deberá desarrollar un Módulo para la administración de usuarios conforme a los roles establecidos.

Gestión de Roles

Los roles para la gestión del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES y el flujo de procesamiento y emisión de pasaportes electrónicos, debe ser propuesto por el proveedor, debiendo contener al menos:

- Separación de roles, los roles de auditoría y protección de los registros de auditoría deben ser independientes de los roles de operación de los sistemas y ambientes.
- El rol del control de calidad debe ser separado del rol de recepción de solicitud de emisión de pasaportes.
- El rol de monitoreo de los ambientes, de las Oficinas Consulares y almacenes debe ser separado de las actividades de producción.
- El rol de monitoreo de los sistemas debe ser separado del rol de la operación y del flujo de producción.

El proveedor deberá documentar una matriz de roles, proponiendo los perfiles que deben ser cumplidos por el personal. La capacitación por cada rol se recibirá como parte del presente contrato con anticipación a la puesta en producción del servicio de emisión de pasaportes electrónicos, conforme al Plan de Capacitación correspondiente.

Gestión de Control de Acceso

Debe ser requerida la autenticación de acceso para permitir el uso o administración mediante certificados digitales o control de acceso biométrico, en caso de no contar con los certificados digitales de acceso o no ser exitosa la verificación biométrica, el Nuevo Sistema de Pasaportes Electrónicos no debe permitir el acceso a la aplicación de solicitud de pasaportes.

En caso de utilizar certificados digitales de acceso deben ser transportados entregados a los administradores por un canal seguro que asegure la autenticidad de la identidad del titular y suscriptor del certificado.

Definición y control de registros de auditoría y trazabilidad

El PROVEEDOR deberá implementar una solución que contenga herramientas de trazabilidad y auditoría para la recolección y manejo de eventos, manejo de logs, que permitan efectuar posteriores búsquedas, correlaciones y generación de reportes, o con el fin de detectar amenazas potenciales o comportamientos anómalos. Considerar registro de por lo menos los usuarios y direcciones IP utilizadas en los diferentes niveles y roles de acceso.

SISTEMA BIOMÉTRICO AFIS

El PROVEEDOR deberá implementar e integrar al SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES, un sistema biométrico basado en impresiones dactilares, el cual

deberá ser utilizado para las solicitudes de pasaporte por primera vez (búsqueda 1:N contra toda la base biométrica), y de autenticación 1:1 del solicitante (comparación biométrica de la solicitud contra la información biométrica contenida en el AFIS para el mismo solicitante) para las solicitudes de nuevo pasaporte cuando concurre por segunda vez.

El PROVEEDOR podrá sugerir el orden en que se ejecuten las verificaciones biométricas en los distintos procesos, pero la forma en que finalmente ello se realice será definida por el MRE.

El sistema AFIS, deberá utilizar las impresiones dactilares almacenadas en la Base de Datos del SAM en el formato actual WSQ de 500 ppi.

La configuración presentada en la propuesta para AFIS debe ser acreditada mediante certificados del fabricante del sistema correspondiente.

El PROVEEDOR deberá informar la cantidad de huellas utilizadas para efectuar la búsqueda mediante AFIS 1:N.

El sistema AFIS debe cumplir los siguientes requerimientos:

- Debe almacenar y procesar registros de las diez huellas dactilares planas de los solicitantes.
- Capacidad de almacenamiento mínimo de quinientos mil (500.000) registros de personas
- Capacidad mínima de procesamiento de doce mil (12.000) comparaciones 1:N por día (para soportar las consultas tanto por parte del MRE y MIGRACIONES).
- Capacidad mínima de procesamiento de cuarenta mil (40.000) comparaciones 1:1 por día (para soportar las consultas tanto por parte del MRE y MIGRACIONES).
- Tiempo de respuesta máxima de 8 segundos para búsqueda AFIS 1:N
- Tiempo de respuesta máximo de 3 segundos para consultas AFIS 1:1
- Tasa de falsa aceptación (FAR) ≤ 0.0001%
- Tasa de falso rechazo (FRR) ≤ 0.01%

El sistema AFIS provisto por el contratista de la solución integral deberá haber pasado satisfactoriamente la evaluación ***Proprietary Fingerprint Template Evaluation II del Instituto NIST o equivalente.***

La verificación se realizará contrastando la información del proveedor del AFIS contra la información publicada en el portal web del Instituto NIST: http://nist.gov/itl/iad/ig/pftii.cfm

SISTEMA DE ATENCIÓN A USUARIOS

En términos generales el Sistema de Atención a Usuarios, provisto por el PROVEEDOR, deberá satisfacer al menos las siguientes funcionalidades:

a) Solicitud presencial de documentos de pasaportes
b) Captura en vivo automatizada de datos e imágenes (fotografías en color e impresiones dactilares)
c) Control automático de la calidad, tamaño y optimización de las imágenes capturadas (fotografías, impresiones dactilares).
d) Verificación de identidad 1:1 para todos los trámites de pasaportes electrónicos.
e) Búsqueda 1:N para todas las solicitudes de primer pasaporte
f) Envío automático de una solicitud de pasaporte a la fábrica (sólo en caso de haber aprobado todas las verificaciones requeridas, con los sistemas internos y externos del MRE).
g) Avisos a los usuarios vía teléfono móvil (SMS), según definición del MRE.

h) Entrega y activación de documentos
i) Bloqueo definitivo de pasaportes de manera presencial y por Internet.

Habilitación de Sedes de Atención de Usuarios

Se deberá implementar el sistema de enrolamiento en las 111 Oficinas Consulares y la sede de expedición en Lima.

El PROVEEDOR deberá suministrar los telones o panel de fondos para toma de fotografías profesionales conforme a ICAO documento 9303 para todas las sedes de expedicion de pasaportes.

Los puestos de trabajo deberán contar con controles de estabilización de energía y apagado seguro en caso de cortes de energía.

ALMACENES DE INSUMOS

El PROVEEDOR debera contar con 2 almacenes adecuados para proteger los insumos y libros pre-impresos en las fábricas que cumplan con los siguientes controles:

- Controles de conservación de los insumos: humedad, temperatura.
- Sistemas contra incendios.
- Controles de acceso fisico.
- Cámaras IP de video vigilancia para el registro de ingresos, salidas y actividades dentro del almacén.
- Puertas resistentes a impacto en caso de robos.
- Cada personal debe ser claramente controlado y sólo personal autorizado debe poder ingresar.
- Registros de auditoria de cada etapa del proceso de gestion de insumos

Para la fábrica de personalización de Lima, el MRE pondrá a disposición del PROVEEDOR el espacio físico necesario para el almacen.

Anualmente, el MRE designará a dos miembros de su personal y/o auditores externos que realicen una inspección y auditoria de los almacenes. El costo de la contratación de los auditores y el transporte y estadía en cada fábrica será cubierto por el PROVEEDOR.

SOLICITUDES DE PASAPORTES

La Solicitud de pasaportes es una función esencial del Sistema de Atención a Usuarios, como también lo es la emisión de los correspondientes documentos. Para cumplir con lo anterior, se requiere de al menos la siguiente funcionalidad:

a) Recibir las solicitudes de documentos en las estaciones de trabajo de atención de usuarios, registrando los datos que aporte el solicitante y el motivo de la solicitud del pasaporte. Adicionalmente, se deberá bloquear automáticamente los pasaportes anteriores, en caso de ser necesario, incluyendo los registrados en el Nuevo Sistema de Pasaportes Electronicos del MRE, los pasaportes mecanizados registrados en el Sistema de Actividades Migratorias del MRE, el Nuevo Sistema de Electrónicos de la Superintendencia Nacional de Migraciones, el Sistema Integrado de Migraciones.

b) Analizar y validar la solicitud, respondiendo en línea si la petición de documento ha sido aceptada o queda pendiente, en cuyo caso el usuario deberá realizar las gestiones pertinentes antes que se pueda emitir el pasaporte.

c) Incorporar a la Base de Datos de Identificación los datos que corresponden a las menciones de los documentos y las imágenes capturadas

d) Realizar un seguimiento de los estados en que se encuentran las solicitudes

e) Enviar a la fábrica correspondiente la orden de producción de los documentos

f) Controlar el sistema de despacho de los documentos desde la fábrica de pasaportes hacia los puntos de entrega al usuario.

g) Activar los nuevos pasaportes y bloquear automáticamente los anteriores si hubiera.

h) Entregar los pasaportes.

i) El acceso al sistema de solicitud de pasaporte por parte de los funcionarios de las Oficinas Consulares debe ser autenticado con una tecnología segura que puede ser certificados digitales o sistemas biométricos o tarjetas inteligentes.

Tipos de Pasaportes:

Pasaportes para menores de 12 años

- No incluye huella dactilar
- Tiempo de vigencia de 3 años

Pasaporte para menores de edad entre 12 y 18 años de edad

- Incluye huellas dactilares
- Tiempo de vigencia de 5 años
- Al cumplir 18 años, el titular deberá solicitar un pasaporte para mayor de edad

Pasaportes para mayores de edad

- Incluye huellas dactilares
- Tiempo de vigencia de 5 años

Pasaportes diplomáticos:

- Incluye huellas dactilares
- Tiempo de vigencia de 5 años

Pasaportes especiales:

- Incluye huellas dactilares
- Tiempo de vigencia de 2 años

El nuevo Sistema de Pasaportes Electrónicos para el MRE (SPE) debe contemplar la operatividad del pasaporte electrónico diplomático y especial para el MRE. La vigencia de los pasaportes deberá ser de 05 años e incluye las huellas biométricas. El MRE podrá cambiar la vigencia de esta clase de pasaportes antes de la puesta en producción del SPE.

El SPE deberá recoger los procesos operativos que se detallan en el presente documento para cada tipo de pasaporte electrónico.

CAPTURA DE DATOS DE LOS SOLICITANTES

El SISTEMA DE EMISIÓN DE PASAPORTES deberá capturar los datos de los solicitantes de pasaportes para:

a) Realizar la primera filiación (enrolamiento)
b) Verificar la identidad del solicitante
c) Completar o actualizar los demás datos del solicitante
d) Procesar solicitudes de documentos

En particular, el Sistema de Atención a Usuarios deberá considerar mecanismos para captura en línea de los datos del solicitante.

El proceso de captura de las diez (10) impresiones dactilares de las personas, deberá repetirse de acuerdo a las definiciones de el Ministerio de Relaciones Exteriores, para asegurar el buen funcionamiento del sistema biométrico AFIS 1:N.

CAPTURA EN LÍNEA

Las 111 Oficinas Consulares y la sede de expedicion en Lima, conectadas en línea mediante canales cifrados, con el SISTEMA DE EMISIÓN DE PASAPORTES deberán estar dotadas de estaciones de trabajo y dispositivos para la captura de datos en línea, todo de acuerdo a lo especificado en la sección "ESTÁNDARES, CERTIFICACIONES Y BUENAS PRÁCTICAS".

Cada puesto de trabajo de captura en línea, llamado tambien kit de captura, deberá considerar al menos lo siguiente:

a) Estaciones de trabajo conectadas con acceso al centro de procesamiento, con la capacidad y rendimiento suficiente para ejecutar el sistema operativo, las aplicaciones de administración y soporte, las aplicaciones de seguridad, las aplicaciones de productividad de oficina y las aplicaciones corporativas que se requiera para su funcionamiento
b) Los elementos para la captura de fotografías digitales, tales como: cámara digital y dispositivos de iluminación.
c) Sistema de captura en vivo de impresiones multidactilares - captura en tres palmadas (4-4-2).
d) Un escaner para la digitalizacion de documentos
e) Un equipo de captura de firma manuscrista
f) Un lector automático de los datos contenidos en el DNI físico (lector OCR), a fin de que los datos sean capturados directamente del DNI presentado por el solicitante.
g) Un lector de pasaportes que permita la lectura OCR y la lectura del chip RFID.

Adicionalmente, el proveedor deberá proporcionar 24 kits equipos móviles para la captura de datos para la personalización de pasaportes, los cuales deberán estar interconectados remotamente con el Nuevo Sistema de Pasaportes y en caso de contingencia deberá almacenar temporalmente la información que posteriormente

deberá ser exportado al Nuevo Sistema de Pasaportes. Cada kit debera estar compuesto de los equipos descritos en los items a), b), c), d), e) y f) de la presente seccion del documento.

OTRAS SOLICITUDES

Las Sedes de Atención a Usuarios que operan en línea con el SISTEMA DE EMISIÓN DE PASAPORTES recibirán además solicitudes de Bloqueo (Anulación) de los pasaportes de lectura mecanizada y de los electrónicos, en casos de pérdida, robo o extravío. También procederá a la anulación del anterior pasaporte cuando la persona ha obtenido un nuevo pasaporte.

ENTREGA DE DOCUMENTOS EN SEDES DEL MRE

El procedimiento de entrega de documentos deberá considerar al menos, las siguientes funcionalidades:

a) Verificación de la identidad de quien retira el documento mediante validación de una huella dactilar.
b) Verificación de los datos almacenados en el chip del pasaporte electrónico
c) Activación de los pasaportes utilizando AFIS 1:1 para el titular que retira el documento y en caso de menores de edad se activa con la huella del padre, madre o apoderado (configurable por sistema).
d) Verificación de los datos del pasaporte electrónico
e) Bloqueo definitivo (Anulación) del documento en caso de no ser retirado desde la sede en un plazo de 60 dias calendario (parámetro configurable) .

El PROVEEDOR debe considerar equipamiento de entrega en las 111 Oficinas Consulares integradas al sistema de emisión de pasaportes y en la sede designada en Lima por el MRE.

Las estaciones de entrega serán las mismas que para la captura de datos.

INVENTARIO DE DOCUMENTOS PERSONALIZADOS

El procedimiento para mantener el inventario de documentos en las Oficinas Consulares de documentos personalizados deberá considerar al menos las siguientes funcionalidades:

a) Emisión, recepción y seguimiento de oficios conductores de los documentos (equivalentes a una guía de despacho)

b) Altas de inventario: considera la recepción y lectura de cada documento mediante lectura del chip, lectura OCR-B u otro mecanismo a proponer.

c) Control de inventario, considera la cuadratura, registro de movimientos y manejo de faltantes y sobrantes en cada sede.

d) Bajas de inventario: considera entrega al usuario y devolución por caducidad o rechazo

e) Pérdidas: por robos en las Oficinas Consulares u otra causa

f) Reportes estadísticos y operativos

El inventario de documentos personalizados deberá ser visualizado y supervisado desde el Centro de Monitoreo que será en el implementado en el MRE.

SISTEMA DE BLOQUEO DEFINITIVO DE DOCUMENTOS

El PROVEEDOR deberá implementar un Sistema de solicitud web que permita el Bloqueo definitivo del pasaporte en caso de extravío, robo o hurto, el mismo que debe estar integrado al Sistema de Actividades Migratorias del Ministerio de Relaciones Exteriores y al nuevo Sistema de Pasaporte Electrónico.

La solicitud de bloqueo definitivo se podrá tambien realizar en alguna Oficina Consular o en el MRE y considerará la verificación de identidad del solicitante.

En ambos casos se requiere contar al menos con la siguiente funcionalidad:

- Generación de archivos con el listado de los documentos bloqueados, para ser enviado a terceros.
- Integración con el Sistema Integrado del MRE y la aplicación central de gestión de pasaportes.
- Implementar un servicio web para consulta por el Sistema Integrado del MRE (SIM) cuando un ciudadano pase por el control migratorio extranjero o peruano, se verifique la vigencia del documento ("Pasaporte Bloqueado-Anulado)".
- Cuando un ciudadano solicite un nuevo pasaporte, y este cuente con un pasaporte bloqueado anteriormente, la aplicación de enrolamiento debe mostrar el mensaje de alerta ("Pasaporte Bloqueado-Anulado)" al operador.
- Este sistema debe ser configurable, y debe poder ser inhabilitado por el Ministerio de Relaciones Exteriores.
- La lista de pasaportes bloqueados debe poder ser exportable para ser enviada a INTERPOL (Stolen and Lost Travel Documents - SLTD).
- El acceso a derechos de administrador de este sistema debe ser controlado con certificados digitales.
- El sistema debe registrar logs de auditoría de las solicitudes realizadas y cambios en la administración.

El procedimiento definitivo para el Sistema de Bloqueo de Documentos será acordado entre el Ministerio de Relaciones Exteriores y el proveedor y deberá estar disponible al comienzo de la emisión de los nuevos documentos y ser totalmente compatible con los anteriores documentos.

Unidad de Identificación y Autenticación AFIS

La Unidad de Identificación y Autenticación AFIS requiere al menos las siguientes funcionalidades:

a) Realizar la gestión operativa de la unidad
b) Emitir informes del proceso de los pasaportes
c) Realizar consultas sobre el estado y la historia de documentos y solicitudes
d) Monitorear el control de procesos y estadísticas
e) Verificar identidad (autenticar) usando AFIS 1:1
f) Identificar solicitantes de pasaportes usando AFIS 1:N
g) Resolver investigaciones de identidad utilizando AFIS
h) Disponer de funciones especializadas de AFIS.
i) Disponer de funciones especializadas para manejar impresiones dactilares.
j) Actualizar la información biométrica si fuera necesario

El PROVEEDOR debe presentar una especificación del hardware, software y un plan de entrega de éste.

Unidad de Control de Procesos

La Unidad de Control de Procesos requiere al menos las siguientes funcionalidades:

a) Realizar la gestión operativa de la unidad
b) Realizar la Gestión de pendientes de las tareas existentes en el proceso de solicitudes de documentos
c) Cambiar la prioridad de algunas solicitudes de documentos (urgencias)

Unidad de Control Policial

La Unidad de Pasaportes requiere al menos las siguientes funcionalidades:

a) Realizar la gestión operativa de la unidad
b) Verificar el cumplimiento de las normas relacionadas a impedimentos policiales.

GESTIÓN DE INFORMACIÓN

El PROVEEDOR deberá proveer un Sistema de Gestión de Información integrado con el SISTEMA DE EMISIÓN DE PASAPORTES, que opere a nivel operativo, estratégico y de auditoría interna, además deberá considerar las herramientas y aplicaciones necesarias para realizar la gestión de información con el menor impacto sobre el rendimiento del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

El PROVEEDOR deberá proveer y mantener los procedimientos que le permitan entregar datos del sistema para su posterior procesamiento por parte de el Ministerio de Relaciones Exteriores.

GESTIÓN ESTRATÉGICA

Se requiere contar con las aplicaciones, los informes y los datos necesarios para realizar la gestión estratégica sobre el funcionamiento del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES. Esta gestión está relacionada con la coordinación adecuada de las necesidades de los diferentes actores del SISTEMA DE EMISIÓN DE PASAPORTES lo que debe significar altos niveles de eficiencia y facilidad de acceso a los servicios otorgados.

Se requiere desarrollar inteligencia de negocio, como por ejemplo, para apoyar la toma de decisiones y para realizar pronósticos en materias tales como:

a) Cierre o apertura de una Sede
b) Pronósticos de demanda de solicitudes de pasaportes.

GESTIÓN OPERATIVA

Se requiere contar con las aplicaciones, los informes y los datos necesarios para realizar la gestión operativa sobre el funcionamiento del SISTEMA DE EMISIÓN DE PASAPORTES. Esta gestión está relacionada con el control, las mejoras que se deben realizar en el sistema y el cumplimiento de los niveles de servicio.

Por ello, el SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES deberá aportar los indicadores necesarios para el cumplimiento de dichos objetivos.

Como parte del Sistema de Gestión de Información el PROVEEDOR deberá proveer y mantener un Sistema de Gestión Operativa y de Infraestructura que esté a disposición de el Ministerio de Relaciones Exteriores, considerando al menos los siguientes aspectos:

a) Administración de usuarios y perfiles
b) Estadísticas operacionales
c) Administración de servicios de información
d) Estadísticas de servicios de información
e) Seguimiento a la implementación de nuevos requerimientos
f) Informe de activación de planes de contingencia
g) Informes sobre la seguridad del sistema
h) Gestión de la infraestructura que compone el SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES

Se requiere realizar una gestión de información en forma multidimensional, con facilidades de drilldown y rollup. A modo de ejemplo se puede mencionar el análisis multidimensional de documentos, donde la navegación sobre las solicitudes del Pasaporte Electrónico deberá ser posible realizarla de acuerdo a las siguientes dimensiones y la fecha:

a) Sede donde se realizó la solicitud
b) Pais, Provincia, Ciudad donde se realizó la solicitud
c) Pais, Provincia, Ciudad del domicilio que informa el solicitante
d) Tiempo de proceso

Adicionalmente y para apoyar la Gestión Operativa el PROVEEDOR deberá proveer y mantener herramientas de gestión de información para:

a) Extracción, transformación y carga de datos (ETL)
b) Análisis de datos tipo On-Line Analitycal Processing (OLAP)
c) Análisis de datos en línea tipo On-Line Transaction Processing (OLTP)
d) Consultas y reportes analíticos estructurados y no estructurados
e) Aplicaciones de acceso a reportes para usuarios finales

Para la administración de los Servicios de la Gestión y Operación el proveedor deberá contar con 3 Políticas base, que tendrá como mínimo las reglas básicas para su atención:

- Política de Monitoreo de Servicios
- Política de Incidentes y Problemas
- Política de Requerimientos y Cambios

AUDITORÍA INTERNA

El SISTEMA DE EMISIÓN DE PASAPORTES, deberá contar con aplicaciones para apoyar las tareas de la Auditoría Interna, tales como: análisis de la eficiencia del sistema, revisión de la eficaz gestión de perfiles y niveles de acceso de usuarios, generar reportes de los usuarios y direcciones IP utilizadas en los diferentes niveles de acceso asi como del uso de materiales, control de la información disponible para los funcionarios que utilizan el sistema y también la disponible para terceros, control de acceso a las aplicaciones, comportamientos anómalos, detección de intentos de fraude, trazabilidad de las

operaciones y documentos y obtención de reportes no estructurados, los cuales podran ser utilizados por el personal o auditores contratados por el MRE para realizar auditorias anuales internas.

