

DIRECCIÓN GENERAL DE REGISTRO CIVIL IDENTIFICACIÓN Y CEDULACIÓN

**ANEXO B**

**TÉRMINOS DE REFERENCIA PARA LA ADQUISICIÓN E IMPLEMENTACIÓN DE UN SISTEMA INFORMÁTICO PARA EMISIÓN DE DOCUMENTOS DE IDENTIDAD Y PASAPORTES ELECTRÓNICOS, Y LA PROVISIÓN DE EQUIPAMIENTO, SUSCRIPCIONES-LICENCIAS DE SOFTWARE, INSUMOS Y SERVICIOS CONEXOS PARA LA DIRECCIÓN GENERAL DE REGISTRO CIVIL IDENTIFICACION Y CEDULACION (DIGERCIC)**

MARZO – 2019

QUITO - ECUADOR

**INDICE**

[1. ANTECEDENTES 5](#_Toc26363)

[2. JUSTIFICACIÓN 6](#_Toc26415)

[3. OBJETO DE LA CONTRATACIÓN 11](#_Toc30071)

[4. OBJETIVOS 11](#_Toc1705)

[4.1. Objetivo General 11](#_Toc9448)

[4.2. Objetivos Específicos 11](#_Toc728)

[5. ALCANCE 14](#_Toc29806)

[5.1. BIENES INCLUIDOS 14](#_Toc7471)

[5.2. SERVICIOS INCLUIDOS 16](#_Toc2898)

[5.3. BIENES Y SERVICIOS EXCLUIDOS 18](#_Toc5270)

[6. METODOLOGÍA DE TRABAJO 20](#_Toc5863)

[7. ESPECIFICACIONES TÉCNICAS 25](#_Toc18389)

[7.1. SISTEMA DE EMISION DE DOCUMENTOS DE IDENTIDAD Y PASAPORTES 25](#_Toc18839)

[7.1.1. DESCRIPCIÓN FUNCIONAL 25](#_Toc4637)

[7.1.2.1. CAPTURA DE DATOS DEMOGRÁFICOS Y BIOMÉTRICOS 30](#_Toc27863)

[7.1.2.1.1 Importar las solicitudes de emisión de documentos desde el SURI 30](#_Toc9907)

[7.1.2.1.2 Autenticar a operadores de captura de datos 32](#_Toc9782)

[7.1.2.1.4. Capturar información biométrica desde estaciones fijas 35](#_Toc16093)

[7.1.2.1.5. Verificar biométricamente la identidad 40](#_Toc5123)

[7.1.2.1.6. Analizar registros biométricos duplicados en el ABIS 41](#_Toc18734)

[7.1.2.1.7. Capturar información biométrica con kits móviles en-línea 42](#_Toc5639)

[7.1.2.1.8. Capturar información biométrica con kits móviles fuera-de-línea 42](#_Toc3038)

[7.1.2.2. PRODUCCIÓN DE DOCUMENTOS 49](#_Toc28897)

[7.1.2.2.3. Preparación de datos y producción del documento 49](#_Toc6965)

[7.1.2.2.2. Control de la producción de documentos 53](#_Toc18770)

[7.1.2.2.3. Control del inventario de documentos e insumos 54](#_Toc19484)

[7.1.2.3. ENTREGA DE DOCUMENTOS 56](#_Toc7948)

[7.1.2.4. CONSULTAS Y REPORTES 57](#_Toc19523)

[7.1.3. REQUERIMIENTOS NO FUNCIONALES 58](#_Toc27317)

[7.1.3.1. ARQUITECTURA 58](#_Toc5258)

[7.1.3.2. RENDIMIENTO 59](#_Toc24892)

[7.1.3.3. CAPACIDAD 60](#_Toc20357)

[7.1.3.4. DISPONIBILIDAD 64](#_Toc11964)

[7.1.3.5. CONTINUIDAD 65](#_Toc23894)

[7.1.3.6. INTEGRACIÓN CON SISTEMAS LEGADOS 66](#_Toc19830)

[7.1.3.7. USABILIDAD 70](#_Toc10043)

[7.1.3.8. SEGURIDAD 71](#_Toc434)

[7.1.3.9. ESTÁNDARES Y BUENAS PRATICAS APLICABLES 75](#_Toc18543)

[7.1.3.10. SOFTWARE A SER UTILIZADO 76](#_Toc2432)

[7.1.3.11. IMPLEMENTACIÓN 77](#_Toc32608)

[7.1.3.12. ADMINISTRACIÓN/PARAMETRIZACION Y MONITOREO 79](#_Toc18358)

[7.2. SISTEMA AUTOMATIZADO DE IDENTIFICACIÓN BIOMÉTRICA (ABIS) 81](#_Toc12613)

[7.2.1. DESCRIPCIÓN FUNCIONAL 81](#_Toc11160)

[7.2.2. REQUERIMIENTOS FUNCIONALES 83](#_Toc23437)

[7.2.3. REQUERIMIENTOS NO FUNCIONALES 87](#_Toc25361)