PASAPORTE ELECTRÓNICO

La Ministerio de Relaciones Exteriores a través del SISTEMA DE EMISIÓN DE PASAPORTES deberá emitir el pasaporte electrónico.

Los pasaportes electrónicos deberán ajustarse a las recomendaciones de la OACI/ICAO, descritos en el Doc. 9303.

Cada PROVEEDOR debe presentar el diseño del nuevo pasaporte en relación a las medidas de seguridad establecidas en el presente documento. Respecto de los pasaportes comunes, el diseño estetico y de seguridad tanto del libro, como de la hoja de datos y del contenido del chip debe ser exactamente el mismo que es utilizado para la produccion de pasaportes electronicos por parte de MIGRACIONES, a fin de asegurar que se trata de un mismo documento para todos los ciudadanos peruanos, ya sea que radiquen en el pais como en el extranjero. Respecto de los pasaportes diplomaticos y especiales, el diseño estetico del libro y la hoja de datos podra variar conforme a las aprobaciones del MRE.

Medidas de Seguridad

Todas las medidas de seguridad tienen que ser identicas al pasporte electrónico de la Superintendencia Nacional de Migraciones.

Seran comunicadas en detalle al PROVEEDOR , siendo elementos de alta seguridad.

El pasaporte electrónico deberá incluir información de tipo texto e imágenes y medidas de seguridad que los protejan contra los intentos de adulteración y falsificación, y que faciliten la detección de este tipo de fraudes.

Los Pasaportes electrónicos deberán tener características de seguridad en los niveles 1, 2 y 3, como también considerar la evolución de estas medidas, de tal forma que los protejan contra los intentos de adulteración y falsificación, facilitando la detección de este tipo de acciones. Para el presente proceso se solicita que como mínimo el PROVEEDOR considere 10 medidas de seguridad distintas de nivel 1, 7 medidas de seguridad distintas de nivel 2, y 4 medidas de seguridad distintas de nivel 3; las mismas que deben estar distribuidas en el libro de pasaportes identicas al pasaporte electrónico de la Superintendencia Nacional de Migraciones.

La numeración de la serie del libro de pasaporte debe ser perforado por láser de una forma igual que el pasaporte electrónico de la Superintendencia Nacional de Migraciones.

La siguiente tabla incluye un detalle al respecto de las medidas de seguridad:

	MEDIDA DE SEGURIDAD	NIVEL	OBSERVACION	CARÁCTER
1	Kinegrama transparente	1		OBLIGATORIO
2	Guilloche o estructura de línea comparables	1	3 tintas	OBLIGATORIO
3	Impresión irisada	1	al menos 2 colores	A PROPONER
4	OVI (Optical Variable Ink)	1		OBLIGATORIO
5	Foto fantasma	1		OBLIGATORIO

6	Marca de agua	1		OBLIGATORIO
7	Lámina plástica de protección de datos	1		OBLIGATORIO
8	Calcografías (tipos y/o imágenes visibles al inclinar)	1		OBLIGATORIO
9	Guilloches patrones modulares	1		OBLIGATORIO
10	Impresión en escalerilla (visible)	1		OBLIGATORIO
17	Impresión UV en laminado	1		A PROPONER
11	Impresión en iris	2		A PROPONER
12	Hilo de seguridad de ventana con microtexto inserto en el papel	2		A PROPONER
13	Hilo costura de seguridad triple y/o fluorescente o ultravioleta	2	al menos 2 colores	OBLIGATORIO
14	Tinta variable térmica	2		A PROPONER
15	Patrones anticopia	2	Debe incluir motivo especial	A PROPONER
16	Fibrillas de seguridad coloreadas	2	al menos 2 colores 130 fibrillas por dcm2	A PROPONER
17	Micro texto	2		A PROPONER
19	Fibrillas fluorescentes (invisibles, UV)	2		OBLIGATORIO
20	Impresión en escalerilla (invisible, UV)	2		OBLIGATORIO
21	Hologramas (3D, cinemáticos)	3		OBLIGATORIO
22	Impresión en nano texto	3		A PROPONER
23	Kinegrama con nano texto	3		A PROPONER
24	Micro elementos con etiquetas en OVI	3		OBLIGATORIO
25	Error deliberado	3	SECRETA	OBLIGATORIO
26	Imagen secreta únicamente visible bajo Rayos X dibujada en el Inlay electrónico sin contacto conforme al diseño actual aprobado por la Superintendencia Nacional de Migraciones y la Unión Europea para el pasaporte electrónico peruano.	3		OBLIGATORIO

Informe de Permanencia de las Medidas de Seguridad

En atención a que los documentos deben conservar sus características de alta seguridad durante toda la vigencia del Contrato, como parte de los servicios contratados, el PROVEEDOR deberá presentar un informe

anual, dentro de los primeros diez (10) días hábiles del mes correspondiente, que presente un análisis global de las características de seguridad propuestas para cada documento y de su permanencia en el tiempo.

Personalización de la Hoja de Datos

El proceso de impresión debe ser por inyección de tinta. La impresión de la tinta debe llegar hasta el sustrato (papel) de modo que si en algún momento la lámina llegara a desprenderse, debe quedar una huella o manifestación de los intentos de adulteración.

La impresión debe ser a color con una resolución mínima de 600 dpi.

El sistema de impresión no deberá imprimir si detecta niveles bajos de tinta.

El proceso de laminación debe emplear una laminación segura mediante una película de laminado holográfico en la Hoja de Datos para proteger los datos personalizados.

La adhesión del laminado debe realizarse de una manera que permita su adhesión permanente, puede ser por efecto térmico o presión. El sistema de personalización debe controlar de manera automática la correcta adhesión del laminado, controlando las condiciones adecuadas de temperatura o de presión según corresponda. La adhesión no debe afectar la resolución de la impresión y la legibilidad de la imagen y los datos biográficos del pasaporte. Puesto que el control debe ser automático, cualquier caso de posterior pérdida de adherencia o pérdida de legibilidad o resolución significativa de la impresión que pueda afectar a la legibilidad de la imagen será comunicado al proveedor, el cual deberá cambiar el equipo y asumir los costos de entrega del pasaporte a los ciudadanos afectados.

PROCESO DE EMISIÓN DEL PASAPORTE ELECTRÓNICO

El proveedor deberá implementar un sistema integrado de software y hardware que se encargue de la ejecución automatizada de cada etapa del proceso de emisión del pasaporte electrónico.

El sistema deberá estar compuesto por:

- Aplicación central de procesamiento y firma digital
- Sistema de personalización y emisión (administrado por el proveedor)
- Sistema de captura de datos y de entrega
- Firma digital y PKI
- Sistema de gestión de insumos e inventario
- Sistema de Firma Desatendida
- Sistema de Información y Generación de Reportes
- Sistema de Seguridad y Auditoría
- Módulo de control de registros de auditoría y trazabilidad.
- Módulo de administración de usuarios (operadores)
- Módulo de Gestión de Roles
- Módulo de Gestión de Control de Acceso

Este sistema deberá ser integrado por el proveedor con el Sistema de Actividades Migratorias del MRE (SAM) y la respectiva base de datos del Ministerio de Relaciones Exteriores, lo que implica la implementación de mecanismos que permitan dicha integración conforme a las necesidades de la solución y a la aprobación por

parte del MRE, teniendo en consideración que el proceso de expedición de pasaportes se encuentra directamente relacionado con otros procesos operativos del MRE.

Además, el sistema deberá realizar consultas al sistema de verificación MIGRACIONES, estar preparado para permitir la consulta a la base de datos del RENIEC, considerando mecanismos de contingencia para evitar la dependencia con estos procesos de consulta, en caso de que estas no estén disponibles. Por otro lado, también deberá contemplar la posibilidad de unir al proceso de consulta a otras entidades. Este tipo de consultas actualmente se realiza mediante las siguientes tecnologías de intercambio de mensajes: socket TCP/IP y Web Service, sin embargo, el proveedor podrá implementar otros mecanismos de consulta en coordinación con dichas entidades; se deben considerar al menos 05 interfaces adicionales para desarrollar futuras conexiones.

En el caso de las Oficinas Consulares, todas las solicitudes de pasaportes deben ser autorizadas además por la autorización electrónica del Cónsul.

En el caso de la sede de expedición en el MRE, todas las solicitudes de pasaportes deben ser autorizadas además por la autorización electrónica de la Dirección de Privilegios.

El sistema deberá brindar todas las funcionalidades que permitan la ejecución automática de las actividades que se describen a continuación:

Emisión de pasaporte de personas mayores de edad por primera vez:

a) El Operador verifica la identidad del ciudadano ingresando su número de DNI o haciendo lectura del mismo mediante un lector OCR de documentos y solicita al ciudadano la lectura de su huella dactilar para ser capturada en formato de compresión WSQ.
b) El módulo enviara la información obtenida en el punto anterior de manera automática a la Base de Datos AFIS del MRE que contiene los datos de emisión del pasaporte electrónico, la misma que validara la existencia de la imagen dactilar en relación de 1:N. La habilitación de esta funcionalidad debe ser configurable por los administradores en el centro de procesamiento. De ser positivo el resultado de esta verificación, es decir, de tratarse de una persona identificada como extranjera, o con un pasaporte con otra identidad, el sistema deberá mostrar en pantalla de una manera claramente visible, el mensaje correspondiente y no permitir la emisión del pasaporte. No obstante, se debe considerar los casos en los que el titular posee una doble nacionalidad legal.
c) Asimismo, el módulo enviara la información obtenida en el punto anterior de manera automática a la Base de Datos AFIS de MIGRACIONES que contiene los datos de emisión del pasaporte electrónico, la misma que validara la existencia de la imagen dactilar en relación de 1:N. La habilitación de esta funcionalidad debe ser configurable por los administradores en el centro de procesamiento. De ser positivo el resultado de esta verificación, es decir, de tratarse de una persona identificada como extranjera, o con un pasaporte con otra identidad, el sistema deberá mostrar en pantalla de una manera claramente visible, el mensaje correspondiente y no permitir la emisión del pasaporte. No obstante, se debe considerar los casos en los que el titular posee una doble nacionalidad legal.
d) En caso de ser negativo el resultado anterior o de estar inhabilitada dicha funcionalidad, el módulo permitirá la CONSULTA de manera manual o automática al RENIEC para ser validados en la base de datos de ciudadanos peruanos (dentro del periodo del contrato, cuando el MRE realice el convenio con RENIEC, se deberá realizar la integración para hacer la consulta automática). En el caso que la verificación de la

identidad del ciudadano no sea positiva, se deberá mostrar un mensaje de advertencia y no permitir la emisión del pasaporte.

e) Para aquellos solicitantes que se identifiquen mediante un pasaporte emitido por la Superintendencia Nacional de Migraciones se deberá realizar la lectura del pasaporte electrónico. Y se deberá realizar consulta a la base de datos del Sistema de Actividades Migratorias del MRE. En caso de existir otros pasaportes habilitados en el Sistema de Actividades Migratorias del MRE y/o el nuevo Sistema de Pasaportes Electrónicos a implementar, vinculados a la identidad verificada del solicitante se debe proceder a anular o inhabilitar en la base de datos estos pasaportes, para así poder proceder a emitir un nuevo pasaporte. Se deberá comunicar la emisión del nuevo pasaporte a Migraciones.

f) Los datos del ciudadano deberán ser tomados de la lectura OCR del DNI, los demás datos deberán poder ser llenados manualmente para consolidar los datos a ser impresos en la hoja de datos del pasaporte y los datos a ser gravados en el chip. El administrador del sistema no debe tener acceso a la modificación de esta información. La imagen de la rúbrica debe ser tomada de la lectura del pad de firma.

g) Los datos referidos a la "Profesión", "Estatura", "color de ojos", "color de cabello", "Teléfono móvil" serán ingresados por el Operador de manera manual.

h) El encargado realizará la captura de la imagen del rostro, las diez huellas dactilares de las manos (correspondientes a los dedos diferentes que posea) del ciudadano.

i) La información consolidada será enviada a la base de datos del MRE para su registro.

j) La aplicación formará el hash de los datos para la formación del objeto de seguridad y serán enviados por un canal telemático seguro cifrado al Centro de procesamiento para la generación de la firma digital correspondiente. El objeto de seguridad será enviado a la Sede de expedición para la personalización del chip, a través de un canal seguro definido, implementado y sugerido por el proveedor de acuerdo a estándares.

k) La aplicación generará un registro de la solicitud, con los datos biográficos y la verificación exitosa de la identidad y deberá solicitar al Operador su firma digital para la protección del registro, y la firma electrónica biométrica del titular, asimismo realizará la firma automatizada a nombre del Ministerio de Relaciones Exteriores.

l) La hoja de datos del pasaporte y el chip son personalizados por el Nuevo Sistema de Pasaporte Electrónico.

m) Previa a la entrega, el Operador encargado, realiza la verificación del control de calidad del documento, y verifica la vinculación del documento con el solicitante ingresando la lectura de su huella dactilar para ser contrastada por el sistema mediante una verificación AFIS 1:1, asimismo, el sistema deberá verificar la autenticidad de la firma digital utilizando la clave pública del certificado del Firmante de Documentos y del certificado de Firma País.

n) El sistema genera un registro de la entrega del documento mediante el resultado exitoso de la verificación AFIS 1:1, y solicita al Operador su firma digital, asimismo el sistema registra la fecha y hora (del servidor central) y realiza la firma digital automatizada del registro completo.

o) Se activa automáticamente el pasaporte electrónico habilitándolo en la base de datos del MRE para ser utilizado por el ciudadano solicitante.

p) Los insumos y documentos pre-personalizados utilizados, son registrados automáticamente en el sistema de software de control de inventario.

Emisión del pasaporte de personas mayores de edad por segunda vez o más:

a) El ciudadano deberá presentarse con su pasaporte electrónico para solicitar un nuevo pasaporte.
b) El Operador solicita al ciudadano la lectura de su huella dactilar para ser verificada contra su Pasaporte Electrónico, en una verificación 1:1. Asimismo, se verifica la autenticidad del Pasaporte, a través de la verificación de la firma digital y se contrastará con la base de datos para verificar que no se trata de un pasaporte perdido, anulado o inhabilitado. Para aquellos solicitantes que se identifiquen mediante un pasaporte emitido por la Superintendencia Nacional de Migraciones se deberá realizar la lectura del pasaporte electrónico. Y se deberá realizar consulta a la base de datos del Sistema de Actividades Migratorias del MRE. En caso de existir otros pasaportes habilitados en el Sistema de Actividades Migratorias del MRE y/o el nuevo Sistema de Pasaportes Electrónicos a implementar, vinculados a la identidad verificada del solicitante se debe proceder a anular o inhabilitar en la base de datos estos pasaportes, para así poder proceder a emitir un nuevo pasaporte. Se deberá comunicar la emisión del nuevo pasaporte a Migraciones.

c) Los datos del ciudadano incluyendo la imagen de la rúbrica y las huellas registradas deberán ser tomados por la aplicación desde la base de datos del Nuevo Sistema de Pasaporte Electrónico para consolidar los datos a ser impresos en la hoja de datos del pasaporte y los datos a ser gravados en el chip. El administrador u operador del sistema no deben tener acceso a la modificación de esta información.
d) Los datos referidos a la "Profesión", "Estatura", "color de ojos", "color de cabello", "Teléfono móvil" serán ingresados por el Operador de manera manual.
e) El encargado realizará la captura de la imagen del rostro y capturará una huella dactilar de verificación del ciudadano.
f) Las imágenes capturadas serán enviadas a la base de datos del Nuevo SISTEMA DE EMISIÓN DE PASAPORTE ELECTRÓNICOS para su registro.
g) La aplicación formará el hash de los datos para la formación del objeto de seguridad y serán enviados por un canal telemático seguro cifrado definido, implementado y sugerido por el proveedor de acuerdo a estándares al Centro de procesamiento para la generación de la firma digital correspondiente. El objeto de seguridad será enviado a la Sede de expedición para la personalización del chip, a través de un canal seguro definido, implementado y sugerido por el proveedor de acuerdo a estándares.
h) La aplicación generará un registro de la solicitud, con los datos biográficos y la verificación exitosa de la identidad y deberá solicitar al Operador su firma digital para la protección del registro.
i) La hoja de datos del pasaporte y el chip son personalizados por el Nuevo Sistema de Pasaporte Electrónico.
j) Previa a la entrega, el Operador encargado, realiza la verificación del control de calidad del documento, y verifica la vinculación del documento con el solicitante ingresando la lectura de su huella dactilar para ser contrastada por el sistema mediante una verificación AFIS 1:1, asimismo, el sistema deberá verificar la autenticidad de la firma digital utilizando la clave pública del certificado del Firmante de Documentos y del certificado de Firma País.
k) El sistema genera un registro de la entrega del documento mediante el resultado exitoso de la verificación AFIS 1:1, y solicita al Operador su firma digital, asimismo el sistema registra la fecha y hora (del servidor central) y realiza la firma digital automatizada del registro completo.
l) Se informa a Migraciones sobre la emisión del pasaporte.

m) Los insumos y libros de pasaportes utilizados son registrados automáticamente en el sistema de software de control de inventario.

Pasaporte de personas menores de edad (Mayor a 12 a menor de 18 años) por primera vez

a) El menor, junto a su padre, madre o apoderado, se acerca al módulo de captura presentando su DNI. El apoderado presenta su DNI (en caso de ser peruano), pasaporte, Carné de Protocolo o Carné de Extranjería, cédula de identidad para los ciudadanos CAN - MERCOSUR, y una copia del mismo (en caso de ser extranjero). En el caso del apoderado, deberá presentar un poder consular legalizado por el Ministerio de Relaciones Exteriores o un documento político apostillado (si fue emitido en el extranjero), notarial o judicial (si fue otorgado en el Perú), el cual será escaneado por el Operador e ingresado en su formato digital al sistema.
b) El padre o apoderado deberá presentar la correspondiente autorización notarial debidamente firmada por ambos padres, o el padre o madre vivo, o el padre reconocido legalmente, o el apoderado según sea el caso, la cual será escaneada por el Operador e ingresado en su formato digital al sistema previa validación visual de la firma del notario con lo que muestra la consulta a la base de datos de RENIEC.
c) Operador designado por la Entidad, verifica la identidad del menor de edad ingresando su número de DNI o haciendo lectura del mismo mediante un lector de documentos y solicita al ciudadano la lectura de su huella dactilar para ser capturada en formato de compresión WSQ
d) El módulo enviara la información obtenida en el literal c) de manera automática a la Base de Datos AFIS del MRE, la misma que validara la existencia de la Imagen dactilar en relación de 1:N. La habilitación de esta funcionalidad debe ser configurable por los administradores en el centro de procesamiento. De ser positivo el resultado de esta verificación, es decir, de tratarse de una persona identificada como extranjera, o ya cuente con un pasaporte con otra identidad, el sistema deberá mostrar en pantalla de una manera claramente visible, el mensaje correspondiente y no permitir la emisión del pasaporte. Considerar los casos en los que el titular posee una doble nacionalidad legal.
e) Asimismo, el módulo enviara la información obtenida en el literal c) de manera automática a la Base de Datos AFIS de Migraciones, la misma que validara la existencia de la imagen dactilar en relación de 1:N. La habilitación de esta funcionalidad debe ser configurable por los administradores en el centro de procesamiento. De ser positivo el resultado de esta verificación, es decir, de tratarse de una persona identificada como extranjera, o ya cuente con un pasaporte con otra identidad, el sistema deberá mostrar en pantalla de una manera claramente visible, el mensaje correspondiente y no permitir la emisión del pasaporte. Considerar los casos en los que el titular posee una doble nacionalidad legal.
f) En caso de ser negativo el resultado anterior o de estar inhabilitada dicha funcionalidad, el módulo permitirá la CONSULTA de manera manual o automática al RENIEC para ser validados en la base de datos de ciudadanos peruanos (dentro del periodo del contrato, cuando el MRE realice el convenio con RENIEC, se deberá realizar la integración para hacer la consulta automática). En el caso que la verificación de la identidad del ciudadano no sea positiva, se deberá mostrar un mensaje de advertencia y no permitir la emisión del pasaporte.
g) De ser positiva la respuesta del RENIEC, respecto de la verificación de la identidad del menor, se identificará en la base de datos del RENIEC la identidad de los padres o apoderados. La respuesta del RENIEC debe contener la identidad de los padres del menor (padre o madre vivo, o padre o madre reconocido legalmente), incluyendo la imagen de sus rostros. El padre o apoderado solicitante realizará la validación de su identidad mediante consulta a la base de datos del RENIEC, o la base de

datos del Sistema de Actividades Migratorias del MRE y se capturarán sus datos para ser incluidos en la personalización del pasaporte. En el caso que la verificación de la identidad del menor, o el padre o el apoderado no sea positiva, se deberá mostrar un mensaje de advertencia de no continuidad de trámite.

h) Para aquellos solicitantes que se identifiquen mediante un pasaporte emitido por la Superintendencia Nacional de Migraciones se deberá realizar la consulta con el Migraciones.

i) Para identificar los casos de menores solicitantes que ya hayan recibido pasaportes con anterioridad, la imagen de la huella debe ser leída y procesada en la Base de Datos del SISTEMA DE EMISIÓN DE PASAPORTE ELECTRÓNICOS, para ubicar todos los registros anteriores vinculados a dicha huella. Si los registros anteriores corresponden a la misma identidad que la persona ha presentado, se debe proseguir con el trámite, de otro modo la aplicación debe enviar un mensaje de advertencia. En caso de existir otros pasaportes habilitados vinculados a la identidad verificada del solicitante se debe proceder a anular e inhabilitar en la base de datos estos pasaportes, para así poder proceder a emitir un nuevo pasaporte.

j) Los datos del menor deberán ser llenados manualmente y contrastados con los datos emitidos por el RENIEC para consolidar los datos a ser impresos en la hoja de datos del pasaporte y los datos a ser gravados en el chip. El administrador del sistema no debe tener acceso a la modificación de esta información.

k) Los datos referidos a la "Estatura", "color de ojos", "color de cabello", "ocupación" y "teléfono móvil" serán ingresados por el Operador de manera manual.

l) El encargado realizará la captura de la imagen del rostro, las diez huellas dactilares de las manos (correspondientes a los dedos diferentes que posea) del menor.

m) La información consolidada será enviada a la base de datos del MRE para su registro.

n) La aplicación formará el hash de los datos para la formación del objeto de seguridad y serán enviados por un canal telemático seguro al Centro de procesamiento para la generación de la firma digital correspondiente. El objeto de seguridad será enviado a la Sede de expedición para la personalización del chip, a través de un canal seguro.

o) La aplicación generará un registro de la solicitud, con los datos biográficos y la verificación exitosa de la identidad y deberá solicitar al Operador su firma digital para la protección del registro, y la firma electrónica con la minucia del apoderado, asimismo realizará la firma automatizada a nombre del Ministerio de Relaciones Exteriores.

p) La hoja de datos del pasaporte y el chip son personalizados por el Nuevo SISTEMA DE EMISIÓN DE PASAPORTE ELECTRÓNICOS.

q) El Operador encargado de la entrega, realiza la verificación del control de calidad del documento, y verifica la vinculación del documento con el solicitante ingresando la lectura de su huella dactilar para ser contrastada por el sistema mediante una verificación AFIS 1:1, asimismo, el sistema deberá verificar la autenticidad de la firma digital utilizando la clave pública del certificado del Firmante de Documentos y del certificado de Firma País.

r) El sistema genera un registro de la entrega del documento mediante el resultado exitoso de la verificación AFIS 1:1, y solicita al Operador su firma digital, y la firma electrónica con la minucia del solicitante, asimismo el sistema registra la fecha y hora (del servidor central) y realiza la firma digital automatizada del registro completo.

s) Se informa a Migraciones sobre la emisión del pasaporte.

t) Los insumos y los libros de pasaportes utilizados son registrados automáticamente en el sistema de software de control de inventario.

Emisión de pasaporte de personas menores de edad (Mayor a 12 a menor de 18 años) por segunda vez o más:

a) El menor, junto a su padre, madre o apoderado, se acerca al módulo de captura presentando su pasaporte electrónico. El apoderado presenta su DNI (en caso de ser peruano), pasaporte, Carné de Protocolo o Carné de Extranjería, cédula de identidad, poder consular o documento político apostillado y una copia del mismo (en caso de ser extranjero). En el caso del apoderado, deberá presentar un poder consular legalizado por el Ministerio de Relaciones Exteriores (si fue emitido en el extranjero), notarial o judicial (si fue otorgado en el Perú), el cual será escaneado por el Operador e ingresado en su formato digital al sistema.
b) El padre o apoderado deberá presentar la correspondiente autorización notarial debidamente firmada por ambos padres o el apoderado según sea el caso, la cual será escaneada por el Operador e ingresado en su formato digital al sistema.
c) El Operador solicita al menor la lectura de su huella dactilar para ser verificada contra su Pasaporte Electrónico ya sea emitido por el MRE o por Migraciones, en una verificación 1:1. Asimismo, se verifica la autenticidad del Pasaporte a través de la verificación de la firma digital y se contrastará con la base de datos para verificar que no se trata de un pasaporte perdido o inhabilitado.
d) El padre o apoderado solicitante realizará la validación de su identidad mediante su huella dactilar y la base de datos del RENIEC, o la base de Carné de Extranjería o de Control Migratorio (en caso de ser extranjero) En el caso que la verificación de la identidad del menor, o el padre o el apoderado no sea positiva, se deberá mostrar un mensaje de advertencia.
e) De ser positiva la respuesta del RENIEC, respecto de la verificación de la identidad del menor y el padre o apoderado. Para aquellos solicitantes que se identifiquen mediante un pasaporte consular se deberá realizar la consulta con el Ministerio de Relaciones Exteriores.
f) Los datos del menor incluyendo la imagen de la rúbrica según corresponda, deberán ser tomados de desde la base de datos de pasaportes emitidos para consolidar los datos a ser impresos en la hoja de datos del pasaporte y los datos a ser gravados en el chip. El administrador u operador del sistema no deben tener acceso a la modificación de esta información.
g) Los datos referidos a la "Estatura", "color de ojos", "color de cabello", "ocupación", "teléfono móvil", serán ingresados por el Operador de manera manual.
h) El encargado realizará la captura de la imagen del rostro y capturará una huella dactilar de verificación del menor de edad.
i) Las imágenes capturadas serán enviadas a la base de datos de pasaportes emitidos de El MRE para su registro.
j) La aplicación formará el hash de los datos para la formación del objeto de seguridad y serán enviados por un canal telemático seguro cifrado al Centro de procesamiento para la generación de la firma digital correspondiente. El objeto de seguridad será enviado a la Sede de expedición para la personalización del chip, a través de un canal seguro.
k) La aplicación generará un registro de la solicitud, Formulario F-001 en su versión digital, con los datos biográficos y la verificación exitosa de la identidad y deberá solicitar al Operador su firma digital para la protección del registro, y la firma electrónica con la minucia del apoderado, asimismo realizará la firma automatizada a nombre del Ministerio de Relaciones Exteriores.
l) La hoja de datos y el chip son personalizados.
m) El Operador encargado de la entrega, realiza la verificación del control de calidad del documento, y verifica la vinculación del documento con el menor ingresando la lectura de su huella dactilar para ser

contrastada por el sistema mediante una verificación AFIS 1:1, asimismo, el sistema deberá verificar la autenticidad de la firma digital utilizando la clave pública del certificado del Firmante de Documentos y del certificado de Firma País.

n) El sistema genera un registro de la entrega del documento mediante el resultado exitoso de la verificación AFIS 1:1, y solicita al Operador su firma digital, asimismo el sistema registra la fecha y hora (del servidor central) y realiza la firma digital automatizada del registro completo.

o) Se informa a Migraciones sobre la emisión del pasaporte.

p) Los insumos y los libros de pasaportes utilizados son registrados automáticamente en el sistema de software de control de inventario.

Pasaporte de personas menores de edad (de 0 a 12 años)

a) El menor, junto a su padre, madre o apoderado, se acerca al módulo de captura presentando su DNI. El apoderado presenta su DNI (en caso de ser peruano), pasaporte, Carné de Protocolo o Carné de Extranjería, cédula de identidad para los ciudadanos CAN - MERCOSUR, y una copia del mismo (en caso de ser extranjero). En el caso del apoderado, deberá presentar un poder consular legalizado por el Ministerio de Relaciones Exteriores o un documento político apostillado (si fue emitido en el extranjero), notarial o judicial (si fue otorgado en el Perú), el cual será escaneado por el Operador e ingresado en su formato digital al sistema.

b) El padre o apoderado deberá presentar la correspondiente autorización notarial debidamente firmada por ambos padres, o el padre o madre vivo, o el padre reconocido legalmente, o el apoderado según sea el caso, la cual será escaneada por el Operador e ingresado en su formato digital al sistema previa validación visual de la firma del notario con lo que muestra la consulta a la base de datos de RENIEC.

c) El Operador verifica la identidad del menor ingresando su número de DNI, y solicita al padre o apoderado la lectura de su huella dactilar para ser capturada en formato de compresión WSQ.

d) El módulo enviará la información obtenida en el literal c) de manera automática a la Base de Datos AFIS del MRE y de MIGRACIONES, la misma que validará la existencia de la imagen dactilar en relación de 1:*N*. La habilitación de esta funcionalidad debe ser configurable por los administradores en el centro de procesamiento. De ser positivo el resultado de esta verificación, es decir, de tratarse de una persona identificada como extranjera o una persona distinta, el sistema deberá mostrar en pantalla de una manera claramente visible, el mensaje correspondiente y no permitir la emisión del pasaporte. Considerar los casos en los que el titular posee una doble nacionalidad legal.

e) En caso de ser negativo el resultado del párrafo anterior o de estar inhabilitada dicha funcionalidad, el módulo debe capturar la imagen de la huella y permitir el ingreso del número de DNI del apoderado, y enviarlos de manera automática para ser validados en la base de datos del RENIEC, mediante una verificación 1:1. En caso de tratarse de un extranjero sin huellas registradas en el AFIS a ser implementado, su identidad deberá ser verificada mediante la consulta a la base de datos del Sistema Integrado de El MRE (Carné de Extranjería y Control Migratorio) utilizando el número de pasaporte o carné de extranjería según corresponda. De ser positiva la respuesta, respecto de la verificación de la identidad del apoderado, la identidad del menor se verificará en la base de datos del RENIEC. La respuesta del RENIEC debe contener la identidad de los padres del menor, incluyendo la imagen de sus rostros (en caso de que ambos o alguno sea peruano). Los datos del padre, madre o apoderado extranjero deberán ser tomados automáticamente de la base de datos del Sistema Integrado de El

MRE (Carné de Extranjería o de Control Migratorio). En el caso que la verificación de la identidad del menor, o el padre o el apoderado no sea positiva, se deberá mostrar un mensaje de advertencia.

f) Para aquellos solicitantes que se identifiquen mediante un pasaporte emitido por MIGRACIONES se deberá realizar la consulta con MIGRACIONES.

g) El pasaporte de menores de 12 años, debe tener una vigencia de 3 años, por tanto cada tres años deberá solicitar un nuevo pasaporte.

h) Los datos del menor deberán ser tomados por el operador desde la respuesta del RENIEC para consolidar los datos a ser impresos en la hoja de datos del pasaporte y los datos a ser grabados en el chip. El administrador u operador del sistema no deben tener acceso a la modificación de esta información.

i) Los datos referidos a la "Estatura", "color de ojos", "color de cabello", "ocupación", "Teléfono móvil del padre o apoderado" serán ingresados por el Operador de manera manual.

j) El encargado realizará la captura de la imagen del rostro. No se tomarán huellas a los menores de 8 años.

k) La información consolidada (datos + imágenes capturadas) serán enviados a la base de datos del Nuevo Sistema de Pasaporte Electrónico para su registro.

l) La aplicación formará el hash de los datos para la formación del objeto de seguridad y serán enviados por un canal telemático seguro al Centro de procesamiento para la generación de la firma digital correspondiente. El objeto de seguridad será enviado a la Sede de expedición para la personalización del chip, a través de un canal seguro.

m) La aplicación generará un registro de la solicitud, con los datos biográficos y la verificación exitosa de la identidad y deberá solicitar al Operador su firma digital para la protección del registro y la firma electrónica con la minucia del solicitante, de contar con un certificado digital o su DNI emitido por el RENIEC el ciudadano podrá usarlo y firmar digitalmente, asimismo realizará la firma automatizada a nombre del Ministerio de Relaciones Exteriores.

n) La hoja de datos del pasaporte y el chip son personalizados por el Nuevo Sistema de Pasaporte Electrónico.

o) El Operador encargado de la entrega, realiza la verificación del control de calidad del documento, y verifica la vinculación del documento con el solicitante verificando la imagen de su rostro, asimismo, el sistema deberá verificar la autenticidad de la firma digital utilizando la clave pública del certificado del Firmante de Documentos y del certificado de Firma País.

p) El sistema genera un registro de la entrega del documento mediante el resultado exitoso de la verificación AFIS 1:1, y solicita al Operador su firma digital, la firma electrónica con la minucia del solicitante, asimismo el sistema registra la fecha y hora (del servidor central) y realiza la firma digital automatizada del registro completo.

q) Se informa a Migraciones sobre la emisión del pasaporte.

r) Los insumos y libros de pasaportes utilizados son registrados automáticamente en el sistema de software de control de inventario.

DOCUMENTACIÓN DEL PROCEDIMIENTO

El PROVEEDOR deberá presentar un documento, con todo el detalle del flujo del proceso de emisión del pasaporte electrónico, el cual deberá ser aprobado por el MRE para que el PROVEEDOR efectúe el desarrollo

de las aplicaciones, debiendo utilizar notación estándar tipo BPM, describiendo las actividades, los actores, sistema y operadores que participan en cada etapa, conforme al proceso descrito precedentemente:

- Verificación de identidad del solicitante
- Captura de datos
- Personalización
- Control de calidad
- Emisión
- Anulación o inhabilitación
- Entrega y verificación de autenticidad del pasaporte
- Control de insumos e inventario

Estos procedimientos deberán ser explicados al personal del Ministerio de Relaciones Exteriores como parte del entrenamiento y transferencia de conocimientos del servicio a implementar. La aplicación central deberá ser configurada de tal modo que permita el funcionamiento del procedimiento.

Las etapas del procedimiento deben cumplir con todos los controles técnicos y de gestión descritos en el presente documento.

CARACTERÍSTICAS DEL PASAPORTE ELECTRÓNICO

El pasaporte electrónico deberá cumplir las especificaciones técnicas para los pasaportes de lectura mecánica, definidas y especificadas en el Documento 9303 de OACI, Parte 1 Volúmenes 1 y 2 en lo que corresponda, especificaciones necesarias para lograr la interfuncionalidad mundial.

El pasaporte electrónico deberá ser producido en formatos de cuadernillos o libretas de treinta y dos (32) páginas. El pasaporte electrónico podrá personalizarse en la primera hoja interior del cuadernillo, de acuerdo con las características técnicas y medidas de seguridad especificadas por el PROVEEDOR.

El chip sin contacto y su antena podrán estar ubicados indistintamente en la tapa o contratapa.

El chip del pasaporte electrónico deberá tener una capacidad de almacenamiento de a lo menos 64 KB y una tasa de transferencia de a lo menos 424 Kbps y compatible con 848 Kbps.

El CHIP y el material de la cubierta deberán soportar las temperaturas en el módulo de laminado del equipo de personalización, aunque estas sean superiores a 50ºC.

El pasaporte electrónico deberá contar con al menos las siguientes funcionalidades de autenticación:

a) Autenticación pasiva de la Estructura Lógica de Datos (LDS) encriptada con datos presentes en el OCR-B y firmada digitalmente por el emisor
b) Control de Acceso Suplementario (SAC) mediante comunicación segura
c) Autenticación activa para comprobar que el pasaporte no ha sido copiado y contiene el chip correcto y para comprobar que el chip no ha sido cambiado
d) Control de Acceso Extendido (EAC) mediante comunicación segura y almacenamiento en el chip de los datos biométricos del titular del documento.

Inlay con un chip sin contacto sin conexión con la antena para mejorar la durabilidad del pasaporte. El inlay tendrá una imagen visible con Rayos-X, para mejorar el nivel de seguridad del pasaporte. Esta imagen será la misma que el inlay del pasaporte de Migraciones.

Especificaciones del Inlay:
Espesor máximo del Inlay : 450µm
Espesor mínimo: 300 µm
Especificaciones de la antena: La antena deberá tener un tamaño máximo externo de ID1 (como se describe en la norma ISO 7810). La antena será de aluminio grabado con imagen específica visible bajo rayos X.
La imagen aprobada por la Unión Europea para el pasaporte electrónico peruano se entrega al adjudicado.

Especificaciones del módulo de protección del chip:
Para obtener la máxima fiabilidad del pasaporte, el chip deberá de ser empaquetado en un módulo con protección de la encapsulación.
La metalización de la cinta del módulo debe de ser de Níquel + Oro con fin de evitar cualquier problema de corrosión.

ESPECIFICACIONES TÉCNICAS DE LOS PASAPORTES ELECTRÓNICOS DIPLOMÁTICOS

De la carátula:

- Deberá ser de Tela plastificada tipo hilo, color azul, con impresiones en color dorado (Pan de Oro Industrial) que se fijará en la portada mediante calor y presión con las siguientes leyendas:
- En la parte superior se consignará la palabra "REPÚBLICA DEL PERÚ", centrado y con letras de 5 mm. de alto y a 1.9 cm. del borde superior.
- El "ESCUDO DE ARMAS DEL PERÚ" circunscrito en un diámetro de 3.5 cm. y centrado a 4.5 cm. del borde superior.
- La palabra "PASAPORTE DIPLOMATICO", centrada y con letras de 4 mm. de alto a 10 cm. del borde superior.
- El material con que esté elaborada la cubierta deberá resistir las temperaturas de laminación (hasta 200º C), la manipulación y el deterioro por su uso, para que el pasaporte pueda ser utilizado con una humedad relativa ambiente del 5% al 95%, a una temperatura máxima de bulbo húmedo de 25º C y poder quedar almacenado a una humedad relativa ambiente del 0% al 100%, de acuerdo a la normativa de la Comunidad Andina de Naciones Decisión 525, Anexo I del inciso 1.5.
- En la parte inferior deberá consignarse el símbolo del pasaporte electrónico, conforme a las dimensiones y ubicación recomendada por el Documento 9303 de OACI.

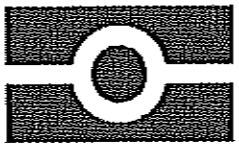
De las páginas interiores:

Tendrán que ser idénticas a las del pasaporte ordinario, en medidas de seguridad, diseño, marca de agua, impresiones de seguridad.

ESPECIFICACIONES TÉCNICAS DE LOS PASAPORTES ELECTRÓNICOS ESPECIALES

De la carátula:

- Deberá ser de tela plastificada tipo hilo, color verde, con impresiones en color dorado (Pan de Oro Industrial) que se fijará en la portada mediante calor y presión con las siguientes leyendas:
- En la parte superior se consignará la palabra "REPÚBLICA DEL PERÚ", centrado y con letras de 5 mm. de alto y a 1.9 cm. del borde superior.
- El "ESCUDO DE ARMAS DEL PERÚ" circunscrito en un diámetro de 3.5 cm. y centrado a 4.5 cm. del borde superior.
- La palabra "PASAPORTE ESPECIAL", centrada y con letras de 4 mm. de alto a 10 cm. del borde superior.
- El material con que esté elaborada la cubierta deberá resistir las temperaturas de laminación (hasta 200º C), la manipulación y el deterioro por su uso, para que el pasaporte pueda ser utilizado con una humedad relativa ambiente del 5% al 95%, a una temperatura máxima de bulbo húmedo de 25º C y poder quedar almacenado a una humedad relativa ambiente del 0% al 100%, de acuerdo a la normativa de la Comunidad Andina de Naciones Decisión 525, Anexo I del inciso 1.5.
- En la parte inferior deberá consignarse el símbolo del pasaporte electrónico, conforme a las dimensiones y ubicación recomendada por el Documento 9303 de OACI.



- De la contra carátula

El diseño de la contra carátula será propuesto por el PROVEEDOR y aprobado por el MRE.

INFRAESTRUCTURA CRIPTOGRÁFICA

Las gestiones para la generación de los certificados y la ejecución de los procedimientos de generación de las claves serán realizadas y gestionadas por el PROVEEDOR.

La PKI será implementada conforme a Politicas de Certificacion provistas por el PROVEEDOR, y que deberán cumplir con los requisitos estipulados en el Documento 9303 de la OACI.

APLICACIONES DE ESCRITORIO

El PROVEEDOR deberá proveer una suite de aplicaciones para procesamiento de texto, hojas de cálculo, presentaciones, dibujos y diagramas, dando cumplimiento a los estándares definidos en la sección Formato de Documentos de Productividad Personal.

Estas aplicaciones deberán estar debidamente licenciadas, actualizadas y disponibles en todas las estaciones de trabajo del SISTEMA DE IDENTIFICACIÓN.

DOCUMENTACIÓN

El PROVEEDOR deberá entregar y mantener la documentación del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

Para cualquier desarrollo a medida que sea necesario, el PROVEEDOR deberá indicar la metodología que utilizará y construir la documentación completa, incluyendo el manual de usuario y procesos de negocio de los sistemas de información.

Para la mantención de la documentación el PROVEEDOR deberá utilizar metodologías y herramientas que faciliten su efectiva actualización. Asimismo, el PROVEEDOR deberá mantener la documentación de los procedimientos operativos necesarios en casos de contingencia, tales como: mantenimiento o fallas en el suministro de energía eléctrica, y fallas en la plataforma tecnológica central y cualquier otra circunstancia excepcional que pudiera afectar el normal funcionamiento del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.

Toda la documentación deberá estar disponible en un repositorio electrónico del SISTEMA DE EMISIÓN DE PASAPORTES y ajustarse a los estándares definidos en la sección "ESTÁNDARES, CERTIFICACIONES Y BUENAS PRÁCTICAS"

CAPACITACIÓN

El PROVEEDOR deberá presentar y mantener un plan de capacitación para todo el personal involucrado en los procesos del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES, cuyo plan será aprobado por el Ministerio de Relaciones Exteriores.

Esta capacitación se realizará conforme al cuadro siguiente y el calendario de ejecución deberá estar en concordancia con las etapas del proyecto especificadas en la sección "ETAPA DE IMPLEMENTACIÓN".