[7.2.3.1. MIGRACIÓN Y SINCRONIZACIÒN DE HUELLAS Y ROSTROS 87](#_Toc27088)

[7.2.3.2. ARQUITECTURA 91](#_Toc4965)

[7.2.3.3. RENDIMIENTO 91](#_Toc23579)

[7.2.3.4. CAPACIDAD 92](#_Toc29894)

[7.2.3.5. DISPONIBILIDAD 94](#_Toc18643)

[7.2.3.6. CONTINUIDAD 95](#_Toc20270)

[7.2.3.7. INTEGRACIÓN DEL ABIS CON EL SISTEMA DE EMISION 96](#_Toc24200)

[7.2.3.8. USABILIDAD 96](#_Toc2923)

[7.2.3.9. SEGURIDAD 97](#_Toc28002)

[7.2.3.10. ESTÁNDARES Y BUENAS PRÁCTICAS APLICABLES 97](#_Toc24906)

[7.2.3.11. SOFTWARE A SER UTILIZADO 98](#_Toc32027)

[7.2.3.12. IMPLEMENTACIÓN 100](#_Toc13368)

[7.2.3.13. ADMINISTRACIÓN/PARAMETRIZACION Y MONITOREO 102](#_Toc23458)

[7.3. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) 103](#_Toc31192)

[7.3.1. DESCRIPCIÓN FUNCIONAL 103](#_Toc12747)

[7.3.2. REQUERIMIENTOS FUNCIONALES 104](#_Toc8798)

[7.3.3. REQUERIMIENTOS NO FUNCIONALES 105](#_Toc22224)

[7.3.3.1. ARQUITECTURA 105](#_Toc30896)

[7.3.3.2. RENDIMIENTO 106](#_Toc8286)

[7.3.3.3. CAPACIDAD 106](#_Toc24729)

[7.3.3.4. DISPONIBILIDAD 106](#_Toc7300)

[7.3.3.5. CONTINUIDAD 107](#_Toc19353)

[7.3.3.6. INTEGRACIÓN CON EL SISTEMA DE EMISION 108](#_Toc19406)

[7.3.3.7. USABILIDAD 109](#_Toc16649)

[7.3.3.8. SEGURIDAD 109](#_Toc25911)

[7.3.3.9. ESTÁNDARES Y BUENAS PRÁCTICAS APLICABLES 110](#_Toc31932)

[7.3.3.10. SOFTWARE A SER UTILIZADO 110](#_Toc15088)

[7.3.3.11. IMPLEMENTACIÓN 111](#_Toc32574)

[7.3.3.12. ADMINISTRACIÓN/PARAMETRIZACION Y MONITOREO 114](#_Toc19971)

[7.4. SISTEMA DE MONITOREO DE LA OPERACIÓN Y SEGURIDAD 115](#_Toc1368)

[7.5. EQUIPAMIENTO PARA AGENCIAS/CONSULADOS 119](#_Toc20567)

[7.5.1. KITS FIJOS PARA CAPTURA DE DATOS 119](#_Toc18578)

[7.5.2. KITS DE PRODUCCION DE PASAPORTES 138](#_Toc4011)

[7.5.3. KITS DE ENTREGA DE DOCUMENTOS 156](#_Toc14520)

[7.5.4. GATEWAYS DE SEGURIDAD PARA CONSULADOS 174](#_Toc22903)

[7.5.5. INSUMOS PARA IMPRESION DE PASAPORTES 181](#_Toc7867)

[7.5.6. KITS DE PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD 183](#_Toc9947)

[7.5.7. KITS MÓVILES DE CAPTURA DE DATOS 197](#_Toc23394)

[8. TRANSFERENCIA DE CONOCIMIENTOS Y ENTRENAMIENTO 206](#_Toc6406)

[9. SERVICIOS POST-IMPLEMENTACION 213](#_Toc18592)

[10. PRODUCTOS MINIMOS ESPERADOS 214](#_Toc20913)

[11. ENTREGA DE LOS BIENES 217](#_Toc14994)

[12. PLAZO 217](#_Toc20648)

[13. EXPERIENCIA GENERAL Y ESPECÍFICA DEL OFERENTE 218](#_Toc17772)

[14. PERSONAL TÉCNICO MÍNIMO 220](#_Toc1659)

[15. FORMA DE PAGO 226](#_Toc22502)

[16. MULTAS 227](#_Toc3530)

[13. ANEXOS 229](#_Toc30177)

[A) AGENCIAS DE EMISION DE DOCUMENTOS DE IDENTIDAD DE LA DIGERCIC 229](#_Toc18371)

[B) AGENCIAS DE EMISION DE PASAPORTES DE LA DIGERCIC 234](#_Toc32091)

[C) PUNTOS DE CAPTURA DE DATOS PARA EMISIÓN DE PASAPORTES DEL MREMH 235](#_Toc15822)

[D) DISEÑO FISICO DE ALTO NIVEL DEL SEDIP 237](#_Toc28656)

[E) ESPECIFICACIONES TECNICAS DE EQUIPOS 238](#_Toc31113)

[F) REQUERIMIENTOS DE LOS SERVICIOS POST-IMPLEMENTACION 260](#_Toc19832)

# ANTECEDENTES

La Dirección General de Registro Civil Identificación y Cedulación (DIGERCIC) es la entidad estatal encargada por Ley de otorgar la identidad a los ciudadanos, registrar sus hechos y actos civiles e identificarlos a través del Documento Único de Identidad (Cédula).

El ámbito de acción de la DIGERCIC es en todo el territorio nacional y en el extranjero, por medio de los consulados del país en el extranjero, que están a cargo del Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). A la fecha la DIGERCIC cuenta con 183 agencias a nivel nacional que facilitan el servicio de emisión de documentos de identidad y de registro civil, entre otros (Anexo A).

Para la prestación del servicio de emisión de documentos de identidad, la DIGERCIC, cuenta con sistemas informáticos que permiten validar la identidad demográfica de los ciudadanos e identificarlos biométricamente, logrando mejorar sustancialmente la calidad de la información, reducir adulteraciones o suplantaciones de identidad y brindar un servicio de calidad.

El documento de identidad que se emite tiene la connotación que es electrónico, debido a que incorpora un circuito electrónico integrado o chip de identificación por radiofrecuencia (del inglés Radio Frequency Identification - RFID), en el cual se graba la información demográfica y biométrica del ciudadano que es igual a la que se imprime. Adicionalmente, para la emisión de un nuevo documento de identidad se registra las huellas dactilares asignándolas a los datos demográficos, para garantizar una identidad única a cada ciudadano en posteriores validaciones.

Por otra parte, desde el año 2017, la DIGERCIC presta también el servicio de emisión de pasaportes ordinarios en 25 agencias a nivel nacional (Anexo B). Para esto se utiliza sistema de emisión pasaportes de lectura mecánica administrado por el MREMH. El pasaporte o documento de viaje garantiza la identidad del portante al momento de viajar, particularmente a otros países.

Los pasaportes que se emiten cumplen con las recomendaciones de la Organización de Aviación Civil Internacional (OACI)[[1]](#footnote-1). La OACI, es la entidad internacional que agrupa a casi todos los países del orbe y que se ha destacado por elaborar y difundir recomendaciones para la elaboración de documentos de viaje estándares para facilitar el tránsito de personas entre los países.

Cabe acotar que, la promulgación de las Leyes Orgánicas de Gestión de la Identidad y Datos Civiles (LOGIDAC) el año 2016; y de Movilidad Humana (LOMH) en el año 2017, han establecido un renovado marco legal para la emisión de documentos de identidad. Particularmente, en el caso de la LOMH otorgó la calidad de documento de viaje al documento de identidad (Artículo 148), y la competencia a la DIGERCIC para que emita pasaportes ordinarios en el país a través de sus dependencias en el territorio nacional y de las misiones diplomáticas u oficinas consulares del Ecuador en el exterior (Artículo 151).

# JUSTIFICACIÓN

La promulgación de la Ley Orgánica de Gestión de la Identidad y Datos Civiles (LOGIDAC) del año 2016, introdujo cambios a los datos de los ciudadanos que deben constar en los Documentos Únicos de Identidad (antes llamadas “cédulas de identidad”). Datos como, el tipo de sangre, sexo, condición de donante de órganos y/o tejidos y condición de discapacidad, de ser el caso, deben ser impresos en los documentos de identidad.

Por otra parte, la Ley Orgánica de Movilidad Humana (LOMH), promulgada el año 2017, concedió la competencia a la DIGERCIC, para la emisión de pasaportes ordinarios en el país y en el extranjero, esto último, por medio de los consulados ecuatorianos en el exterior, que dirige el MREMH. Además, la mencionada ley otorga la connotación de documento de viaje al Documento Único de Identidad. La LOMH establece adicionalmente que, la emisión de los otros tipos de pasaportes, a saber: diplomáticos, oficiales y de emergencia están a cargo del MREMH.

En este sentido, al finalizar el año 2017, el MREMH delegó a la DIGERCIC la implementación del proyecto para emisión de pasaportes electrónicos. Esto, en consideración del proceso en el que está inmerso el Gobierno Ecuatoriano para la exención del visado Schengen; y para cumplir con lo que establece la OACI, en lo que tiene que ver a la producción o emisión de Documentos de Viaje de Lectura por Maquina Electrónicos (EMRTD, por sus siglas en ingles)[[2]](#footnote-2).

La emisión de pasaportes electrónicos conlleva la aplicación de las recomendaciones de la OACI, publicadas en el documento *“Doc 9303, Documento de Viaje de Lectura Mecánica”, Séptima Edición, 2015*[[3]](#footnote-3), en todo lo relacionado a su producción y uso en los puntos de control fronterizo. La emisión de documentos de identidad y pasaportes electrónicos bajo esas normas garantiza la identidad del portante, la integridad de los datos de identificación y disminuye riesgos de seguridad para el ciudadano y para el país emisor y receptor.