El proveedor deberá considerar la preparación de videos tutoriales para las capacitaciones dirigidas a las Oficinas Consulares.

El PROVEEDOR deberá encargarse directamente de capacitar a la totalidad del personal de el Ministerio de Relaciones Exteriores que utiliza el Sistema Central de Identificación incluyendo al personal dedicado a la atención de usuarios en las distintas Sedes del MRE. Las capacitaciones deberán ser realizadas por especialistas con experiencia acreditada en cada tema por los fabricantes de las soluciones a implementar. Se deberan otorgar certificados provistos por los fabricantes de las tecnologias a entregar, de acuerdo al cuadro siguiente:

ENTRENAMIENTO DEL PERSONAL ENCARGADO DE LA ADMINISTRACIÓN Y SOPORTE DE LA APLICACIÓN CENTRAL DE PROCESAMIENTO Y FIRMA DIGITAL

CURSO	N° HORAS	PERSONAS	LUGAR
Operación de Estaciones de Atención de Público	6	250	internacional
Operación general de los Centros de Personalización	8	12	Lima

CURSO	N° HORAS	PERSONAS	LUGAR
Supervisores (control del centro de monitoreo y revisión de informes de avance y de cumplimiento de niveles de servicio)	8	10	Lima
Curso de laboratorio forense para peritaje de documentos de viaje	15	20	Lima
Administrador de Sistema AFIS	8	12	Lima
Administración del Sistema de PKI (ceremonias de claves y componentes)	8	12	Lima
Administración del Módulo y Hardware de Seguridad (seguridad del ciclo de vida y descripción general de funcionamiento)	8	12	Lima
Usuarios del Sistema de Mesa de Ayuda	12	8	Lima
Curso de administradores del Sistema de Control de Producción y control de Stock, con certificado a nombre del proveedor	12	20	Lima

Los cursos deberán ser realizados por instructores certificados con experiencia internacional. Se deberán emitir certificados por los cursos realizados a nombre de la empresa fabricante o el PROVEEDOR.

La modalidad de los cursos que se realizarán en Lima deberá ser presencial

PLAN DEL PROYECTO

El Plan del Proyecto del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES considerará dos grandes etapas:

a) **Etapa de Implementación**, que comienza al día siguiente de la suscripción del Contrato y culmina con el fin de la implementación de todas las Oficinas Consulares y en Lima del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.
b) **Etapa de Explotación,** que comienza al día siguiente de la conformidad de las pruebas de recepción definitiva en las 111 Oficinas Consulares del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES y culmina al terminar el servicio (36 meses).

Junto con el Plan del Proyecto el PROVEEDOR debe especificar la Metodología que utilizará para la gestión del proyecto y asegurar el cumplimiento de los hitos, considerando para ello el funcionamiento permanente de una Oficina Técnica del Proyecto (PMO),

El PROVEEDOR debe entregar un Plan de Trabajo Detallado del Proyecto para el desarrollo de la etapa de implementación y el cumplimiento de los hitos planteados para la implementación y podrá establecer los hitos adicionales si así lo estima conveniente. Este plan debe señalar claramente las fechas en que se cumplirán, a lo menos, las etapas y todos los hitos considerados en su Plan de Proyecto.

El PROVEEDOR deberá entregar mensualmente, durante los primeros diez (10) días hábiles del mes correspondiente, un Informe de Avance y Estado del Proyecto (Informe de Gestión). Estos informes estarán sujetos a la aprobación del Ministerio de Relaciones Exteriores.

Metodología

El PROVEEDOR debe gestionar el Proyecto conforme a la Metodología de Gestión de Proyectos PMI que permita cumplir al menos las siguientes metas:

a) Mantener la continuidad operacional del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.
b) Transferir conocimiento del MINISTERIO DE RELACIONES EXTERIORES al PROVEEDOR, y viceversa
c) Minimizar el tiempo requerido entre la instalación y la puesta en marcha
d) Maximizar la utilización de los recursos del MRE y del PROVEEDOR
e) Generar los modelos de "Procesos de Negocio" y manuales de "Operación" que serán usados en la operación del MRE, como subproducto de la implantación del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES.
f) Entrenar al equipo de proyecto del MRE.
g) Entrenar a los usuarios utilizando un enfoque orientado a los procesos
h) Involucrar al usuario en la aceptación y buen uso del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES

La metodología debe considerar diferentes aspectos para gestionar los riesgos propios de una implementación de esta envergadura, tales como:

a) Identificación de los factores críticos para el éxito
b) Requerimientos por parte de los colaboradores del MRE (instructores, equipo técnico, usuarios líderes, usuarios finales, alta dirección)
c) Entendimiento de los objetivos estratégicos por unidades y/o procesos
d) Rediseño continuo de procesos
e) Definición de parámetros predefinidos para que los usuarios identifiquen sus necesidades
f) La integración de personas, procesos y tecnologías
g) Cumplimiento de los estándares de calidad y buenas prácticas
h) Gestión del cambio

Además, debe permitir realizar un control y seguimiento preciso y detallado de la implementación del proyecto en cualquiera de sus fases y establecer los procedimientos para solucionar las falencias detectadas.

Con la finalidad de dinamizar la estructura organizacional del servicio, se creará en el MRE roles de Gestores de Servicios como interlocutores con el proveedor. En esta sección se describe la organización, metodología y procedimientos requeridos por el MRE para la administración del servicio. A continuación, se presenta los roles organizacionales a fin de que el PROVEEDOR estructure una organización que se encuentre alineada para el desarrollo de las diferentes fases en transición y operación del servicio.

Organización para el servicio

Como contraparte, se espera del PROVEEDOR contar con una organización donde se asuma roles operacionales de Líder de Proyecto para la fase de transición y Service Manager para la fase de operación.

Las frecuencias mínimas de reuniones por niveles serán:

- Nivel Estratégico. Reuniones Semestrales.
- Nivel Táctico. Reuniones Mensuales.
- Nivel Operacional. Reuniones Semanales.

En cada nivel se esperan tener reuniones periódicas para revisar los avances del proyecto, los cambios mayores, mejoras en el servicio o cualquier tema conveniente para garantizar el buen desenvolvimiento del servicio, además de considerar reuniones no programadas en caso de urgencia las mismas que serán concertadas en coordinación conjunta.

El PROVEEDOR debe considerar:

- Un Director de Proyecto a tiempo parcial durante la vida del contrato.
- Un Gerente de Proyecto dedicado a tiempo completo durante la etapa de implementación y después de forma remota durante la vida del proyecto.
- Un Service Manager para la etapa de operación a tiempo completo.

Organización para la implementación y explotación

Gerencia del Proyecto

La administración de cualquier proyecto requiere buenas herramientas para planear, asignar personal administrativo, calcular, hacer seguimiento e informar el avance. Debe combinar herramientas y técnicas que le permitirán al Gerente y Líder de Proyecto emitir informes oportunos, estar en capacidad de identificar potenciales áreas problemáticas y, por lo tanto, tomar las acciones correctivas para cumplir con el trabajo según lo planeado. El Gerente de Proyecto elaborará un "Informe de Gestión" mensual, en el cual se detallan las labores de servicio realizadas y se resaltan los resultados de Niveles de Servicio.

Junto con este Informe de Gestión, el Gerente de Proyecto completará un "Acta de Conformidad" para cada tarea finalizada que represente un entregable tangible o un logro que se definirá durante la Fase de Transición del Proyecto. El Gerente de Proyecto de El MRE utilizará este documento para revisar el logro o tarea terminada frente a los criterios de terminación que se definirán durante la Fase de Transición del Proyecto, dándolo por aceptado o haciendo las observaciones pertinentes para que el PROVEEDOR corrija las desviaciones respecto de los criterios definidos por ambas partes.

Otra característica importante de la Gerencia del Proyecto del PROVEEDOR es que permite una buena comunicación y documentación. De cada reunión se elabora un acta en un formato llamado "Acta de la Reunión" que refleja los asistentes, el orden del día, los tópicos discutidos, las resoluciones y decisiones tomadas, elementos de acción (identificando al responsable y la fecha esperada de resolución) y aspectos críticos de alarma que requieren la atención inmediata de la Gerencia del Proyecto y/o de la Gerencia Ejecutiva. Las actas se distribuyen a los asistentes y también se almacenan en la biblioteca del proyecto para referencia futura.

Este proceso es sólo una muestra de la metodología que el PROVEEDOR usa para administrar un proyecto. Durante la fase de planificación el PROVEEDOR deberá proponer formatos de control para documentos de diseño, procedimientos de documentación para aspectos o solicitud de cambio y procesos de control y de informe que les permitirá a los Ejecutivos de Proyecto del equipo del PROVEEDOR mantenerse informados sobre los servicios a ser prestados.

De esta manera, la organización del servicio cumplirá con las siguientes características:

- Será formal, permanente y estará dentro de la estructura administrativa del MRE y del PROVEEDOR. Asimismo, el flujo de decisiones e información se hará a través de la organización designada explícitamente por el MRE para la prestación del servicio.
- Contará con el apoyo y responsabilidad gerencial directos de las dos partes. Para esto se designarán, en el MRE y en el PROVEEDOR, Ejecutivos de Proyecto (Ejecutivo de proyecto del PROVEEDOR y gestor de servicios de parte del MRE) como responsables que tienen como objetivo velar por el cumplimiento del servicio. Dichos Ejecutivos de Proyecto y sus delegados tendrán en el proyecto suficiente autoridad y atribución para resolver los conflictos que puedan poner en riesgo los objetivos, metas o resultados del servicio.
- Será simétrica entre el PROVEEDOR y el MRE, de manera que se permita un ágil entendimiento entre niveles equivalentes y se garantice un esquema adecuadamente escalado para la solución de problemas.

Metodología de la Gerencia de Proyectos

La metodología de Gerencia de Proyectos contempla los procesos de planeación y seguimiento durante toda la vida del proyecto. Su objetivo es proveer al Gerente de Proyecto con los mecanismos para poder entregar el servicio acordado en el tiempo acordado y al costo acordado.

Se basa en el concepto de un único punto de contacto entre el MRE y el PROVEEDOR, para colocar la información a disposición de los niveles aprobados oportunamente.

La metodología de Gerencia de Proyectos del PROVEEDOR debe ejecutarse con estándares globales y mejores prácticas del mercado internacional.

La metodología debe cubrir los pasos básicos de la administración de un proyecto de servicios, tales como estimación de esfuerzo, planeación, elaboración del plan de trabajo, descomposición de componentes de trabajo, definición de dependencias, seguimiento y estimación del estado actual del proyecto.

Esto se complementa con metodología para manejo de excepciones, manejo de riesgos y su contención.

Roles y Responsabilidades del PROVEEDOR

Para el desarrollo del servicio el PROVEEDOR designará diferentes recursos, quienes tendrán las responsabilidades que se detallan a continuación.

Director del Proyecto

Ejecutivo designado como el responsable de más alto nivel del proyecto, que tiene como misión velar por el cumplimiento del servicio. El Director y sus delegados tendrán la suficiente autoridad y atribución para resolver los conflictos que puedan poner en riesgo los objetivos, metas o resultados del servicio.

Gerente de Proyecto

Sus responsabilidades son:

- Notificar al MRE de cualquier falla o problema que afecte la disponibilidad de los servicios provistos por él.
- Permanecer en continuo contacto con el responsable del proyecto parte del MRE, para definir los posibles cambios o adecuaciones que se deban realizar en el servicio por modificación en las aplicaciones y/o hardware.
- Ejecutar las actividades y procedimientos acordados de acuerdo al Plan General del Proyecto el mismo que será presentado y aprobado al Inicio del Proyecto.
- Mantener al día la documentación de los reportes de problemas y sus soluciones.
- Informar acerca del desempeño de acuerdo a los niveles de servicio requeridos, mediante reportes mensuales y reuniones periódicas.
- Coordinar todo cambio que afecte los niveles de servicio, con el Gerente de Proyecto por parte del MRE.
- Mantener y actualizar el manual de procedimientos de operación del servicio.
- Coordinar con el personal del MRE los aspectos técnicos a que haya lugar.
- Administrar el Procedimiento de Control de Cambios.
- Elaborar en conjunto con el MRE el procedimiento de inspección del servicio.
- Asegurar que la transición de servicios se realice de forma ordenada y con el menor impacto operativo para El MRE.
- Realizar la transición de los servicios hasta su fase en operación.
- Coordinar los cronogramas de transición con El MRE.
- Estabilizar los servicios de hasta los niveles establecidos en el acuerdo de servicio.

Service Manager

Es el encargado de Gestionar la operación del servicio in situ en el horario laboral del Ministerio de Relaciones Exteriores, con las siguientes responsabilidades:

- Gestionar los servicios, disponiendo de los recursos necesarios para que se ejecuten de acuerdo a lo previsto. Asimismo, monitoreando los indicadores de niveles de acuerdo de servicio establecidos.
- Realizar la gestión de los incidentes y requerimientos, para que estos sean atendidos oportunamente.
- Hacer que los servicios prestados cumplan los acuerdos de niveles de servicio establecidos.
- Asegurarse que el personal a cargo este propiamente entrenado, tenga las instrucciones, herramientas y metodología para realizar sus trabajos.
- Realizar la coordinación con el MRE para mantenimientos de equipos y software.
- Realizar las comunicaciones al MRE, ante cualquier incidente que afecten servicios relacionados a su operatividad.

- Elaborar informes mensuales de recomendaciones de acuerdo a los valores de indicadores de acuerdo de nivel de servicio alcanzado.

Equipo de Operación y Soporte Técnico (Staff TI)

Sus responsabilidades son:

- Operación y monitoreo de los servicios provistos 24x7.
- Resolución de tareas específicas (especialistas).
- Generación de copias de respaldo en cintas.
- Mantenimiento preventivo y correctivo de hardware y sistema operativo.
- Mantenimiento de equipos de comunicación especificados en el alcance.
- Mantenimiento de la infraestructura.
- Mantenimiento del software.

Roles y Responsabilidades del MRE

- El MRE administrará este proyecto teniendo los siguientes roles y responsabilidades:
- Director del Proyecto
- Gerente de Proyecto
- Líder de Área Usuaria
- Staff TI de El MRE.

Adicionalmente, el MRE definirá las personas que considere necesarias para cubrir las responsabilidades asignadas.

Director del Proyecto

Ejecutivo responsable de la gestión corporativa de tecnología de información y comunicaciones de El MRE.

Gerente del Proyecto

Sus responsabilidades son:

- Velar porque los compromisos contractuales se cumplan.
- Mantenerse informado sobre el mantenimiento y actualización del manual de procedimientos de operación del servicio.
- Mantener comunicación formal con todo el personal que participa en la prestación del servicio, tanto del MRE como del PROVEEDOR, tanto a nivel ejecutivo como a nivel Operativo.
- Coordinar la participación de todas las áreas involucradas del MRE, en la totalidad de las actividades relacionadas con la prestación del servicio.
- Dirigir y responder por el adecuado desarrollo del Procedimiento para Control de Cambios al servicio, manteniendo al día la documentación de los cambios.
- Dirigir y responder por el adecuado desarrollo del manejo de problemas en el servicio.
- Mantener actualizada la documentación sobre el estado del servicio y el registro histórico de los eventos desarrollados y sus causales con base en la información proporcionada por el PROVEEDOR.

- Coordinar y facilitar la relación con las áreas del MRE y el PROVEEDOR relacionados con los servicios.
- Responder a los informes y/o reportes del Gerente de Proyecto o Service Manager del PROVEEDOR en un plazo no mayor a cinco (5) días hábiles o de acuerdo a lo que se defina en el modelo de gobierno a ser establecido en la fase de planificación del servicio.

Líder de Área Usuaria

- Participar en las reuniones de planificación del Proyecto.
- Proponer la prioridad a los requisitos durante el desarrollo del Proyecto.
- Responder a las dudas del equipo.
- Estar disponible durante el transcurso del proyecto para responder a las preguntas que puedan aparecer.
- Participar en la reunión verificación de entregables, revisando los requerimientos completados.

Staff TI de El MRE.

El equipo de soporte técnico del MRE será encargado de brindar las facilidades para la transición de los servicios en operación en sus instalaciones o de terceros. Asimismo, mantendrá constante interacción durante la operación de los servicios.

Comités

Para el adecuado desarrollo del proyecto y los servicios, se tienen contemplados dos (2) niveles de comités, estos son el Comité Ejecutivo y el Comité Operativo.

Comité Ejecutivo

El objetivo de este comité es darle al proyecto un control estratégico y buscar la oportuna toma de decisiones sobre aspectos que lo modifiquen en tiempo, alcances y costo. Estará conformado como mínimo por: El Director del Proyecto del PROVEEDOR, el gerente de proyectos del PROVEEDOR, el Director del Proyecto de El MRE, el gerente del proyecto del MRE. Es la instancia superior de decisión. Se reunirá bimestralmente o cuando sea requerido por el Comité Operativo. Asimismo, este comité podrá contar con la participación de otros ejecutivos de alto nivel del PROVEEDOR a solicitud del MRE.

Responsabilidades:

- Obtener información y tomar decisiones estratégicas sobre el proyecto y los problemas identificados.
- Resolver cualquier desacuerdo o controversia entre las partes, relacionados con la ejecución del proyecto que no haya podido resolverse en instancias previas.
- Velar por el cumplimiento de los acuerdos y Niveles de Servicio del Proyecto.
- Ajustar las líneas base de los servicios durante la operación.

- Definir y comunicar las directrices en los procesos y estructura.
- Aprobar los cambios que impliquen modificación en tiempo, costos, Niveles de Servicio o alcance del proyecto.
- Dirigir la estrategia de comunicación y visibilidad corporativa del proyecto.

Comité Operativo

El objetivo de este comité es el de realizar la gestión táctica y de campo en el proyecto. Deberá estar conformado por el Gerente de Proyecto del PROVEEDOR, el Gerente del Proyecto del MRE. Se reunirá semanalmente durante la fase de transición y mensualmente durante la fase de operación. También se debe considerar que en los períodos pico del proyecto o cuando lo estimen conveniente, según el estado del proyecto.

Debe dar solución a inconvenientes presentados durante el desarrollo del proyecto siempre y cuando estos no afecten el desarrollo del mismo en alcance, tiempo y costos, así como alertar a los miembros del Comité Ejecutivo sobre situaciones que excedan su competencia.

Responsabilidades:

- Revisar el alcance del proyecto. Decidir las acciones requeridas para el cumplimiento del Cronograma de Actividades. Determinar prioridades y acordar el planeamiento detallado para las diferentes actividades. Identificar los recursos necesarios para terminar las actividades.
- Resolver los problemas o alertar a los miembros del Comité Ejecutivo del Proyecto sobre inconvenientes presentados en el desarrollo y coordinar una reunión extraordinaria con dicho comité en caso de ser necesario.
- Preparar las reuniones periódicas de seguimiento.
- Coordinar la aprobación de los objetivos de Niveles de Servicio presentados por el PROVEEDOR.
- Coordinar la aprobación final de los Acuerdos de Niveles de Servicio, según los criterios definidos en los objetivos de niveles de servicio.
- Determinar prioridades y acordar el planeamiento detallado para las diferentes actividades.
- Identificar los recursos necesarios para terminar las actividades
- Resolver los conflictos y problemas que se presenten durante la ejecución del proyecto. En caso de no ser posible, los Gerentes de Proyecto los comunicarán en la reunión del Comité Ejecutivo, con las recomendaciones del caso para su solución en este Comité.
- Coordinar las aprobaciones por parte del MRE de las Actas correspondientes a las Pruebas de Aceptación.

ETAPA DE IMPLEMENTACIÓN

La etapa de implementación tendrá una duración máxima de siete (07) meses, en caso contrario el MRE podrá aplicar las PENALIDADES que se especifican en la sección "PENALIDADES". Esta etapa considera la

implementación y recepción gradual de al menos los hitos mencionados a continuación: la capacitación, la transición de entrada y la habilitación de Sedes.

La Etapa de Implementación puede estar definida de forma tal que una vez finalizadas las pruebas de aceptación sea posible empezar de inmediato a atender usuarios.

Hitos de la Implementación

Cada fase del proyecto está compuesta de hitos y/o entregables de control, los cuales, una vez realizados, integran la conformidad contractual del programa de implementación.

Transición de Entrada

Políticas y Estrategias de la Migración de los Servicios

Se debe desarrollar la transición de los servicios cumpliendo las siguientes políticas y estrategias generales:

- En la fase de planeamiento inicial el proveedor deberá desarrollar un plan de transición a detalle. Cualquier cambio será autorizado por el MRE.
- El proveedor en conjunto con El MRE elaborará un plan de contingencia y plan de Rollback para la implementación de cada servicio a fin de minimizar la parada de los servicios.
- Se podrán aplicar penalidades por incumplimiento de nivel de servicio en la etapa de transición.
- Si el tiempo de indisponibilidad es atribuible el MRE, no se impondrán penalidades al proveedor.

Plan de Migración de Servicios TI

El proveedor debe cumplir con las siguientes actividades generales en tres etapas:

- Preparación. Tiene por finalidad planificar, programar y alistar los servicios para la migración e implementación de la solución integral.
- Implementación. Consiste en la ejecución de la implementación de los servicios.
- Post-Implementación. Es la etapa de verificación de los servicios en operación.

Las actividades específicas por etapa son:

Etapa de Preparación

La Etapa de Preparación tiene como finalidad ejecutar todas las actividades y coordinaciones necesarias para iniciar la implementación de los servicios

Las actividades a realizar durante esta etapa serán las siguientes:

- Reuniones de coordinación entre el MRE y el proveedor.
- Programa de actividades de implementación de servicios.
- Identificar los responsables de cada actividad.
- Elaborar el plan de contingencia y rollback para cada servicio.