La aplicación de la normativa legal antes referida demanda la implementación de cambios operativos en los servicios de emisión de documentos de identidad y de viaje electrónicos.

Con relación a la emisión de documentos de identidad electrónicos, se debe implementar procesos para recolectar nuevos datos desde entidades externas, los cuales deben ser impresos en los documentos de identidad. Adicionalmente, la ratificación por ley, que los documentos de identidad son también documentos de viaje, involucra que se implementen cambios en el formato del documento, tanto en la sección visual o impresa como en la electrónica, que permitan cumplir con las recomendaciones de la OACI vigentes.

En cuanto a los pasaportes electrónicos, se deberá implementar procesos para grabar la información demográfica y biométrica en el chip de los pasaportes, conforme las recomendaciones de la OACI. Esto permitirá convertir a los documentos de viaje de lectura mecánica (pasaportes) que actualmente se emiten, en documentos de viaje de lectura mecánica electrónicos (pasaportes electrónicos).

En ambos casos, la validación de la identidad de los ciudadanos es requisito fundamental según la estrategia del programa de identificación de viajeros de la OACI conocida como “Traveller Identification Programme (OACI TRIP) Strategy”, publicada en el año 2913[[4]](#footnote-4).

En este contexto, la DIGERCIC es la entidad llamada a garantizar la identidad de los solicitantes de documentos de viaje por medio de la validación de los datos demográficos obtenidos de los registros de los actos y hechos civiles de los ciudadanos. Adicionalmente, se debe implementar la captura biométrica de huellas dactilares planas y rostros de los solicitantes para realizar la validación biométrica de la identidad, previa a la emisión de un documento de identidad o de viaje electrónico. La captura y grabación de la foto del rostro del ciudadano y de otros datos de identidad, firmados electrónicamente, en el chip de los documentos de viaje, permitirá comprobar fehacientemente la identidad del portante, la integridad de los datos y del propio documento.

La emisión de documentos de viaje electrónicos conlleva la responsabilidad del país con otros países para reportar documentos de viaje perdidos o robados. Esto para disminuir riesgos de fraude o mal uso de tales documentos por personas inescrupulosas.

Desde la perspectiva informática, a la fecha la emisión de documentos de identidad electrónicos y de pasaportes ordinarios se realiza con el soporte de dos sistemas informáticos diferentes.

Para el caso de los documentos de identidad, desde al año 2009, se producen los mismos en formato electrónico con un sistema informático implementado en ese año en la DIGERCIC, cuyos requisitos legales y requerimientos funcionales correspondieron a esa fecha. A la fecha, el sistema de emisión de cédulas funciona de forma integrada con un Sistema de Identificación de Huellas Dactilares (AFIS, por sus siglas en ingles)[[5]](#footnote-5). El AFIS permite buscar huellas dactilares capturadas de los ciudadanos en la base de datos de huellas al momento de solicitar una cédula.

Adicionalmente, los datos demográficos y biométricos que se almacenan en el chip son firmados electrónicamente por un sistema de firmado electrónico de una Infraestructura de Clave Pública (PKI, por sus siglas en inglés)[[6]](#footnote-6) que opera también de forma integrada al sistema de emisión de cédulas. Sin embargo, tanto la grabación de datos en el chip como la lectura o acceso cumplen parcialmente con las recomendaciones de la OACI. Cabe acotar que, la infraestructura informática a nivel de hardware y software del AFIS y de la PKI están alcanzando su vida útil por lo que se justifica un cambio de esas plataformas. El sistema de emisión de cédulas en operación ha permitido emitir a la fecha más de 12 millones de cédulas con validación biométrica dactilar.

El sistema de emisión de pasaportes data del año 2003. A la fecha no cumple con los requerimientos para emisión de pasaportes electrónicos. El sistema actual de pasaportes tampoco permite realizar validación biométrica de la identidad ni codificar o grabar electrónicamente datos en el chip de pasaportes electrónicos. Ante tales circunstancias, a finales del año 2017, el MREMH delegó a la DIGERCIC la contratación de elaboración de libretines de pasaportes electrónicos y su sistema (plataforma) de personalización en sus diferentes tipos. Así mismo, el MREMH ha solicitado a la DIGERCIC, la implementación de kits de captura y entrega de pasaportes para 78 consulados del extranjero y 2 oficinas en el Ecuador (Quito y Guayaquil). El detalle consta en el Anexo C. Adicionalmente, la implementación de 3 centros de producción de pasaportes electrónicos situados en Quito (MREMH), Nueva York (USA) y Madrid (España).

Los beneficios para el país, de la implementación de un nuevo sistema de emisión de documentos de identidad y pasaportes, radican en el fortalecimiento la identificación única y segura de los ciudadanos, por medio de la cual acceden a servicios y tramites públicos; el aseguramiento de la identidad del portante del documento cuando viajan; la disminución de riesgos de seguridad asociados a delitos de identidad; el avance en la modernización del servicio de emisión de documentos de identidad y pasaportes manteniendo altos niveles de servicio, el cumplimiento con las recomendaciones y estándares internacionales para emisión de documentos de viaje y el aporte a la eliminación del visado Schengen a los ecuatorianos por parte de la Comunidad Europea. Adicionalmente, el control fronterizo y procedimientos de entrada/salida del país, así como su seguridad, podrán ser mejorados mediante sistemas automáticos de control o el uso de biometría dactilar o facial.

La implementación del nuevo sistema de emisión de documentos de identidad y pasaportes está alineado al Plan Nacional de Desarrollo 2017-2021, objetivo 7 "Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía."

El nuevo sistema deberá ser amigable, seguro en extremo, fácil de usar y mantener, flexible para adaptar nuevos requerimientos y/o equipos e independiente de tecnologías, productos o proveedores, hasta donde sea posible. El sistema de emisión deberá gestionar la emisión de los documentos desde la captura de las solicitudes de documentos de identidad o pasaportes pasando por la validación biométrica de identidad, la codificación electrónica del chip e impresión del documento hasta la entrega del mismo al ciudadano. El sistema estará integrado a un sistema automatizado de identificación biométrica para validación biométrica de la identidad y una infraestructura de clave pública para firmar los datos que se graban en los chips de los documentos y su posterior acceso o lectura. La arquitectura del sistema de emisión será tipo Web centralizada y el acceso y uso a través de programas navegadores desde las agencias de la DIGERCIC en el país o consulados del MREMH en el extranjero. Esto para beneficiar la gestión del soporte, de incidentes, de mantenimientos y la actualización tecnológica. Debido a que los servicios de emisión de documentos de identidad y pasaportes son críticos para la ciudadanía y el estado, la capacidad, disponibilidad, rendimiento, continuidad y seguridad del sistema, en su conjunto, deberán ser asegurados.

# OBJETO DE LA CONTRATACIÓN

Adquisición e implementación de un sistema informático para emisión de documentos de identidad y pasaportes electrónicos; y la provisión de equipamiento, suscripciones/licencias de software, insumos y servicios conexos.

# OBJETIVOS

# Objetivo General

Implementar un sistema informático para emisión de documentos de identidad y pasaportes electrónicos en las agencias de la DIGERCIC a nivel nacional y los consulados del MREMH a nivel internacional aplicando el marco legal ecuatoriano y las recomendaciones de la Organización de Aviación Civil Internacional vigentes.

# Objetivos Específicos

1. Gestionar y controlar la producción de documentos de identidad y pasaportes electrónicos desde agencias de la DIGERCIC y consulados del MREMH mediante el sistema centralizado para emisión de documentos de identidad y pasaportes (SEDIP).
2. Consultar información demográfica de los ciudadanos y solicitudes de documentos de identidad y pasaportes por medio de la integración del SEDIP con el Sistema Unificado de Registro Civil (SURI) de la DIGERCIC.
3. Capturar huellas dactilares, rostros y firmas manuscritas de los ciudadanos mediante escáneres y cámaras especializados conectados al SEDIP.
4. Validar la identidad biométrica de los ciudadanos a través de un Sistema Automatizado de Identificación Biométrica (ABIS, por sus siglas en inglés)[[7]](#footnote-7) integrado al SEDIP.
5. Preparar y firmar electrónicamente los datos a grabar en los chips de los documentos de identidad y pasaportes mediante un sistema de Infraestructura de Clave Pública (PKI, por sus siglas en inglés)[[8]](#footnote-8) integrado al SEDIP.
6. Grabar los datos en los chips de los documentos y garantizar su lectura por medio de la implementación del Control de Acceso Básico (BAC, por sus siglas en inglés)[[9]](#footnote-9) y el Control de Acceso Suplementario (SAC, por sus siglas en inglés)[[10]](#footnote-10) según las recomendaciones de la OACI vigentes.
7. Imprimir la información demográfica y biométrica en los documentos utilizando impresoras e insumos especializados para cada tipo de documento.
8. Controlar y asegurar la calidad de la información impresa y grabada en los chips electrónicos empleando equipos o lectores especializados según el tipo de documento.
9. Asegurar la entrega de los documentos producidos a los ciudadanos por medio de la autenticación biométrica de rostro.
10. Validar y certificar el funcionamiento completo del SEDIP mediante la ejecución de pruebas exhaustivas a nivel operativo e informático y los ajustes respectivos de ser el caso.
11. Controlar el inventario de los documentos en blanco, insumos de producción según el caso, documentos producidos y rechazados por medio del SEDIP.
12. Asegurar la transferencia de conocimiento del proyecto y del SEDIP mediante la elaboración de documentación operativa y técnica.
13. Garantizar el uso correcto del SEDIP, así como de los equipos suministrados por medio del entrenamiento en ámbitos operativos e informáticos al personal designado.
14. Minimizar interrupciones de los servicios de emisión de documentos mediante el despliegue ordenado y progresivo en las agencias de la DIGERCIC; y posteriormente en los consulados del MRHEMH.
15. Asegurar el acceso, uso y trazabilidad de las operaciones del sistema implementando autenticación biométrica de los usuarios y registros detallados de actividades.
16. Implementar servicios electrónicos para autenticación e identificación biométrica por medio del Sistema Automatizado de Identificación Biométrica (ABIS).
17. Obtener información para estadísticas, toma de decisiones e interoperabilidad por medio de la implementación de consultas y replica de bases de datos
18. Garantizar la capacidad, rendimiento, disponibilidad y continuidad del sistema a través de la implementación de configuraciones de alta disponibilidad y tolerancia a fallos de todos los componentes.
19. Asegurar el normal funcionamiento y operación del SEDIP por medio de mantenimientos preventivos y correctivos a todos los componentes de hardware y software.
20. Garantizar la vigencia tecnológica del sistema a través de la actualización a nuevas versiones del software de emisión y/o del software base.
21. Gestionar incidentes del sistema a través de niveles de servicio establecidos por la DIGERCIC.
22. Monitorear la operación diaria y normal y la seguridad de todos los componentes del SEDIP mediante un sistema centralizado de monitoreo