- Programar ventanas de trabajo para la implementación de servicios.
- Verificar que las instalaciones se encuentren preparadas para la implementación de los servicios.
- Entrega de la Ingeniería de detalle de la implementación de los servicios, incluyendo todos los diseños, planos, manuales de usuario y administración de cada componente de hardware, software, comunicaciones, redes, acondicionamiento y equipamiento de los centros de datos, equipos de captura de datos biométricos, cámaras, firma digital, etc., que forma parte de la solución integral descrita en el presente documento. La documentación debe ser entregada impresa y en 3 copias de DVD.
- Identificación de Riesgos / Mitigación por parte del proveedor.

Etapa de Migración de los Servicios

La Fase de Migración tiene como finalidad ejecutar todas las actividades necesarias para el correcto pase a producción o salida en vivo de los servicios.

Las actividades a realizar durante esta etapa serán las siguientes:

- Provisión de infraestructura de hardware para los servicios que brindará el proveedor.
- Implementación de ambientes de producción, calidad y desarrollo.

Los cronogramas específicos para cada actividad serán propuestos por el Gerente de Proyecto del PROVEEDOR y aprobados por el MRE.

El soporte de los aplicativos implementados por el proveedor serán de su responsabilidad exclusiva durante la migración.

La instalación de los módulos del SISTEMA DE ACTIVIDADES MIGRATORIAS (SAM) que son necesarios para los procesos operativos diarios en las estaciones de trabajo se realizara en coordinación con el MRE.

Etapa de Post-Migración de los Servicios

La Etapa de Post-Migración tiene como finalidad optimizar el servicio luego de concluida la Etapa de Implementación. En esta Etapa el ambiente de producción, soportará la carga real de usuarios.

Se dará como conforme el servicio de transición cuando todos los servicios descritos en estos términos de referencia se encuentren operando en su totalidad en el Ministerio de Relaciones Exteriores.

Pruebas de recepción de los servicios

El PROVEEDOR será el responsable por todas las pruebas técnicas pertinentes referidas únicamente a los servicios. Esta responsabilidad incluye la realización de las mismas, mantener un registro y la elaboración de los documentos correspondientes. Asimismo, todas las herramientas, instrumentos y equipos necesarios para la realización de las pruebas, serán otorgados por el Proveedor.

Las pruebas funcionales sobre las aplicaciones dentro del alcance del presente servicio, deberán ser realizadas por el personal del MRE. Si las pruebas funcionales fallan, se debe recurrir al plan de contingencia o rollback para que el servicio o aplicación afectada no salga en vivo.

El MRE validará el protocolo del plan de pruebas de aceptación o conformidad de cada servicio.

El PROVEEDOR elaborará durante la fase de planificación el documento "Protocolo de Inspección y Pruebas de Recepción" conteniendo como mínimo las actividades a realizar, una breve explicación de las mismas, el

objetivo de calidad a cumplir y un recuadro vacío para indicar el resultado de la evaluación, este recuadro será llenado únicamente por la empresa y según su juicio exclusivamente. Este documento será revisado y aprobado por el MRE, previo al inicio de las Pruebas de Recepción.

Las pruebas se clasificarán en:

- Las Pruebas de Implementación; son aquellas que el Proveedor ejecutará una vez finalizada la implementación del servicio. Estas serán previas a las de Recepción Provisional, la participación del MRE es opcional.
- Las Pruebas de Recepción Provisional; tendrán por objeto verificar que el servicio implementado cumpla con lo establecido en las especificaciones del contrato y lo definido en el documento "Plan de Proyecto" a ser definido durante la fase de planificación. Dichas pruebas e inspección serán realizadas por el Proveedor con participación de personal de las empresas siguiendo el documento "Protocolo de Inspección y Pruebas de Recepción", previamente aprobado. La firma del Acta de Recepción Provisional, marcará el inicio del Periodo de Evaluación. El protocolo de inspección y pruebas de recepción debe ser aprobado por el MRE. Para esto el proveedor deberá entregar dicho protocolo y el MRE tendrán un plazo máximo de hasta 5 días calendario para emitir conformidad u observaciones.
- Las Pruebas de Recepción Definitiva; se realizarán luego del Periodo de Evaluación, siguiendo nuevamente lo estipulado en el documento "Protocolo de Inspección y Pruebas de Recepción" en las observaciones o "Reparos" establecidos anteriormente si existiesen, además de corregir posibles problemas ocurridos en el Periodo de Evaluación. La firma del Acta de Recepción Definitiva, marcará el fin del Proyecto de Implementación. El plazo para emitir conformidad u observaciones en las pruebas de recepción definitiva será de hasta 5 días calendario.

La clasificación de resultados por cada ítem en el Protocolo de Inspección y Pruebas es como sigue. "CONFORME" cuando la prueba específica ha cumplido en 100% lo esperado, "REPARO A" cuando la prueba ha fallado y el impacto en el desempeño, disponibilidad y calidad del servicio es alto; "REPARO B", cuando la prueba ha fallado y el impacto sobre el servicio es medio y "REPARO C" cuando la prueba ha fallado y el impacto sobre el servicio es bajo.

Cuadro 1 - Clasificación de reparos

Tipo	Descripción
Reparo A	Impacto severo al negocio ya sea económico o de imagen.
Reparo B	Impacto medio al negocio ya sea económico o de imagen.
Reparo C	Impacto bajo al negocio ya sea económico o de imagen.

El PROVEEDOR está obligado a repetir las pruebas y asumir todos los costos en uso de recursos y pago de penalidades si existieran retrasos en el calendario del proyecto; hasta suprimir todos los "Reparos" del tipo "A" y "B". La firma del Acta de Recepción Provisional se dará cuando no existan estos "Reparos" mencionados.

El Acta de Recepción Definitiva se firmará toda vez que no exista ningún "Reparo" por cada ítem del documento de protocolo de pruebas e inspección y se reciba toda la documentación pertinente descrita a continuación en formato físico y digital.

- Dos (02) juegos del diagrama (gráfico), planos y topologías de la solución propuesta suscritos por el especialista colegiado correspondiente.
- Dos (02) juegos de la solución implementada al detalle, incluida configuración de equipamiento.
- Dos (02) juegos de documentación de los Protocolos de Pruebas con las anotaciones realizadas por El MRE.
- Dos (02) juegos de documentos conteniendo el inventario detallado de los equipos y accesorios suministrados. (marca, modelo, número de serie, etc., manual de servicio de los equipos del Sistema de Personalización y Especificaciones técnicas de equipos de cómputo y comunicaciones instalados).
- Dos (02) juegos de diagramas de disposición de equipos por cada gabinete o rack.
- Dos (02) juegos de los manuales de usuario y técnico de los sistemas de información implementados.
- Dos (02) juegos de los roles y perfiles de operador usuario y técnico de los sistemas de información implementados, según los controles de separación de roles solicitados en la sección gestión de roles.
- Documentos relacionados a las declaraciones de las responsabilidades y derechos propiedad intelectual referidas a cada aplicación de software entregada.
- Dos (02) DVD's conteniendo toda la documentación anteriormente descrita, incluyendo los planos y diagramas solicitados en su formato de origen.
- Cualquier información adicional referente al proyecto que le sea requerida por El MRE con el fin de aclarar la prestación de los servicios.

Sistema Central de Identificación

a) Entrega y aprobación de las especificaciones detalladas de los sistemas de información que se implementarán.
b) Entrega y aprobación de las aplicaciones.
c) Entrega y aprobación del plan de capacitación.
d) Inicio de la capacitación de los instructores.
e) Inicio de la capacitación de los funcionarios.
f) Prueba del SISTEMA DE IDENTIFICACIÓN con carga simulada.

Interoperabilidad con otros Sistemas de Información

a) Demostración de la aplicación piloto de interacción entre el SISTEMA DE EMISIÓN DE PASAPORTES, y los Sistemas de Actividades Migratorias del MRE.
b) Demostración de la aplicación piloto de interacción entre el SISTEMA DE EMISIÓN DE PASAPORTES, y el Sistema Integrado de Migraciones.
c) Demostración de la aplicación piloto de interacción con sistemas externos.

Fábricas de Personalización de Documentos

a) Disposición de al menos 2 fábricas principales de pasaportes electrónicos.
b) Demostración de emisión del pasaporte electrónico con datos reales y en el formato definitivo.

Mesa de Ayuda

a) Funcionamiento del Nivel 1
b) Funcionamiento del Nivel 1 y escalamiento al Nivel 2

Sistemas Biométricos

a) Entrega y aprobación de AFIS 1:1
b) Entrega y aprobación de AFIS 1:N
c) Demostración del Sistema de Peritos Biométricos
d) Entrega y aprobación del Sistema de Peritos Biométricos

Back Office

a) Instalación del equipamiento para el funcionamiento del Back Office
b) Entrega y aprobación de las funcionalidades para la Unidad de Identificación
c) Entrega y aprobación de las funcionalidades para la Unidad de Consulta Policial
d) Entrega y aprobación de las funcionalidades para la Unidad de Peritos Biométricos (AFIS)

Sistema de Atención de Usuarios

a) Entrega y aprobación del Sistema de Solicitudes de Pasaportes.
b) Entrega y aprobación Sistema de Entrega de Pasaportes.
c) Demostración del funcionamiento de una Sede.

Pasaporte Electrónico

a) Entrega y aprobación del plan de despliegue de sistemas de captura en las Oficinas Consulares.
b) Inicio de la habilitación de Sedes.
c) Capacitación para funcionarios (por parte de los instructores).

Sistema de Bloqueo Definitivo de Documentos

a) Entrega y aprobación del Sistema de Bloqueo de pasaportes en Sedes.
b) Entrega y aprobación del Sistema de Bloqueo de los pasaportes por Internet.

Gestión de Información

a) Entrega y aprobación del Sistema de Gestión Operativa
b) Entrega y aprobación del Sistema de Gestión Estratégica
c) Entrega y aprobación del Sistema de Auditoría Interna y trazabilidad.

Pruebas

Una vez completada la implementación cada hito, el PROVEEDOR podrá iniciar el período de pruebas, el cual está definido en base a un paralelo reducido.

El periodo de pruebas se dará por concluido cuando el SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES haya funcionado sin ninguna objeción por parte del MRE y se hayan aprobado las pruebas solicitadas por el MRE como parte de la evaluación.

Pruebas integrales

Cuando el back office sea implementado y se haya realizado el despliegue de los sistemas de captura en las Oficinas Consulares, se realizarán 03 días de pruebas integrales por cada sede, la cual será monitoreada y guiada de manera presencial o remota.

Las pruebas integrales de Pasaporte Electrónico estarán regidas por los siguientes plazos:

a) Duración mínima: tres (3) días calendarios
b) Duración máxima: diez (10) días calendarios

En el caso de prolongarse más de diez (10) días calendarios, el MRE podrá aplicar las PENALIDADES descritas en la sección "PENALIDADES".

Los pasaportes electrónicos emitidos durante las pruebas no podrán ser activados ni entregados a los usuarios y sólo se usarán para control de calidad y luego serán destruidos por el MRE.

Habilitación Inicial

Previo a iniciar la Etapa de Explotación, el PROVEEDOR deberá tener operativos: la recepción de solicitudes de documentos, emisión, despacho y entrega de documentos. Este periodo de explotación puede comenzar en cada sede en periodos distintos, conforme se logre su habilitación.

Dentro de los primeros 150 días calendario luego de firmado el contrato, el PROVEEDOR deberá tener habilitadas, funcionando en línea y recibidas a total conformidad por el MRE, según corresponda, al menos las Oficinas Consulares de la Unión Europea de mayor demanda (Madrid, Milán, Barcelona y Ámsterdam). Para esta habilitación, dichas Oficinas Consulares podrán operar utilizando su sistema actual de Back Office.

Luego de esta etapa comienza la puesta en producción de la emisión del pasaporte electrónico.

El plazo de implementación y entrega de la solución integral en las demás sedes es de hasta 180 días calendario luego de firmado el contrato, incluyendo la capacitación del personal encargado de la atención a los usuarios y despliegue, luego de esta etapa comienza la fase de explotación de la emisión del pasaporte electrónico.

Especialistas requeridos para la implementación del sistema de personalización y emisión del pasaporte electrónico

La Ministerio de Relaciones Exteriores requiere la participación presencial de este grupo de especialistas durante el periodo de tiempo necesario en cada etapa del proyecto. Es por ello que deberá contarse con el siguiente personal, como mínimo:

Personal	Responsabilidades	Dedicación mínima
Gerente de proyecto	1) Gestionar el proyecto de acuerdo al estándar del PMI 2) Coordinar con el personal supervisor del Ministerio de Relaciones Exteriores 3) Presentar informes y reportar el estado del proyecto	Desde el inicio hasta el final de la implementación a tiempo completo en Lima y durante el período de contratación de forma presencial o remota
	Desarrollo de las capacitaciones:	

Coordinador de capacitación y capacitadores	**1)** personal encargado de la administración y soporte de la Aplicación central de procesamiento y firma. 2) personal encargado de la captura de datos a nivel nacional	Desde el inicio de las capacitaciones hasta su culminación
Ingeniero TI	Configuración y puesta en marcha de los sistemas, servidores, red, etc.	Hasta la entrega del Centro de procesamiento
Ingeniero de seguridad	Diseño e implementación de los controles de seguridad del Centro de procesamiento	Hasta la entrega del Centro de procesamiento
Especialista en Mesa de ayuda	Diseño e implementación de la Mesa de ayuda a nivel nacional	Hasta la entrega de la Mesa de ayuda a nivel nacional
Especialista PKI	Implementación del sistema PKI y la firma digital correspondiente	Hasta la entrega de la Aplicación central de procesamiento y firma

La experiencia mínima requerida para el grupo de especialistas, en los últimos siete (07) años, es la siguiente:

Personal	Experiencia mínima
Director de Proyecto	- Dirección de dos (02) proyectos complejos de despliegue a nivel internacional
Gerente de proyecto	- Dirección de proyectos complejos de despliegue a nivel internacional
Coordinador de capacitación	- Dirección de un (01) programa de capacitación vinculado a sistemas PKI - Dirección de un (01) programa de capacitación vinculado a sistemas de emisión de pasaporte electrónico
Capacitadores	- Participación en un (01) programa de capacitación vinculado a sistemas PKI - Participación en un (01) programa de capacitación vinculado a sistemas de emisión de pasaporte electrónico
Ingeniero TI	- Participación como Ingeniero TI en la implementación de dos (02) centros de datos (servidores)
Ingeniero de seguridad	- Participación como Ingeniero de seguridad en la implementación de dos (02) centros de datos (seguridad)

Personal	Experiencia mínima
Especialista en Mesa de ayuda	- Participación como Especialista en Mesa de ayuda en la implementación de dos (02) sistemas de Mesa de ayuda a nivel nacional o regional
Especialista PKI	- Participación en la implementación de dos (02) proyectos relacionados a la firma digital (sistemas de valor añadido)
Service Manager	- Participación como Gestor de compromiso o equivalente en la implementación de dos (02) sistemas de Mesa de ayuda a nivel nacional o regional.

El PROVEEDOR deberá asegurar la continuidad del personal con las mismas capacidades y experiencia solicitadas, a fin de no afectar el desarrollo normal del proyecto.

El Ministerio de Relaciones Exteriores solicitará y aprobará la documentación sustentatoria necesaria para validar el perfil del personal propuesto.

ETAPA DE EXPLOTACIÓN

La Etapa de Explotación del sistema comienza una vez terminada la habilitación de todas las Sedes.

La duración de la etapa de explotación es de 36 meses

Transición de Salida

La Transición de salida se aplicará en caso de término de contrato o de Resolución Contractual debido al incumplimiento.

La duración de la fase de transición de salida será como máximo de cuatro (4) meses, previos al término de los 36 meses de operación del SERVICIO DE EMISIÓN DE PASAPORTES ELECTRÓNICOS COMUNES, DIPLOMÁTICOS Y ESPECIALES (fase de explotación).

En caso de resolución contractual la fase de transición de salida se iniciara al día siguiente de su notificación al PROVEEDOR, la misma que no deberá exceder de cuatro (4) meses.

Políticas y Estrategias de Migración de Salida de los Servicios TI

El PROVEEDOR deberá desarrollar en forma coordinada con el MRE, un plan de transición de salida que detalle la secuencia de migración de servicios.

Las actividades de transición del MRE deberán ser desarrolladas en una ventana de tiempo coordinada entre el proveedor, y el MRE los fines de semana, días feriados no laborables u horas no laborables a fin de minimizar el impacto en el servicio.

Se han definido dos (2) etapas para la transición de salida, estas son:

Etapa de Preparación de Salida

La Etapa de Preparación tiene como finalidad ejecutar todas las actividades y coordinaciones necesarias para iniciar la salida de los servicios.

Las actividades a realizar durante esta etapa serán las siguientes:

- Reuniones de coordinación entre el MRE y el PROVEEDOR.
- Programa de actividades de migración para el traslado de los servicios.
- Programar ventanas de trabajo para el traslado de los servicios.

Etapa de Traslado de Servicios

La Fase de traslado de servicios tiene como finalidad ejecutar todas las actividades necesarias para el correcto traslado de los servicios hacia una ubicación que determine El MRE.

Las actividades a realizar durante esta etapa serán las siguientes:

- Migración de datos.
- Migración de ambientes desarrollo y calidad.
- Retiro y transferencia de derechos de acceso (del proveedor a personal asignado por el MRE)

Los cronogramas específicos para cada actividad serán propuestos por el Gerente de Proyecto del PROVEEDOR y aprobados por el MRE y deberán culminarse a más tardar quince (15) días antes del inicio de la salida de los servicios.

Responsabilidades del PROVEEDOR durante la Transición de Salida

- El PROVEEDOR será responsable de aplicar las mejores prácticas en la realización de las tareas incluidas en el plan de trabajo presentado para ser llevadas a buen término, con la seguridad y confiabilidad, minimizando todos los riesgos dentro de los alcances de la presente propuesta.
- El PROVEEDOR será responsable por el mantenimiento, salvaguarda y respaldo de las configuraciones (Sistema Operativo, redes y Aplicaciones) presentes en todos los servidores, sistemas de almacenamiento y demás Componentes de Hardware y Software hasta su entrega a El MRE o quien designe este. En el caso que la entrega al futuro proveedor, sobrepase la fecha de culminación del contrato, se gestionará a través del proceso de control de cambios para la ampliación del servicio.
- Dar las facilidades técnicas y de acceso al MRE.
- Entregar las últimas copias de respaldo de la información tanto de las bases de datos, las aplicaciones y configuración de los equipos del servicio.
- Entregar el código fuente de todos los desarrollos específicos realizados para el proyecto.
- Trasladar procedimientos y políticas de operación al MRE o a quien este designe.
- Capacitar al personal que El MRE designe considerando para ello, por lo menos 10 horas de capacitación a 10 personas En los roles de Service Manager, Gestor de Operaciones y, resolución de incidentes.

El proveedor debe asumir los costos y acciones necesarias de la Transición de Salida:

Todo el equipamiento, información, insumos, repuestos, media, y cualquier otro componente que forma parte de la solución descrita en el presente documento pasará a ser de propiedad del MRE.

PRUEBAS DE LOS EQUIPOS DE PERSONALIZACIÓN DE PASAPORTES

PRUEBAS DE ACEPTACIÓN EN FÁBRICA (FAT)

a. Las pruebas y los procedimientos de las FAT consistirán en la verificación del funcionamiento de los equipos y de todas las características técnicas funcionales contempladas en este contrato previo a su embarque al Perú.

b. Los equipos que serán probados en la fábrica, comprenden a los equipos destinados a los procesos de personalización del pasaporte electrónico, tales como:
   i. Carga y repositorio de selección de página
   ii. Detección y lectura de la serie perforada del libro de pasaporte
   iii. Codificación del chip
   iv. Personalización gráfica del pasaporte
   v. Control de calidad automático de lectura del chip y de personalización
   vi. Salida o expulsión del pasaporte personalizado
   vii. Lector de microchip

c. Los equipos computacionales de uso común, tales como PCs, impresoras, escáneres de huellas, servidores, etc. estarán exentos de estas pruebas. El proveedor deberá proporcionar los informes de control de calidad / resultados de test de producción de estos equipos, antes del envío.

d. El PROVEEDOR deberá comunicar al MRE la fecha y lugar donde se desarrollarán las FAT, por lo menos cuatro (04) semanas antes del inicio de dichas pruebas.

e. El PROVEEDOR deberá remitir a el MRE el protocolo de pruebas FAT por lo menos quince (15) días antes del inicio de dichas pruebas. El MRE notificará al contratista la revisión y los comentarios efectuados dentro de los diez (10) días a partir de entonces. El contratista deberá modificar y elevar nuevamente los procedimientos FAT acorde a los comentarios recibidos dentro de los cinco (5) días a partir de dicha revisión.

f. Al final de las FAT se levantará el acta de pruebas FAT a ser suscrito por el MRE y por el PROVEEDOR. Si al caso un sistema o sub-sistema presenta fallas leves, esto será levantado durante las pruebas de aceptación en sitio, de lo contrario, de presentarse fallas críticas, las FAT deberán extenderse o posponerse en fecha a fin de levantar dichas fallas, considerando que todos los gastos adicionales deberán ser asumidos por el PROVEEDOR. el MRE se reserva el derecho de decidir la realización solamente de las pruebas no aceptadas o realizar todas las pruebas FAT nuevamente, en caso de encontrarse deficiencias graves.

g. Cualquier demora por fallas en las FAT no implicará una extensión del plazo de entrega de los equipos.