# ALCANCE

# BIENES INCLUIDOS

* Un sistema informático, de arquitectura Web, para emisión de documentos de identidad y pasaportes electrónicos implementado en alta-disponibilidad y con tolerancia a fallos. Incluye la provisión de licencias o suscripciones para al menos 965 usuarios concurrentes; y del hardware y licencias o suscripciones de software necesarios para su implementación, así su cómo respaldo y restauración.
* Un Sistema de Identificación Biométrica Automatizado (ABIS), de arquitectura Web de preferencia, integrado al SEDIP e implementado en alta-disponibilidad y con tolerancia a fallos. Incluye la provisión de licencias o suscripciones para 16 millones de huellas deca-dactilares y 16 millones de rostros; y del hardware y licencias o suscripciones de software necesarios para su implementación, así como su respaldo y restauración.
* Un Sistema de Infraestructura de Clave pública (PKI), de arquitectura Web de preferencia, integrado al SEDIP e implementado en alta-disponibilidad y con tolerancia a fallos. Incluye la provisión de licencias o suscripciones de software necesarios para su implementación, así como su respaldo y restauración. Adicionalmente, la integración o conexión tecnológica al Directorio de Claves Publicas de la OACI. El sistema PKI comprenderá, al menos:
  + La Autoridad de Certificación Firmante de País (CSCA, por sus siglas en inglés)[[11]](#footnote-11)
  + Los Firmantes de Documentos (DS, por sus siglas en inglés)[[12]](#footnote-12) para documentos de identidad y pasaportes
  + El Directorio de Claves Públicas Nacional (nPKD, por sus siglas en inglés)[[13]](#footnote-13)
  + El software para gestión de la PKI.
  + Cualquier otro componente de hardware y/o software necesario para implementación de la PKI y la conexión/integración a la PKD de la OACI.
* 1 sistema de servicios Web para búsquedas 1 a 1 y 1 a n de huellas y rostros integrado al ABIS.
* 1 set de equipos módulos de seguridad de hardware (HSM), para desbloqueo de los chips de las tarjetas y libretas en blanco, instalados en alta disponibilidad en el centro de datos principal, y contingencia en el centro de datos secundario. Incluye licencias/suscripciones de software respectivas.
* 1 sistema de emisión para pruebas en operación con una capacidad de procesamiento de hasta el 1% del sistema de producción. Incluye el ABIS, la PKI de pruebas y HSMs para desbloqueo de chips. Incluye el hardware y las licencias/suscripciones necesarias.
* 1 sistema centralizado de monitoreo que permita monitorear al menos la capacidad y disponibilidad de todos los componentes de hardware y software suministrados. Se deberá suministrar el hardware y licencias o suscripciones de software necesarios para su implementación, así su cómo respaldo y restauración.
* 1 sistema de gestión de eventos y seguridad de la información (SIEM, por sus siglas en inglés) incluyendo el hardware y licencias o suscripciones de software necesarios para su implementación, así su cómo respaldo y restauración.
* Kits de equipos para captura biométrica, producción y entrega de documentos, que comprende:
* 635 kits fijos para captura de datos.
* 88 kits completos para entrega de documentos.
* 290 kits parciales para entrega de documentos.
* 67 kits para producción de documentos de identidad con impresión de tecnología por grabado por láser. Incluye software de monitoreo de las impresoras con las licencias o suscripciones de software necesarias para su implementación.
* 13 kits para producción de pasaportes con impresión de tecnología de tinta. Incluye software de monitoreo de las impresoras con las licencias o suscripciones de software necesarias para su implementación.
* Insumos para impresión de 1’000.000 de pasaportes.
* 4 gateways de seguridad para los consulados con centros de producción.
* 70 kits móviles para captura de datos.
* Software antivirus; y de seguridad de punto final (endpoint security software) para todos los computadores a suministrar. Incluye las licencias o suscripciones de los dos tipos de software necesarias para su implementación.

# SERVICIOS INCLUIDOS

* **SERVICIOS DE IMPLEMENTACION**
* Planificación, ejecución y control del plan y cronograma de trabajo.
* Elaboración del diseño lógico y físico del SEDIP integrado al ABIS y la PKI en configuraciones de alta disponibilidad (centro de datos principal) y de recuperación de desastres (centro de datos secundario) en base a los requerimientos y especificaciones técnicas establecidas por la DIGERCIC.
* Instalación, configuración, puesta en operación, pruebas unitarias y de integración del SEDIP, ABIS, y la PKI en los centros de datos principal y secundario según el diseño elaborado.
* Migración de la base de datos actual de imágenes de huellas dactilares, rostros y firmas manuscritas a la base de datos del SEDIP y posterior inserción de huellas dactilares y rostros al ABIS. Incluye de-duplicación de las huellas dactilares.
* Sincronización del ABIS con el AFIS en operación para garantizar la integridad y consistencia de la validación biométrica de la identidad hasta que termine el despliegue del SEDIP.
* Integración del SEDIP con los sistemas internos de la DIGERCIC para captura de solicitudes de emisión de documentos, envío de notificaciones electrónicas, gestión de la seguridad, gestión del inventario de materiales para producción de los documentos e interoperabilidad del SEDIP con otros sistemas.
* Ejecución de pruebas integrales de emisión de documentos de identidad y pasaportes electrónicos.
* Implementación de piloto de emisión de pasaportes y documentos de identidad en paralelo con los sistemas actuales.
* Elaboración de documentación operativa y técnica de los sistemas y componentes suministrados.
* Entrenamiento operativo y técnico al personal designado.
* Asesoría y acompañamiento para inscripción y pagos de tasas del Directorio de Claves Públicas Nacional de la PKI en el Directorio de Claves Púbicas de la OACI previo a la puesta en operación del sistema.
* Puesta en operación progresiva del sistema para emisión de pasaportes en 25 agencias de la DIGERCIC en el país; y en 3locaciones del MREMH (Consulados de Nueva York y Madrid; y oficina en Quito).
* Puesta en operación progresiva del sistema para emisión de documentos de identidad en 183 agencias de la DIGERCIC en el país.
* **SERVICIOS POST-IMPLEMENTACION**
* Mantenimiento preventivo y correctivo de todos los componentes de hardware y software suministrados por 3 años contados a partir de la recepción completa del sistema por parte de la DIGERCIC.
* Soporte técnico especializado por 3 años contados a partir de la recepción completa del sistema por parte de la DIGERCIC.
* Gestión de incidentes y problemas que provoquen la indisponibilidad o degradación completa o parcial del funcionamiento del SEDIP o de los componentes de hardware y software del sistema en la modalidad 24x7x365 por 3 años contados a partir de la recepción completa del sistema por parte de la DIGERCIC.
* Actualización tecnológica de los componentes de software del sistema a las versiones recientes estables por 3 años contados a partir de la recepción completa del sistema por parte de la DIGERCIC.
* Gestión del cambio del sistema para incorporación de nuevos modelos de chips RFID, nuevas versiones de sistemas operativos de chips RFID, nuevos materiales para impresión de documentos de identidad y/o pasaportes, nuevas marcas de equipos para kits, entre otros.

# BIENES Y SERVICIOS EXCLUIDOS

* Provisión de tarjetas en blanco con chip RFID para producción de documentos de identidad. Las tarjetas serán suministradas por el Instituto Geográfico Militar (IGM) a la DIGERCIC. Las tarjetas serán manufacturadas conforme las recomendaciones de la OACI y los estándares ISO respectivos y vigentes. El material definido es POLICARBONATO. El chip RFID tendrá instalado un sistema operativo JCOP y una aplicación OACI BAC/SAC (PACE) estándares. La DIGERCIC facilitará toda la información necesaria para asegurar la integración de las libretas en blanco al proceso de producción de los pasaportes. El diseño del documento de identidad, las especificaciones técnicas de las tarjetas en blanco y muestras de las mismas podrán ser entregados a los proveedores que participen en el proceso de contratación.
* Provisión de libretas en blanco con chip RFID (en la contrapasta) para producción de pasaportes. Las libretas serán suministradas por el IGM a la DIGERCIC. Las libretas son manufacturadas conforme las recomendaciones de la OACI y los estándares ISO respectivos y vigentes. El material de la página de datos definido es PAPEL. El chip RFID tendrá instalado un sistema operativo JCOP y una aplicación OACI BAC/SAC (PACE) estándares. La DIGERCIC facilitará toda la información necesaria para asegurar la integración de las libretas en blanco al proceso de producción de los pasaportes. El diseño de la página de datos del pasaporte, las especificaciones técnicas de las libretas en blanco y muestras de las mismas podrán ser entregados a los proveedores que participen en el proceso de contratación.
* Provisión de rollos de láminas holográficas de seguridad para laminación de la página de datos de los pasaportes. Los rollos de láminas serán suministrados por el IGM a la DIGERCIC y cada rollo consta de 2 componentes la capa de soporte o transportador, y la lámina de seguridad. . Las rollos de láminas holográficas de seguridad son manufacturadas por reconocidos fabricantes de láminas de seguridad de pasaportes conforme las recomendaciones de la OACI y los estándares internacionales respectivos y vigentes. La DIGERCIC facilitará toda la información necesaria para asegurar la integración de los rollos de láminas a las impresoras que suministre el proveedor conforme la marca, modelo y especificaciones técnicas de las mismas.
* Provisión y/o acondicionamiento de centros de datos para instalación y operación de los componentes centrales de hardware y software. Los componentes del sistema deberán ser instalados y operar en los centros de datos que señale la DIGERCIC, ubicados en el país.
* Provisión de redes de datos y/o enlaces de datos o aumento de la capacidad de estos tanto en el país como en el extranjero para acceso y uso del sistema. Para acceso y uso del sistema desde agencias de la DIGERCIC, se utilizará la Red Nacional de Datos de la DIGERCIC, para acceder a los componentes de centro de cómputo. Para acceso y uso desde consulados del MREMH, oficinas remotas y equipos móviles en-línea, se utilizarán enlaces de acceso a la Internet que serán provistos o dispuestos por el MREMH o la DIGERCIC.
* Ampliación, remodelación o acondicionamiento de edificios, oficinas o espacios físicos desde los cuales se operará el SEDIP, tanto en el país a cargo de la DIGERCIC, como en el extranjero a cargo del MREMH. De existir requerimientos relacionados a este rubro, el proveedor deberá especificar oportunamente para que sean atendidos por la DIGERCIC a nivel del país o por el MREMH en el extranjero.
* Servicio de mensajería o courier para envío de materiales, equipos, partes, piezas, insumos o documentos producidos fuera del país.