PRUEBAS DE ACEPTACIÓN EN SITIO (SAT)

a. Las pruebas y los procedimientos de las SAT deberán consistir en la verificación del funcionamiento de los equipos y de todas las características técnicas funcionales contempladas en este contrato para un entorno operacional real. Las SAT deberán también verificar que los equipos contemplados en un eventual contrato, incluyendo repuestos, hayan sido enviados y que toda la documentación, diseños, planos de fabricación, etc., hayan sido completados y enviados.

b. El contratista deberá presentar para la revisión y aprobación del MRE las pruebas y procedimientos SAT, por lo menos 15 días antes del inicio de dichas pruebas. el MRE notificará al PROVEEDOR la revisión y los comentarios efectuados dentro de los 10 días a partir de entonces. El contratista deberá modificar y elevar nuevamente los procedimientos SAT acorde a los comentarios recibidos dentro de los cinco (5) días a partir de dicha revisión.

c. Si un sistema o subsistema (o varios) no es capaz de pasar una o más de las pruebas, es decir, las pruebas demuestran que el sistema no cumple con los requisitos de las especificaciones, el contratista deberá corregir la causa del fallo. El MRE se reserva el derecho de decidir la realización solamente de las pruebas no aceptadas o realizar todas las pruebas SAT nuevamente. Todos los gastos que demanden estas pruebas correrán a cargo del contratista, incluidos los gastos de viaje y estancia (que cubren alojamiento, comidas y transporte local) para los representantes del MRE que vuelvan a participar en las mismas.

d. En caso que las discrepancias detectadas no sean solucionadas o en caso que el equipo no se ajuste a las especificaciones u otros requisitos del contrato, el MRE, a su entera discreción, podrá rechazar o negarse a aceptar el equipo. A tal efecto informará al PROVEEDOR y este, dentro de los 5 días siguientes a la recepción de la notificación de rechazo o de la negativa a aceptar el equipo, a la sola opción del MRE, deberá:

   - Reparar el equipo de forma que permita al mismo cumplir con las especificaciones u otros requisitos del contrato; o,
   - Reemplazar el equipo con uno de calidad igual o superior;

   Para ello, todos los gastos que demanden estas tareas serán asumidos integralmente por el proveedor.

e. Los certificados de aceptación en sitio deberán firmarse inmediatamente después que se cumplan satisfactoriamente las siguientes condiciones:

   a) Se hayan levantado las fallas leves presentadas durante las FAT.
   b) Las SAT son exitosas;
   c) Los programas de formación se han realizado satisfactoriamente;
   d) Toda la documentación, planos conforme a obra (as-built), planes, manuales, etc., se han completado y entregado;
   e) Todos los repuestos, accesorios, equipos de prueba, etc. proporcionados bajo este contrato se han verificado de forma operativa y probados durante las SAT.

f. El contratista proporcionará el equipo de prueba requerido para el SAT. Todo el equipo de ensayo utilizado durante estas pruebas deberá estar debidamente calibrado con los certificados correspondientes.

RESPONSABILIDADES DEL PROVEEDOR

RESPONSABILIDADES DEL PROVEEDOR DURANTE LA OPERACION

a) Proporcionar el equipamiento y software para la Administración de Eventos Operacionales, Monitoreo de la Disponibilidad de los Servidores y Equipos de Comunicación, Monitoreo del Desempeño y Capacidad de los Servidores.
b) Proporcionar el equipamiento y software para la Administración de Incidentes y Problemas Operacionales y Administración de Cambios.
c) Asignar en el Centro Único de Contacto los analistas que atenderán los Incidentes, Cambios y Requerimientos.
d) Asignar el o los administradores de las herramientas de Monitoreo.
e) Asignar el o los administradores de las herramientas de Gestión de Incidentes, Problemas, Requerimientos y Cambios.
f) Implementar la herramienta de gestión de requerimientos e incidentes.
g) El proveedor deberá disponer de personal encargado de la administración de la Base de Datos, soporte y monitoreo central del sistema de producción de pasaportes. El servicio de administración deberá cubrir un horario de 24 horas x 7 días de la semana durante un periodo de 3 años, de los cuales 10 horas X 5 días deben ser ON SITE, en el local asignado por El MRE. Este personal brindará servicios de monitoreo, soporte de primer nivel y cambios solicitados por El MRE a la base de datos y a la aplicación de administración central.
h) El proveedor deberá disponer de personal encargado de soporte y monitoreo de la base de datos central del sistema de producción de pasaportes. El servicio de administración deberá cubrir un horario de 24 horas x 7 días de la semana durante un periodo de 3 años conforme lo establece los niveles de servicio.
i) El personal asignado deberá tener conocimientos de programación compatible con la aplicación central de producción de pasaportes, de modo que pueda realizar cambios sobre la aplicación y sobre la base de datos
j) Durante toda la vigencia del Contrato el PROVEEDOR deberá proporcionar todos los servicios de mantención necesarios para la operación y funcionamiento del SISTEMA DE EMISION DE PASAPORTES.
k) En el caso del software, el PROVEEDOR deberá proveer un equipo de trabajo con profesionales calificados, expertos en el SISTEMA DE EMISIÓN DE PASAPORTES (Atención de Usuarios, Back Office, Biometría y Gestión de Información, interoperabilidad con otros sistemas), con disponibilidad de hasta 1.500 horas para el caso de nuevos requerimientos solicitados por el Ministerio de Relaciones Exteriores.
l) Será responsabilidad del PROVEEDOR la habilitación del área asignada por el MRE para su funcionamiento, y de la implementación de las estaciones de trabajo para este personal.
m) El PROVEEDOR será responsable de todas las actualizaciones y mejoras del software provisto, que se requieran para el adecuado funcionamiento del SISTEMA DE EMISIÓN DE PASAPORTES.
n) El PROVEEDOR deberá proporcionar mantención preventiva y correctiva para todo el hardware del SISTEMA DE EMISIÓN DE PASAPORTES
o) El proveedor debe brindar el servicio de garantía por 5 años, en caso de errores en el desempeño de la aplicación, el proveedor deberá realizar todas las correcciones necesarias de los errores identificados en este período.

p) Además de la mantención del SISTEMA DE EMISIÓN DE PASAPORTES, el PROVEEDOR deberá implementar todos los cambios que se requieran en los procesos, procedimientos, prácticas, formularios y en los pasaportes, sin costo adicional para el MRE.

q) El PROVEEDOR deberá realizar una actividad permanente de supervisión y de análisis de la calidad, y cumplimiento de las normas y estándares y de la seguridad de los documentos de viaje.

r) En el caso que el Ministerio de Relaciones Exteriores detecte que la seguridad de los documentos se encuentra comprometida o que deduzca, como resultado del análisis del informe anual requerido en la sección "PASAPORTE ELECTRÓNICO", el PROVEEDOR estará obligado a formular recomendaciones sobre mejoras y/o cambios evolutivos que se podrían realizar a nivel de los materiales e insumos, de los procesos de producción y/o de personalización de los pasaportes, necesarios para recuperar el nivel de seguridad adecuado.

s) En caso de ser necesario, el PROVEEDOR deberá realizar la mantención post emisión de los documentos electrónicos.

t) El costo de envío de mensajes SMS por definir por el MRE para al menos un (01) mensaje por cada pasaporte emitido.

u) Proveer mil) especímenes de pasaportes electrónicos diplomáticos y especiales personalizados para difusión institucional los cuales no serán contabilizados como parte del total contratado (400.000).

RESPONSABILIDADES DEL PROVEEDOR EN LA TRANSICIÓN DE ENTRADA (MIGRACION)

a) Proveer el soporte de los sistemas operativos de los equipos a ser migrados durante la migración. El procedimiento se definirá en la fase de planificación.

b) Proveer el soporte de los aplicativos implementados por el proveedor durante la migración.

c) Ejecutar todas las pruebas técnicas pertinentes referidas únicamente a los servicios. Esta responsabilidad incluye la realización de las mismas, mantener un registro y la elaboración de los documentos correspondientes. Asimismo, todas las herramientas, instrumentos y equipos necesarios para la realización de las pruebas, serán otorgados por el Proveedor.

RESPONSABILIDADES DEL PROVEEDOR EN LA TRANSICIÓN DE SALIDA

a) El proveedor será responsable de aplicar las mejores prácticas en la realización de las tareas incluidas en el plan de trabajo presentado para ser llevadas a buen término, con la seguridad y confiabilidad, minimizando todos los riesgos dentro de los alcances de la presente propuesta.

b) El proveedor será responsable por el mantenimiento, salvaguarda y respaldo de las configuraciones (Sistema Operativo, redes y Aplicaciones) presentes en todos los servidores, sistemas de almacenamiento y demás Componentes de Hardware y Software hasta su entrega al MRE o quien designe este. En el caso que la entrega al futuro proveedor, sobrepase la fecha de culminación del contrato, se gestionará a través del proceso de control de cambios para la ampliación del servicio.

c) Dar las facilidades técnicas y de acceso al MRE.

d) Entregar las últimas copias de respaldo de la información tanto de las bases de datos, las aplicaciones, código fuente y configuración de los equipos del servicio.

e) Trasladar procedimientos y políticas de operación al MRE o a quien este designe.

PERSONAL DEL PROYECTO

El PROVEEDOR proporcionará todo el personal necesario para la implementación y puesta en operación del SISTEMA DE EMISION, como asimismo del acompañamiento a los funcionarios encargados de la operación del SISTEMA durante los 180 días al inicio de la entrada en operación

El proveedor deberá disponer de personal encargado de la administración de la Base de Datos del MRE, soporte y monitoreo central del sistema de producción de pasaportes. El servicio de administración deberá cubrir un horario de 24 horas x 7 días de la semana durante un periodo de 5 años, de los cuales 10 horas X 5 días deben ser ON SITE, en el local asignado por el MRE. Este personal brindará servicios de monitoreo, soporte de primer nivel y cambios solicitados por el MRE a la base de datos y a la aplicación de administración central.

El personal asignado deberá tener conocimientos de programación compatible con la aplicación central de producción de pasaportes, de modo que pueda realizar cambios sobre la aplicación y sobre la base de datos.

ADVERTENCIA SOBRE EL CONSUMO DE LIBROS

El proveedor deberá realizar el seguimiento de la producción, reportando el consumo de los pasaportes contratados. En caso que la proyección del proceso de producción consuma los 400.000 libros hasta un 70% del total antes del término del periodo de contratación, el Proveedor deberá emitir una advertencia al MRE para que se pueda realizar la Adenda de Contratación correspondiente para cubrir las proyecciones de la entidad

TRANSPORTE

El PROVEEDOR será responsable del transporte de todos los pasaportes personalizados y los repuestos desde su lugar de origen o las fábricas de personalización hasta las 111 Oficinas Consulares y la sede de expedición en Lima, como sea dispuesto por el Ministerio de Relaciones Exteriores.

La entrega de pasaportes electrónicos diplomáticos y especiales deberá realizarse con una frecuencia diaria (a excepción de los días declarados no laborables) entre las 9:00 y 16:30 horas al personal designado por el MRE. El MRE se reserva la facultad de solicitar pasaportes en cualquier otro horario en casos de emergencia.

La entrega de pasaportes comunes deberá realizarse entre las 9:00 y 16:00 horas (horario local del país destino).

HORAS DE DESARROLLO DE SOFTWARE

Para el caso de nuevos requerimientos solicitados por el Ministerio de Relaciones Exteriores después de la puesta en producción, el proveedor deberá considerar como mínimo una bolsa 1500 horas de desarrollo.

DIMENSIONAMIENTO DE LOS EQUIPOS

El proveedor deberá dimensionar la cantidad, capacidad y tamaño de los equipos a entregar en cada Sede de Expedición y en las Oficinas Consulares, en función de las capacidades y cantidades registradas en el presente documento.

INFORMACIÓN Al MRE EN CASO DE PERDIDA DE INSUMOS

En caso de pérdida o robo de los insumos durante el proceso de transporte o almacenamiento por parte del proveedor, éste será responsable de reponer los insumos, informar a el Ministerio de Relaciones Exteriores,

generar un informe indicando el código de serie de todos los insumos perdidos, incluyendo los rollos de laminado y los tramos de laminados perdidos (de ser el caso), asesorando al MRE en el registro en el inventario de insumos y en la base de datos de pasaportes emitidos, los números de serie de los libros perdidos o robados. Asimismo, el proveedor deberá hacer las denuncias policiales correspondientes y todos los demás trámites correspondientes que permitan la reposición de lo perdido o robado.

COSTO DE INSPECCIÓN DE CALIDAD A FÁBRICAS DE LIBROS DE PASAPORTES

Anualmente, un equipo multidisciplinario de mínimo 03 personas del Ministerio de Relaciones Exteriores y/o auditores externos, realizará visitas técnicas de inspección de calidad a las Fábricas de pasaportes; el costo de estas visitas y de la contratación de los auditores será cubierto por el Proveedor. En caso que la Fábrica, el proceso de fabricación o el producto fabricado no cumpla con los requerimientos descritos en el presente documento, el Ministerio de Relaciones Exteriores podrá resolver el contrato.

COSTO DE VERIFICACIÓN DE MUESTRAS POR LABORATORIOS

El MRE podrá enviar muestras de los pasaportes pre-impresos a laboratorios especializados seleccionados por el MRE cuando menos una vez al año, para su verificación, cuyo costo deberá ser asumido por el proveedor, los análisis y resultados deben incluirse en los informes de avance y estado del proyecto correspondientes, como también las medidas que se requieran tomar para solucionar las deficiencias que se hubiesen detectado.

ROLES Y RESPONSABILIDADES DEL PROVEEDOR EN LA ORGANIZACIÓN DEL PROYECTO

Para el desarrollo del servicio el proveedor designará diferentes recursos, quienes tendrán las responsabilidades que se detallan a continuación:

a) Director del Proyecto

Es el ejecutivo designado como el responsable de más alto nivel del proyecto, que tiene como misión velar por el cumplimiento del servicio. El Director y sus delegados tendrán la suficiente autoridad y atribución para resolver los conflictos que puedan poner en riesgo los objetivos, metas o resultados del servicio.

b) Gerente de Proyecto

Sus responsabilidades están relacionadas con la coordinación de las actividades entre el proveedor y el MRE, para notificar fallas, ejecutar las actividades y procedimientos acordados, mantener actualizado el manual de procedimientos, realizar la transición de los servicios, coordinar los cronogramas.

c) Servicie Manager

Es el encargado de Gestionar la operación del servicio in situ en el horario laboral del Ministerio de Relaciones Exteriores, con las siguientes responsabilidades:

- Gestionar los servicios, disponiendo de los recursos necesarios para que se ejecuten de acuerdo a lo previsto. Asimismo, monitoreando los indicadores de niveles de acuerdo de servicio establecidos.
- Realizar la gestión de los incidentes y requerimientos, para que estos sean atendidos oportunamente, Hacer que los servicios prestados cumplan los acuerdos de niveles de servicio establecidos.
- Asegurarse que el personal a cargo este propiamente entrenado, tenga las instrucciones, herramientas y metodología para realizar sus trabajos.
- Realizar la coordinación con el MRE para mantenimientos de equipos y software.
- Realizar las comunicaciones al MRE, ante cualquier incidente que afecten servicios relacionados a su operatividad.

- Elaborar informes mensuales de recomendaciones de acuerdo a los valores de indicadores de acuerdo de nivel de servicio alcanzado.

PENALIDADES

El Ministerio de Relaciones Exteriores podrá cobrar administrativamente penalidades al PROVEEDOR cuando éste no cumpla con sus obligaciones contractuales. el MRE podrá aplicar una penalidad por mora por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente o, de ser el caso, del monto del ítem que debió ejecutarse, en concordancia con el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Donde:

F = 0.25 para plazos mayores a sesenta (60) días calendario.

F = 0.40 para plazos menores o iguales a sesenta (60) días calendario.

Esta penalidad será deducida del pago final, o de los pagos parciales o mensuales; o si fuese necesario se cobrará del monto resultante de la ejecución de la Garantía de Fiel Cumplimiento.

Cuando se llegue a cubrir el monto máximo de la penalidad, el MRE podrá resolver el contrato por incumplimiento.

La justificación por el retraso se sujeta a lo dispuesto por la Ley de Contrataciones del Estado y su Reglamento, el Código Civil y demás normas aplicables, según corresponda, de la República del Perú.

La Ministerio de Relaciones Exteriores podrá cobrar penalidades al PROVEEDOR, por incumplimientos respecto de los siguientes ítems:

a) Atraso en la presentación de Informes, de Avance del Proyecto, de Calidad de Servicio, de Seguridad de los documentos.
b) Incumplimiento de Niveles de Servicio, de funcionamiento y de rendimiento, Plazos de implementación, de entrada en operación y de salida.

OTRAS PENALIDADES

Etapa de implementación:

MOTIVO: ETAPA DE IMPLEMENTACIÓN	PENALIDAD
Por cada día de atraso, en la entrega del Plan de Trabajo.	4 UIT *
Por cada día de atraso, en cada uno de los entregables de acuerdo al cronograma del Plan de Trabajo aprobado para su implementación en las sedes del Grupo Lima	2 UIT *
Por cada día de atraso, en cada uno de los entregables de acuerdo al cronograma del Plan de Trabajo aprobado para su implementación en las sedes del Grupo 1	1 UIT *
Por cada día de atraso, en cada uno de los entregables de acuerdo al cronograma del Plan de Trabajo aprobado para su implementación en las sedes del Grupo 2	0.75 UIT *
Por cambio de personal del PROVEEDOR sin autorización del MRE	10 UIT *
MOTIVO: ETAPA DE TRANSICIÓN DE SALIDA	**PENALIDAD**
Por cada día de atraso, en la entrega del Plan de Trabajo Transición de Salida.	4 UIT *
Por cada día de atraso, en cada uno de los entregables de acuerdo al cronograma del Plan de Trabajo del Plan de Salida aprobado por el MRE	2 UIT *

Donde (*) UIT: La UIT son las iniciales de Unidad Impositiva Tributaria y es un valor de referencia que se utiliza para determinar impuestos, infracciones, multas u otro aspecto tributario que las leyes del país establezcan. En la República del Perú, la UIT es fijada al inicio del año por el Ministerio de Economía y Finanzas.

Estas penalidades se calcularán de forma independiente a la penalidad por niveles de servicio de funcionamiento.

Estas penalidades serán deducidas de los pagos a cuenta o si fuese necesario se cobrará del monto resultante de la ejecución de las garantías de fiel cumplimiento o por el monto diferencial de propuesta.

Para el caso de la aplicación de OTRAS PENALIDADES detalladas en el punto 4.14.1., el valor de la UIT será el vigente a la fecha de la suscripción del ACTA consignando las observaciones del MRE o al momento de operado el incumplimiento; ello de acuerdo con lo dispuesto por el artículo 176° del Reglamento de la Ley de Contrataciones del Estado Peruano.

RESPONSABILIDADES DEL USUARIO FINAL

COORDINAR LOS ACCESOS A APLICACIONES

El MRE será responsable de coordinar los accesos a las aplicaciones de RENIEC, Migraciones, Sistema de Actividades Migratorias del El MRE.

PRUEBAS DE CALIDAD DE LOS PASAPORTES TERMINADOS

De manera periódica, el MRE realizará pruebas de calidad en todos los sistemas de personalización a nivel nacional. Los sistemas entregados e instalados por el proveedor deberán permitir inyectar solicitudes de pasaportes con datos de prueba para Pasaportes Electrónicos, los cuales deberán ser impresos y marcados como "inutilizados", de manera automática.

Estas muestras serán enviadas a un laboratorio de calidad especializado seleccionado por el MRE, cuyo costo deberá ser asumido por el proveedor. Los análisis y resultados deben incluirse en los informes de avance y estado del proyecto correspondientes, como también las medidas que se requieran tomar para solucionar las deficiencias que se hubiesen detectado.

La primera revisión deberá realizarse antes de la puesta en producción de la Solución Integral contratada. La revisión será realizada de manera semestral.

TAREAS RELACIONADAS CON LA MIGRACIÓN

Implementar los cambios de configuración si la migración de la plataforma de los sistemas del MRE lo requiriera. Dichos configuraciones deben ser entregadas previamente por el proveedor para su implementación.

Brindar la información disponible para que el proveedor pueda solicitar las configuraciones en la etapa de planificación.

PRUEBAS FUNCIONALES DE RECEPCIÓN DE APLICACIONES

Realizar por el personal del MRE las pruebas funcionales sobre las aplicaciones dentro del alcance del presente servicio. Si las pruebas funcionales fallan se debe recurrir al plan de contingencia o rollback para que el servicio o aplicación afectada no salga en vivo.

El MRE validará el protocolo del plan de pruebas de aceptación o conformidad de cada servicio.

PROTOCOLO DE INSPECCIÓN Y PRUEBAS DE RECEPCIÓN

Aprobar el documento "Protocolo de Inspección y Pruebas de Recepción" presentado por el proveedor.

INSPECCIÓN PROGRAMADA DURANTE LAS ETAPAS DEL PROYECTO

Durante el periodo del contrato el personal del MRE o auditores externos seleccionados por el MRE (01 persona) realizarán la inspección programada de tres Oficinas Consulares (a libre elección por parte del MRE) por año, donde el proveedor deberá cubrir los costos del transporte aéreo y la estadía.

CENTRO DE DATOS

El PROVEEDOR debera proveer el servicio de alquiler del Centros de Datos, principal y contingente, en la ciudad de Lima para ubicar los equipos de la infraestructura Tecnologica del centro de procesamiento durante un periodo de 4 años, para lo cual debera considerar lo siguiente como minimo:

- El centro de datos debera tener mínimo la certificacion de TIER III
- Alquiler de espacio necesario en el Centro de Datos principal contratado por el periodo de servicio el cual debera ser dimensionado por el PROVEEDOR, ademas de un 20% adicional para crecimientos futuros.
- Servicio de interconexion por Fibra Optica entre el Centro de Datos actual del MRE y los Centros de Datos contratados (la cantidad de hilos debera ser dimensionada por el PROVEEDOR), por el tiempo que dure el servicio (4 años). La conexión sera cifrada por canales VPN.
- Todo el Equipamiento necesario de Comunicaciones y de seguridad perimetral en el Centros de datos contratado.
- El PROVEEDOR administrara todo el equipamiento de servidores y comunicaciones durante el periodo del contrato.

ROLES Y RESPONSABILIDADES PARA LA ORGANIZACIÓN DEL PROYECTO

El MRE designará los siguientes ejecutivos responsables de la administración del proyecto:

a) Director del Proyecto
b) Gerente de Proyecto
c) Líder de Área Usuaria
d) Staff TI de El MRE.

Adicionalmente, El MRE definirá las personas que considere necesarias para cubrir las responsabilidades asignadas.

EXCEPCIONES A LAS OBLIGACIONES DEL PROVEEDOR

Será responsabilidad del MRE proporcionar:

e) El PROVEEDOR debe presentar su propuesta, así como cualquier correspondencia escritas en el idioma español.
f) Las empresas que forman parte de un consorcio no pueden ser incluidos en más de una propuesta diferente. Una empresa no puede enviar una propuesta como contratista principal o como joint-venture y ser incluido en otra propuesta como parte de otro consorcio.
g) Otros antecedentes a solicitud del MRE. (Boletin Comercial, otros).
h) Experiencia de haber gestionado o haber participado en la gestión de la producción y personalización de pasaportes electrónicos en al menos dos proyectos en los últimos 10 años, con una emisión mínima de 300.000 pasaportes en un año o, un proyecto, en los últimos 10 años, con una emisión mínima de 1.000.000 de pasaportes biométricos en un año.
i) Copia simple del Registro Nacional de Proveedores (RNP) vigente.

CONTENIDO DE LA PROPUESTA

CONTENIDO DE LA PROPUESTA

Aspectos Generales

Podrán presentarse a esta selección las personas naturales o jurídicas cuyo giro social comprenda los servicios solicitados en estas Bases y que, en forma individual o como consorcio, cumplan con los requisitos exigidos, lo que deberá ser acreditado en su oportunidad, con la documentación correspondiente.

No obstante, en la postulación de consorcios, cada propuesta deberá ser presentada por una única persona jurídica a la que se denominará el "PROVEEDOR". Dicha persona jurídica, cuando forme parte de un consorcio, actuará por sí y en representación del resto de los integrantes de éste y será la única responsable de la propuesta ante el MRE, independientemente de cualquier alianza o acuerdo que haya efectuado con otras empresas con el objeto de presentarse a esta selección.

El PROVEEDOR asume plena responsabilidad frente al MRE por su propuesta técnica y económica, por los términos de referencia y por lo establecido en el contrato, en tal sentido las relaciones internas que pudiera tener el PROVEEDOR con terceros no lo exime de las responsabilidades y obligaciones asumidas ante el MRE.

Precio y Forma de Pago

El PROVEEDOR podrá solicitar hasta un 30% del valor del contrato pago como adelanto.

Se realizará un pago del 5% del valor de lograrse la expedición de pasaportes electrónicos en las 04 Oficinas Consulares de mayor demanda, localizadas en la Unión Europea (Madrid, Milán, Barcelona y Ámsterdam).

Se realizará un pago del 5% del valor del contrato a la puesta en operación del servicio (finalización de la implementación de los sistemas y de la habilitacion de las 111 Oficinas Consulares y sedes de expedicion, y firma de conformidad), y luego se realizarán pagos mensuales iguales por el servicio de administracion mantenimiento y gestion de equipos, entrega de insumos, mantenimiento correctivo y evolutivo del sistema valorizados en 1/36 avo del restante del contrato. Al finalizar la transisión de salida, al logro de la conformidad del MRE, se realizará el pago del 10% restante.

a) Las Oficinas de atención de usuarios
b) Los servicios necesarios para el funcionamiento de sus dependencias (agua potable, electricidad y teléfonos de transmisión de voz servicio local medido y dentro de la red del MRE)
c) No se considerará responsabilidad del PROVEEDOR cualquier falla de los sistemas externos interconectados.

CALENDARIO DE IMPLEMENTACIÓN

PLAN DE IMPLEMENTACIÓN

El Plan de Implementación, considerando el cumplimiento de todas las actividades descritas en el presente documento, se presentará dentro de un plazo de 21 días calendario contados luego de la firma del contrato. Este Plan deberá ser aprobado de manera expresa por El MRE.

ACOMPAÑAMIENTO DEL PROVEEDOR

El plazo del periodo de acompañamiento deberá realizarse durante 180 días calendario posteriores a la puesta en producción de la emisión del pasaporte electrónico.

REPORTES DE SEGUIMIENTO

Los reportes de seguimiento y monitoreo deberán implementarse a los 30 días de inicio de la puesta en producción de la emisión del pasaporte electrónico.

TRANSICIÓN DE SALIDA

Las coordinaciones para las actividades de transición de salida deberán iniciarse con 4 meses de anticipación al término del periodo contractual.

ENTRENAMIENTO DEL PERSONAL

Las fechas de entrenamiento del personal deberán coordinarse con el Ministerio de Relaciones Exteriores.

CALIFICACIONES REQUERIDAS

REQUISITOS

El PROVEEDOR debe cumplir con los siguientes requisitos:

a) Presentar una declaración jurada con firma legalizada ante Notario de no encontrarse comprendido en ninguna de las prohibiciones indicadas en la Ley de Contrataciones del Estado de la República del Perú y su Reglamento, así como en sus normas modificatorias correspondientes.
b) Presentar una declaración jurada de cumplimiento de los términos de referencia.
c) No tener vigente los efectos de una declaratoria de quiebra
d) Tratándose de consorcios, la propuesta deberá ser presentada comprometiendo legalmente a todos los integrantes del consorcio en forma mutuamente solidaria conforme al FORMATO de Compromiso Solidario de Consorcio

Estos pagos se realizarán a la presentación de la copia de Ficha del Registro Único de Contribuyentes (RUC), con el comprobante de pago respectivo.

Conformidad

La conformidad requiere del informe del funcionario responsable del área usuaria quien deberá verificar la calidad, cantidad y cumplimiento de las condiciones contractuales, debiendo realizar las pruebas que fueran necesarias.

La documentación que sustenta la conformidad será la siguiente:

a) Informe del área usuaria conteniendo la conformidad
b) Otros documentos necesarios que sustenten la conformidad

De existir observaciones se consignarán en el acta respectiva, indicándose claramente el sentido de estas, dándose al PROVEEDOR un plazo prudencial para su subsanación, en función a la complejidad del bien o servicio. Dicho plazo no podrá ser menor de dos (2) ni mayor de diez (10) días calendario. Si pese al plazo otorgado, el PROVEEDOR no cumpliese a cabalidad con la subsanación, el MRE podrá resolver el contrato, sin perjuicio de aplicar las penalidades que correspondan.

Este procedimiento no será aplicable cuando los bienes y/o servicios manifiestamente no cumplan con las características y condiciones ofrecidas, cuyo caso el MRE no efectuará la recepción, debiendo considerarse como no ejecutada la prestación, aplicándose las penalidades que correspondan.

Plazo de duración del servicio

El servicio tendrá una duración de tres (3) años, contados desde el día siguiente de la puesta en operación del servicio (finalización de la implementación a nivel nacional y firma de conformidad).

Ampliación de plazo

Procede la ampliación del plazo de operación del contrato en los siguientes casos:

1. Cuando se apruebe el adicional, siempre y cuando afecte el plazo. En este caso, el PROVEEDOR ampliará el plazo de las garantías que hubiere otorgado.
2. Por atrasos o paralizaciones no imputables al PROVEEDOR.
3. Por atrasos o paralizaciones en el cumplimiento de la prestación del PROVEEDOR por culpa del MRE y,
4. Por caso fortuito o fuerza mayor.

El PROVEEDOR deberá solicitar la ampliación dentro de los siete (7) días hábiles a la notificación de la aprobación del adicional o de finalizado el hecho generador del atraso o paralización.

El MRE debe resolver dicha solicitud y notificar su decisión al PROVEEDOR en el plazo de diez (10) días hábiles, computado desde el día siguiente de su presentación. De no existir Pronunciamiento expreso, se tendrá por aprobada la solicitud del contratista, bajo responsabilidad del Titular del MRE.

Domicilio del PROVEEDOR

La persona natural o jurídica o consorcio que se adjudique la selección, deberá constituir domicilio legal en la ciudad de Lima, Perú, para todos los efectos legales derivados del Contrato.

Solución de Controversias y Legislación Aplicable

El Contrato que celebre el Ministerio de Relaciones Exteriores con el PROVEEDOR, se regirá por las leyes de la República de Perú.

Propuesta Económica

La Propuesta Económica debe indicar específicamente, en valores totales incluido el Impuesto General a las Ventas (IGV) del 18% y todo impuesto de ley aplicable por la normativa de la Republica del Perú. Debe considerar todos aquellos costos que incidan en la prestación del servicio.

Propuesta Técnica

La Propuesta Técnica debe incluir una descripción detallada de cada elemento, a fin de cumplir con los requerimientos del MRE, que han sido solicitados en estos Términos de Referencia. También deberá incluirse la justificación del diseño de la solución propuesta.

El PROVEEDOR debe describir en detalle los servicios solicitados, componentes de software y configuraciones de hardware, prácticas, procesos, procedimientos o cualquier componente de la solución ofertada.

La propuesta técnica del PROVEEDOR deberá incluir lo siguiente:

Componentes propuestos por el PROVEEDOR para el proceso de emisión del Pasaporte Electrónico:

Describir los componentes según cada etapa descrita en la sección "Proceso de emisión del pasaportes electrónico" del presente documento.

Características de la aplicación central de procesamiento y firma digital:

- Funcionalidades de la aplicación
- Capacidad de integración a bases de datos
- Módulo de preparación de datos
- Módulo criptográfico redundante, indicando cantidad, marca y modelo
- Capacidad de rendimiento del servidor de firma digital
- Características de rendimiento del hardware propuesto

Características del sistema de personalización que será utilizado por el proveedor:

- Número de impresoras, marca y modelo por cada sede de expedición
- Capacidad de impresión por hora de cada impresora
- Controles para el control de calidad
- Tintas a emplear
- Repuestos
- Insumos que serán provistos y periodicidad de entrega

Características de los puntos de captura:

- Números de cámaras, marca, modelo, indicando dos proveedores diferentes que brinden el servicio.
- Número de lectores de huellas, marca, modelo, indicando dos proveedores diferentes que brinden el servicio (soporte).
- Diseño de los controles de seguridad contra robo en las Oficinas Consulares indicando marca y modelo.
- Presentar plan de mantenimiento de impresoras, camaras y lectores de huella durante los 3 años de duración del contrato.
- Presentar dos proveedores distintos que suministran los equipos de captura.

Descripción de las medidas de seguridad a ser incorporadas en el documento del pasaporte electrónico:

- Carátula, tapa, contracarátula, contratapa
- Hoja de datos (incluye laminado), Hojas de Visado
- Libro, Acabado, Numeración, Lámina

Características del chip:

- Capacidad de memoria
- Estructura lógica de datos
- Sistema Operativo
- Velocidad de transmisión
- Capacidad de procesamiento

Características de la aplicación de control de insumos y stock:

- Funcionalidades
- Rendimiento

Aseguramiento de calidad del fabricante de los documentos:

- El PROVEEDOR debe describir sus procesos de aseguramiento de calidad y seguridad (organización física y lógica).
- El proceso de control de calidad debe estar enfocada en todos los estados de producción que pueden tener impacto negativo en la calidad y seguridad del producto final, entre los que se puede mencionar:
  - Manejo y consistencia de la materia prima usada para la fábricación de los pasaportes, por medio de un estricto control de las entradas del proceso;
  - La puesta a punto de las máquinas usadas durante la producción de la libreta del pasaporte electrónico;
  - Las pruebas de consistencia y estabilidad por medio de pruebas de simulaciónde envejecimiento.

El PROVEEDOR debe presentar la configuración propuesta de AFIS 1:1, indicando los siguientes datos:

- Escala y granularidad para la calidad de las impresiones dactilares
- Tasa de falsa aceptación (FAR) en porcentaje y por millón.
- Tasa de falso rechazo (FRR) en porcentaje y por millón
- Tasa de aceptación positiva (TAR=1-FRR) para una tasa de falsa aceptación (FAR) de 0,0001% o uno (1) en un millón (1.000.000)

- Curvas de comportamiento para las tasas indicadas
- Tiempo de respuesta mínimo y máximo.

El PROVEEDOR debe presentar la configuración propuesta de AFIS 1:N, indicando los siguientes datos:

- Escala granularidad para la calidad de las impresiones dactilares
- Tasa de falsa coincidencia (FMR) en porcentaje y por millón
- Tasa de falsa no coincidencia (FNMR) en porcentaje y por millón
- Exactitud(1-FNMR)
- Curvas de comportamiento de las tasa indicadas
- Indicadores de calidad de la selección
- Mejor correspondencia (best fit)
- Segunda correspondencia (second fit)
- Tiempo de respuesta mínimo y máximo.
- Plan de mantenimiento propuesto durante los 3 años
- Servicio de soporte y garantía
- Características del servicio de administración de base de datos
- Propuesta de adecuación del almacén central de insumos
- Propuesta de preparación de los ambientes de captura en las Oficinas Consulares
- Sistema de seguridad en las Oficinas Consulares
- Cantidad, características y dimensionamiento del equipamiento del centro de procesamiento
- Características y dimensionamiento de la SAN
- Características y dimensionamiento del servicio y sistema de almacenamiento en cinta
- Características y controles del acondicionamiento del centro de procesamiento sala de servidores y monitoreo
- Características del centro de video vigilancia propuesto
- Características del sistema de control de producción propuesto
- Cursos de entrenamiento y capacitación del personal
- Características del grupo electrógeno
- Especialistas requeridos para la implementación del sistema de personalización y emisión descentralizada del pasaporte electrónico (Director de Proyecto, Gerente de Proyecto y Especialista PKI)
- Servicio de acompañamiento
- Servicio de gestión del proyecto

GLOSARIO

- **Administrador del Centro de Procesamiento:** Personal asignado por el Proveedor o por el Ministerio de Relaciones Exteriores, que debe supervisar y administrar las funcionalidades del sistema centralizado y de los sistemas de personalización a nivel nacional.
- **Aplicación Central de Procesamiento y firma digital:** Aplicación encargada de controlar el proceso integro de solicitud, captura de datos, interconexión con otras fuentes de consulta y con las Oficinas Consulares para el control de los sistemas de personalización.
- **Auditoría y Trazabilidad:** Las herramientas que presente el sistema para poder llegar a determinar los pasos seguidos por un proceso o una acción dentro del sistema.

- **Área de Monitoreo:** Área del Centro de procesamiento conformada por dos sistemas: el Sistema central de video vigilancia y el Sistema de control de producción.
- **Base de Datos de Extranjeros:** Base de Datos de Control Migratorio
- **Base de Datos de Pasaportes Emitidos:** Base de Datos generada por la aplicación central de procesamiento y firma digital, que contiene todos los datos biográficos, huellas, imágenes, y rubricas de los ciudadanos que han adquirido un pasaporte electrónico en el Ministerio de Relaciones Exteriores.
- **Certificado de Firma País:** Certificado digital empleado para la firma de los certificados del Firmante de Documentos.
- **Certificado del Firmante de Documentos**: Certificado Digital empleado para la firma del contenido del CHIP de los pasaportes electrónicos conforme al estándar ICAO, Documento 9303.
- **Centro de procesamiento:** Centro de datos donde se realiza el procesamiento de los pasaportes electrónicos: generación de la firma desatendida y la firma del contenido del CHIP. Esta conformado por la sala de Servidores y Área de Monitoreo.
- **Firma desatendida:** Firma digital que se realiza en un servidor de manera automática al recibir una transacción exitosa de un proceso funcional, ningún administrador u operador de la aplicación de firma puede alterar o influir en la realización de la firma.
- **Hoja de Datos:** Hoja laminada que forma parte del libro del pasaporte electrónico en la cual se visualizan los datos biográficos del titular del documento y los datos contenidos en la Zona de Lectura Mecánica conforme a lo definido en el Documento 9303 de la ICAO.
- **Módulos de personalización:** Aplicación de software que permite la integración entre los Puntos de Captura, las impresoras en las Sedes de expedición a nivel nacional y las Bases de datos de consulta.
- **Objeto de seguridad:** Componente que forma parte de la estructura de datos del pasaporte electrónico, que va contenido en el CHIP y que a su vez contiene la firma digital a nombre de el Ministerio de Relaciones Exteriores.
- **Operador:** Personal de el Ministerio de Relaciones Exteriores responsable de ejecutar las funciones correspondientes a la recepción de la solicitud de pasaportes, captura de datos, personalización para la emisión de pasaportes en las Sedes de Expedición a nivel nacional.
- **PROVEEDOR:** PROVEEDOR seleccionado contractualmente para la implementación, administración y soporte de la Solución integral.
- **Puntos de captura:** Puestos de atención que se encuentran en cada Sede de expedición , donde se realizara la toma de datos a incluir en el Pasaporte electrónico.
- **Punto de entrega y verificación**: Puestos de atención que se encuentran en cada Sede de expedición, donde se realizara la verificación de calidad y entrega del Pasaporte electrónico.
- **Servicio de operación:** Servicio de soporte y administración brindado por el proveedor en la etapa de producción del servicio de emisión de pasaportes electrónicos.
- **Servicio de transición**: Periodo de implementación y despliegue de los sistemas a nivel nacional, incluye el entrenamiento del personal y transferencia de conocimiento.
- **Sistema Central de video vigilancia:** Sistema integrado de monitoreo que permita visualizar en vivo las imágenes de las cámaras de video vigilancia a nivel nacional.
- **Sistema de control de producción**: Sistema integrado que muestra el desempeño de la producción de pasaportes electrónicos, estado de insumos y buen funcionamiento de los sistemas a nivel nacional.
- **Sedes de expedición:** (Agencia Descentralizada de Pasaportes): Locales distribuidos de el Ministerio de Relaciones Exteriores donde se emiten los pasaportes mecanizados, y donde se emitirán los pasaportes electrónicos.
- **Sistema Integrado de El MRE(SIM)**: Solución de software que automatiza los procedimientos operativos de el Ministerio de Relaciones Exteriores.

- **Sistemas de personalización:** Sistemas de software, hardware y componentes mecánicos que realizan la personalización de los pasaportes electrónicos: impresión, laminado, control de calidad, registro de auditoria, . Se ubican en cada Sede de expedición.
- **Sala de servidores:** Área del Centro de procesamiento destinada a albergar los equipos servidores y HSM, encargados de generar la firma desatendida y la firma del contenido del CHIP.
- Solución integral: Solución que abarca la implementación y entrega de todos los sistemas, servicios, procesos, personal y componentes descritos en el presente documento.
- **Transición de Entrada:** La transición de entrada abarca todas las acciones donde el proveedor deberá desarrollar las políticas y acciones de la migración al nuevo sistema.
- **Transición de salida:** La transición de salida es la transición que abarca todas las acciones que realiza el proveedor para transferir el conocimiento, el control y administración de la solución a el Ministerio de Relaciones Exteriores o a otro proveedor asignado, se aplica en caso de termino de contrato o de Resolución Contractual debido a incumplimiento.
- **Fábricas de Personalización:** Instalación en cada Sede del MRE destinada a la personalización del pasaporte electrónico.

ANEXO 1: ESPECIFICACIONES TECNICAS MINIMAS DE LOS EQUIPOS DE ESCRITORIO PARA LOS PUNTOS DE CAPTURA DE DATOS Y ENTREGA DE PASAPORTES

	Características	Solicitud
1	EQUIPOS BASE	Tipo Small Desktop (dimensiones máximas 40x12x43.5 centímetros), se pueden aceptar equipos con especificación tipo "Tool-less". Se aceptarán equipos Small Form Factor, mientras sus medidas se encuentren dentro de las dimensiones máximas exigidas.
2	Procesador	Puntuación mínima: 7.7, en cálculos por segundo. El procesador deberá de la última generación disponible de la marca en el mercado. (Intel 3era generación o AMD APU)
3	Soporte de virtualización por hardware	Si
4	Memoria RAM	Mínimo de 8 GB DDR3 1333 MHz expandible a 16 GB
5	Disco Duro	Mínimo 320 GB SATA III con 7.200 RPM
6	Unidad Óptica	Lectora de DVD
7	Ranuras de expansión	1 PCI, 1 PCI Express (Libres)
8	Puertos	Debe tener 2 puertos seriales integrados en el Mainboard. Los puertos seriales podrán estar integrados en la parte posterior del equipo y uno (01) de ellos podrá ser instalado en una ranura o calado hecho para este propósito en el case, mediante un adaptador (cable) que se conecte a la Mainboard. Se aceptarán puertos seriales instalado en un slot PCI del equipo de cómputo siempre y cuando el número de puertos PCI y PCI Express libres sean los solicitados. Un mínimo de 8 puertos USB, de los cuales 2 de ellos son frontales y 6 deben ser posteriores.
9	Teclado	USB de membrana, de 102 o 104 teclas idioma castellano (incluyendo letra "ñ" y tilde). Indicadores luminosos de estado. No inalámbrico.
10	Mouse	USB laser o tipo óptico. Dos botones y rueda scroll. No inalámbrico.
11	Gráficas	Integrado de por lo menos 256 MB Video Compartido, con salida VGA y/o DVI. Si la salida fuera solamente tipo digital, el monitor (componente) debe tener también este tipo de conector digital. Deberá ser compatible con el estándar DirectX 11 de Microsoft.
12	Tarjeta de red	10/100/1000 Gigabit Ethernet integrada

	Características	Solicitud
13	Forma de Case	Para trabajo Horizontal y vertical indistintamente
14	Drivers necesarios para el correcto funcionamiento de la microcomputadora	Si
16	Incluir todos los cables necesarios para su funcionamiento con conectores planos con toma a tierra	Si
17	Fuente de Poder 110-220 auto voltaje	Si, 240 W Mínimo, 60 Hz, con corrección activa del factor de potencia y 85% de eficiencia.
18	Audio Integrado (parlante interno incorporado)	Si
19	Chip de Seguridad integrado a la placa que permita la encriptación de datos mediante hardware y software	Sí, que cumpla estándar TPM 1.2
20	Case con llave física	Si, o en su defecto el case debe contar con un sistema de seguridad mediante el cual se pueda asegurar la apertura del equipo mediante un cable de seguridad con seguro tipo Kensington con clave de seguridad de por lo menos cuatro dígitos.
21	Sistema Operativo	Windows 8 Professional 64 bits (OEM) en español, instalado. Incluye CD ó DVD de instalación o recuperación en partición del disco duro.
22	Software Ofimática	Licencia de Cliente Antivirus con actualización centralizada.

	Características	Solicitud
23	Administration out of band mediante hardware (DASH)	Habilitada
23	Monitor	Monitor LED de 18.5" con una resolución por lo menos de 1366x768, con aspect ratio 16:9, con puerto VGA y DVI. Altura máxima respecto a la mesa incluyendo la base de 38 cm.

ANEXO 2: ESPECIFICACIONES MINIMAS DE LOS SERVIDORES

CHASSIS DE SERVIDORES BLADE	
Cantidad	La cantidad Deberá ser dimensionado por el PROVEEDOR el cual deberá tener en cuenta que hay Centro de Datos Principal y Un Centro de Datos de Contingencia
Formato	Rack 10u como máximo
Soporte de servidores	El chasis debe soportar configuraciones que combinen servidores blade con procesadores de arquitectura x86 de 2 y 4 procesadores físicos (eight-core) y servidores blades con procesadores de arquitectura EPIC/RISC de 64bits. El chasis debe soportar al menos 16 servidores tipo blade de dos procesadores físicos en tecnología INTEL y AMD (x86)
Conectividad LAN	El chasis deberá soportar la instalación de al menos 2 módulos redundantes de interconectividad de Ethernet hacia la infraestructura principal de redes. Estos módulos deberán permitir la conectividad de todos los blades instalados (10GbE) sin impactar el rendimiento general de los blades o de la red. Los módulos de ethernet deberán contar con al menos 2 puertos 10GbE (SR) y 2 1GbE (rj45) uplinks con el fin de reducir el cableado necesario. Estos módulos deberán soportar redes virtuales por puerto físico del servidor y permitir administrar las direcciones físicas (MAC Address) del mismo asignado a cada red virtual. Deberá soportar la agregación (trunking) de conexiones hacia la infraestructura principal de redes. La administración del módulo deberá ser transparente para el administrador de redes. Estos módulos de interconectividad de Ethernet deberán de ser compatibles con los switches actuales de la compañía. El chasis debe estar en capacidad de soportar Switch LAN de 40GbE
Conectividad SAN	El chasis deberá soportar la instalación de al menos 2 módulos redundantes de interconectividad de Fibra hacia los switches principales de la SAN (del cliente). Estos módulos deberán permitir la conectividad de todos los blades que cuenten con tarjeta HBA de fibra. Los módulos de SAN deberán contar con al menos 4 puertos de 8Gb con el fin de reducir el cableado necesario. Estos módulos deberán soportar zonas virtuales por puerto físico del servidor y permitir administrar las conexiones físicas (WWN) de manera dinámica a cada conexión virtual. La administración del módulo deberá ser transparente para el administrador de la SAN.
Fuentes de poder y ventiladores	El chasis debe poseer fuentes de poder de al menos 2400 watts y ventiladores, tanto fuentes como ventiladores deben ser redundantes, integrados en el chasis, y cambiables en caliente. Deberán permitir ser configuradas N+N.

CHASSIS DE SERVIDORES BLADE	
Funcionalidades	El chasis deberá contar con indicadores físicos que permitan monitorear el estado de los diferentes componentes que alberga el chasis. Los servidores sean capaces de guardar un log con todos los cambios de hardware ocurridos en el mismo. En caso de falla del servidor, sea posible tener acceso a este log de forma remota y sin necesidad de sistema operativo en el servidor dañado. Que este log mantenga los cambios ocurridos de los últimos doce meses.
Administración y gestión	Incluir el software y todas las licencias necesarias que permitan la administración tanto los equipos Blade como del enclosure. Este software de administración debe de tener al menos las siguientes características: - Software que permita la administración y manejo de servidores Blades (Sistema operativo, aplicaciones, actualizaciones de drivers, obtener y aplicar imágenes del software instalado en el servidor). - Encendido y administración remota gráfica del Servidor Blade; independientemente del sistema operativo. - Proveer acceso detallado a problemas de fallas del sistema e información de rendimiento del sistema. - Gráficamente proveer el control completo del servidor desde un sitio remoto. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización remota de un servidor o grupo de servidores. - Capacidad de crear imágenes de un servidor, almacenarla y aplicarla bajo solicitud del administrador. - Capacidad de "Rip and Replace" es decir que al fallar uno de los blades se pueda extraer de su "slot", en su lugar insertar otro y automáticamente el nuevo blade herede las direcciones (MAC y WWN) del servidor que falló. Para que sea configurado en forma idéntica de cómo estaba el servidor dañado. - Capacidad de instalar un servidor en base a una imagen de un servidor existente. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente independiente del sistema operativo. - Administración de máquinas físicas y virtuales desde una misma consola de administración. - Incluir software para la migración de sistemas operativos y datos existentes en la compañía a estos nuevos servidores blades. - Los servidores deberán ser capaces de poder monitorear su salud remotamente, componentes de hardware básico como procesadores, fuentes de poder, ventiladores, memoria y discos duros. Deberán mandar alertas sin necesidad de tener cargado un sistema operativo en los servidores. - Software que permita monitorear contratos de garantías existentes y mande alertas antes de que estos contratos expiren desde la misma consola de administración. - Poder monitorear consumo de energía del chasis, como los servidores internos. Que esta misma herramienta te permita poder configurar el máximo consumo de energía por servidor o chasis.
Garantía y soporte	Tres años 24x7 con seis horas de tiempo de reparación

CHASSIS DE SERVIDORES BLADE	
Servicio de instalación	Debe ser ejecutado por personal certificado por el fabricante

SERVIDOR(ES) BLADE	
Cantidad	La cantidad de Servidores deberá ser dimensionada por el PROVEEDOR para albergar EL SISTEMA DE EMISION DE PASAPORTES ELECTRONICO durante el periodo del servicio (3 años) y se debe considerar servidores para el centro de Datos Principal y Centro de Datos de contingencia
Formato	Blade
# Procesadores Instalados	**Cantidad dimensionada por el PROVEEDOR deben ser Intel v3**
Máximo # de procesadores soportados	Dos o Cuatro (deberá ser dimensionamiento por PROVEEDOR)
Memoria RAM Instalada	**64GB o superior (deberá ser dimensionado por el PROVEEDOR)**
Máxima RAM soportada	512GB o superior ((deberá ser dimensionado por el PROVEEDOR)
Slot de memoria	Mínimo 16 Slot de memoria como mínimo
Puertos de red	Dos de 10GbE (FCoE, TCP/IP y iSCSI) y debe soportar (opcionalmente) puertos de 40GbE
Controlador RAID	SAS, debe soportar RAID 0 y 1 con 512MB de memoria Flash-Backed Write Cache para evitar perdida de datos y debe contar con las siguientes características: • Aumentar discos al arreglo en caliente • Migrar de nivel de RAID en caliente • Aumento de la capacidad del RAID en caliente • Actualización de firmware en caliente Garantía pre-falla
Disco Duro instalados	Dos discos de 300GB 6G SAS 15K rpm SFF configurados en RAID 1
Puertos de FC	Dos puertos de 8Gb
Slot de expansión	Mínimo dos
Interfases	Slot Micro SDHC: 1 Puerto USB 2.0: 1

Certificaciones	ACPI 2.0 Microsoft® Logo certifications USB 2.0 Support IPMI 2.0 Secure Digital 2.0 TPM 1.2 Support IEEE (specific IEEE standards depending on Ethernet adapter card(s) installed) Advanced Encryption Standard (AES) Triple Data Encryption Standard (3DES) SNMP SSL 2.0 DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) Active Directory v1.0 PCIe 3.0
Seguridad	Power-on password Administrator's password Keyboard password (QuickLock) SSL encryption Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser, CLP and XML scripting interface AES and RC4 encryption of video External USB port enable/disable Network server mode Serial interface control Advanced Encryption Standard (AES) Intel® Advanced Encryption Standard-New Instructions (AES-NI)
Administración remota	Debe permitir el acceso de hasta tres sesiones en simultaneo Implementación de servidor Control de energía Revisión del estado del servidor Acceso vía: Browser y línea de comandos Seguridad: AES y RC4 Puerto dedicado
Software de Gestión	Despliegue y migración de servidores (P2P, P2V y V2V) Análisis del rendimiento del servidor alertando cuellos de botella. Análisis predictivo de falla Optimización del consumo de energía Integración con VMware vCenter y Microsoft System Center
Garantía y soporte	Tres años 24x7 con seis horas de tiempo de reparación

Servicio de instalación	Debe ser ejecutado por personal certificado por el fabricante

ANEXO 3: ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SISTEMA DE ALMACENAMIENTO

CARACTERÍSTICAS	DESCRIPCIÓN
Fuente de Poder	Redundantes (Configuración N+1)
Ventiladores	Redundantes (Configuración N+1)
Tecnología	Fibre Channel
Arquitectura	Se precisa que cuente con una arquitectura unificada SAN/NAS en un par de controladoras como mínimo.
Número de controladoras activas y redundantes entre si	2 controladores con por lo menos 40Gb de memoria caché nativa en total. No se aceptará memoria emulada.
Memoria cache	La memoria cache no deberá estar basada en discos de estado sólido o flash. Una batería de respaldo en cada controlador que permita preservar la información en memoria cache, en caso de falla no planeada del fluido eléctrico u otro mecanismo de protección de la memoria cache (mínimo 96 horas).
Conectividad SAN	Se deberá de incluir como mínimo (04) puertos fibra canal de 8Gbps cada uno. Cada uno de los puertos fibra canal indicados debe poder conectarse en modalidad FC-switch (SAN) y tener la capacidad de conectarse directa o a través de la SAN con los servidores. Cada uno de los puertos fibra canal indicados debe incluir un cable de fibra LC-LC de un mínimo de 5 metros de longitud, compatible con la solución.
Conectividad NAS	Se deberá de incluir como mínimo (04) puertos Ethernet de 1Gb para conectividad a la red LAN para brindar servicios de NAS
Tipo de discos soportados	SAS de 10Krpm, 15krpm; NL-SAS o SATA de 7.2Krpm y discos de estado sólido (SSD) Debe incluir licenciamiento ilimitado para la administración al total de su capacidad de crecimiento sin necesidad de licenciamiento adicional
Mantenimiento microcódigo de las controladoras	Los procesos de upgrade de microcódigo del arreglo de discos debe realizarse sin interrumpir el funcionamiento

Escalabilidad	Capacidad de escalar con gabinetes de expansión adicionales hasta 240 discos
Niveles de RAID	El sistema de almacenamiento de discos magnéticos debe incluir la capacidad de definir arreglos de discos magnéticos de tipo RAID 0, RAID 1, RAID 5 y RAID 6 como mínimo; no se aceptarán otro tipo de arreglos que no sean estándares de la industria.
Capacidad total instalada en el almacenamiento	La cantidad necesaria para albergar EL SISTEMA DE EMISION DE PASAPORTES ELECTRONICOS por el periodo de tres (03) años, y esos deberán ser configurados en RAID 5, de 600GB c/u de 10,000RPM. El PROVEEDOR deberá considerar el equipamiento y/o componentes necesario para el centro de Datos Principal y Centro de Datos de Contingencia
Gabinete de discos	El PROVEEDOR deberá dimensionar la cantidad de gabinetes necesarios para albergar el almacenamiento requerido por EL SISTEMA DE EMISION DE PASAPORTES ELECTRONICOS por el periodo de tres (03) años. El PROVEEDOR deberá considerar los gabinetes necesarios para el centro de Datos Principal y Centro de Datos de Contingencia
Conectividad de gabinetes de discos	Cada controlador (2 en total) debe tener conexiones redundantes hacia cada uno de los gabinetes de discos.
Conectividad	El sistema de almacenamiento debe contar el licenciamiento perpetuo para la conexión del total de servidores soportados.
Licenciamiento de software de administración	Se debe incluir la licencia perpetua de software de administración, de interface gráfica. Esta licencia debe tener la cobertura para administrar la capacidad total soportada del sistema de almacenamiento sin limitar el número de servidores a conectar a éste ni la cantidad de discos soportados por el arreglo. Debe tener también la capacidad de monitorear el nivel de rendimiento o performance del sistema de almacenamiento.
Sistemas Operativos	El arreglo de discos ofertado debe incluir las licencias necesarias que permitan la conectividad de servidores operando con sistemas operativos Windows 2003 o 2008 32/64bits, VMWare ESX Server 3.X y versiones posteriores, Linux, IBM-AIX, HP-UX, SUN Solaris, XEN como mínimo.

Funcionalidades requeridas en el software de administración	Definir arreglos RAID de discos físicos sin interrumpir el funcionamiento del sistema de almacenamiento de discos magnéticos. Asignar y desasignar discos lógicos (LUNs) entre los servidores de plataforma soportada, sin interrumpir el funcionamiento del servidor de almacenamiento. Expandir en línea (sin interrumpir el funcionamiento del sistema de almacenamiento de discos magnéticos) la capacidad de discos lógicos (LUNs) previamente definidos. Incrementar en línea (sin interrumpir el funcionamiento del sistema de almacenamiento) el número de discos magnéticos físicos que conforman un arreglo previamente definido.
Software de aprovisionamiento	Se deberá de incluir la capacidad de realizar Thin Provisioning a los diferentes volúmenes del arreglo de discos; esta licencia deberá de cubrir la capacidad máxima del arreglo de discos.
Clonación de datos	Se deberá de incluir la capacidad de realizar copias totales de los volúmenes sin necesidad de intervención de los servidores; dicha funcionalidad deberá de cubrir la capacidad máxima del arreglo de discos.
Funcionalidad NAS	Deberá de soportar los protocolos SMB 3.0, 2.1, 2.0; NFSv4.0, v3.0 Soporte de protocolo NDMP Integración nativa con Active Directory Soporte de Encriptación de datos (FIPS 140-2) Se deberá de tener una consola unificada de administración para ambiente NAS y SAN.
Optimización de datos	El equipo deberá de soportar la funcionalidad que permita el movimiento de datos de manera automática (autotiering) entre los diferentes tipos de discos soportados por el arreglo de disco.
Calidad de Servicio	El equipo deberá de soportar la funcionalidad de asignar calidad de servicios (QoS) a los diferentes volúmenes creados en el Storage; se deberá de poder definir niveles máximos y mínimos de IOPS, Throughput y además definir un tiempo mínimo de respuesta. No se aceptará la funcionalidad de optimización de datos (autotiering) para cumplir este requerimiento.
Software de fail over y balanceo de carga (conectividad de servidores al arreglo de discos)	Se debe incluir el software que permita la funcionalidad de fail over y balanceo de carga para servidores en conectividad al arreglo de discos, de requerir una licencia esta debe incluir a la

	totalidad de servidores soportados por el sistema de almacenamiento.
Soporte	El soporte debe ser del tipo 24x7 por 3 años. Los servicios de soporte durante la garantía deben ser ejecutados directamente por el fabricante
Servicios durante el tiempo de soporte	- Generar reporte de incidentes trimestralmente - Análisis y administración de versiones de Firmware del Storage semestralmente. - Análisis y administración de versiones de Firmware de los dispositivos de Red semestralmente. - Escaneo proactivo semestral. - Asesoramiento técnico operacional presencial a través de una persona que atenderá de manera personalizada la infraestructura ofertada.
Servicios de Instalación	Los servicios de instalación y puesta en marcha deben ser ejecutados directamente por el fabricante.
Servicios de notificación de eventos	El arreglo de discos debe contar con la funcionalidad de notificación en forma automática (a través de internet utilizando protocolo TCP/IP) los eventos hacia el centro de soporte del fabricante.

ANEXO 4: ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SISTEMA DE RESPALDO DE INFORMACIÓN

SISTEMA DE RESPALDO DE INFORMACIÓN		
Descripción	Este componente permite extraer copias de seguridad de la información de los servidores y servicios del sistema (tal como el almacenamiento de video).	
Servidor de Respaldo	Cantidad	A Dimensionar
	Tipo	Rack
	Procesador	Dimensionado por el PROVEEDOR
	Memoria	64GB mínimo o superior
	Conexiones	04 puertos Ethernet 10/100/1000 Mb 01 HBA SAS de 6 Gbps
	Almacenamiento	02 discos SAS-2 de 300GB de 10000 RPM. Debe soportar al menos 8 discos en total.
	Disponibilidad	Debe contar con fuentes y ventiladores redundantes e intercambiables en vivo
	Ranuras de expansión	Al menos 03 slots PCI-E
	Sistema operativo	Debe incluir licencia de Windows Server Standard Edition con soporte de 3 años
	Soporte y Garantía	05 años de soporte del fabricante en modalidad 24x7x365. Con 4 horas de respuesta en el sitio y 24 horas como máximo para dar solución al incidente presentado. Debe cubrir todos los componentes físicos del servidor de gestión
Librería de Cintas de respaldo	Cantidad	Dimensionado por el PROVEEDOR, se deberá considerar que hay un Centro de Datos Principal y Un centro de Datos de Contingencia
	Tipo	Rack
	Fuente de poder	Redundantes y hot-swap
	Número de Drive	Al menos 02 Tape Drive LTO 6 de conexión SAS de 6Gbps, con capacidad de instalar uno adicional.
	Administración	Administración Web, Lector de código de barras
	Capacidad	Capacidad de albergar al menos 20 slots
	Cartuchos	Al menos 20 cartuchos LTO 6y 02 de limpieza

SISTEMA DE RESPALDO DE INFORMACIÓN		
	Cantidad de Cintas	Las necesarias para mantener respaldada la Solución en cinta durante el tiempo que dure la prestación del servicio.
	Interfaz	SCSI o SAS
	Software de Monitoreo	Deberá de incluir las siguientes características: - Mitigar los riesgos de errores de dispositivos, mediante el análisis de la probabilidad de fallos de dispositivos. - Planificar las futuras inversiones en hardware mejor mediante el análisis de los cuellos de botella en la utilización de la unidad / de la cinta. - El software deberá de generar reportes y graficar opciones para monitorear los indicadores clave de rendimiento, la salud y la utilización de unidades de cinta y cartuchos.
	Soporte y Garantía	03 años de soporte del fabricante en modalidad 24x7x365, con 4 horas de respuesta en el sitio y máximo 24 horas para dar solución definitiva al incidente Presentado. Debe cubrir todos los componentes físicos de la Librería Tape
Software de backup	Librerías	El software de backup deberá administrar las librerías de almacenamiento tanto locales como remotas.
	Catálogo	El software debe facilitar la réplica tanto del catálogo como de las imágenes de respaldo haciendo uso de tecnologías de de-duplicación (opcional) hacia un sitio alterno con el propósito de recuperación ante desastres basado en respaldo de datos
	Base de Datos	El software debe tener la capacidad de realizar respaldo y recuperaciones en caliente de base de datos sql, oracle (32 y 64 bits) 9, 10 y 11 en plataformas Windows (32 y 64 bits) como mínimo
	Recuperación de datos	La solución de recuperación de datos debe tener la capacidad de realizar respaldo en caliente de archivos abiertos sin perder la integridad de los datos.
	Políticas	El software debe tener la capacidad de rotar y reciclar los medios que cumplan la política de retención, además poder diferenciar cuales respaldos son diarios, semanales y mensuales

SISTEMA DE RESPALDO DE INFORMACIÓN		
	Administración	El software debe incluir administración y monitoreo centralizado de todas las tareas de protección de datos, en la que se pueda configurar la administración de políticas desde una única interfaz GUI.
	Backup	El software debe soportar los métodos de backup tradicionales tales como backup full, incremental, diferencial en las plataformas descritas
	Reportes	El software debe contar con la posibilidad de definir políticas que permitan manejar el ciclo de vida del respaldo y la posibilidad y de incluir dentro del ciclo diferentes tecnologías de almacenamiento así como diferentes sitios o ubicaciones geográficas
	Licencias	El soporte del licenciamiento ofertado deberá ser de 03 años.
Instalación	La instalación y puesta en Marcha deberá ser realizada por el fabricante	