# METODOLOGÍA DE TRABAJO

El proveedor deberá aplicar una metodología de trabajo que asegure la consecución de los objetivos previamente planteados y mitigue los riesgos que identifique para la ejecución del contrato.

La metodología deberá apegarse a estándares internacionales y buenas prácticas para la ejecución de un proyecto con el alcance mencionado. Se requiere que la metodología haya sido aplicada en proyectos previos similares cuya ejecución haya sido exitosa.

La metodología deberá también tener un enfoque ágil que permita alcanzar hitos fundamentales del proyecto. Esto hitos se constituirán en elementos tangibles del avance del proyecto a partir de la firma del contrato respectivo.

Se deberá elaborar el plan del proyecto y el cronograma de ejecución y su ruta crítica junto con la metodología de trabajo. La gestión del proyecto deberá basarse en buenas prácticas como las que recomienda el Project Management Institute (PMI, por sus siglas en inglés).

El proveedor deberá especificar en el cronograma las actividades que dependerán exclusivamente de la DIGERCIC, así como los plazos de cumplimiento. Deberá existir paralelismo en la ejecución de actividades no dependientes y de esa optimizar el tiempo para el cumplimiento de los hitos del cronograma.

El control y seguimiento del proyecto deberá ser permanente, detallado y documentado por parte del oferente. Todo problema o potencial desviación del cronograma deberá ser gestionado y comunicado oportunamente a la DIGERCIC para toma de decisiones. El oferente deberá proporcionar un gestor documental basado en software libre open source en el cual almacenará toda la documentación que genere el proyecto hasta la recepción a satisfacción de la DIGERCIC, en adición a los documentos físicos que se generen.

La metodología deberá permitir alcanzar el objetivo relacionado al diseño, implementación y puesta en operación completa del sistema en hasta 12 mesescontados a partir la firma del contrato. Adicionalmente, se deberá contemplar 36 meses adicionales de servicios de mantenimiento preventivo/correctivo, soporte técnico, gestión de incidentes y actualización de los componentes de hardware y software del sistema contados a partir de la recepción del mismo por la DIGERCIC.

El proveedor deberá considerar los siguientes hitos claves para la DIGERCIC para el plan y cronograma de trabajo, a saber:

* SEDIP, ABIS y PKI implementados en el centro de datos principal y el secundario o de contingencia
* Información biométrica existente migrada al SEDIP y al ABIS
* ABIS y AFIS actual sincronizados previo al comienzo de operaciones
* SEDIP integrado a los sistemas internos de la DIGERCIC
* Pruebas unitarias y de integración en sitio ejecutadas satisfactoriamente
* Pruebas de emisión de pasaportes con el sistema nuevo y el actual ejecutadas
* Pruebas de emisión de documentos de identidad con el sistema nuevo y el actual ejecutadas
* Sistema aceptado y certificado por usuarios designados
* Personal operativo y técnico entrenado
* Documentación elaborada y entregada
* Emisión de pasaportes implementada en agencias de la DIGERCIC y agencia del MREMH en Ecuador, y consulados de Nueva York y Madrid en el extranjero.
* Emisión de documentos de identidad implementada en agencias de la DIGERCIC en Ecuador y consulados de Nueva York y Madrid en el extranjero.
* Sistema de servicios Web para búsquedas 1 a 1 y 1 a n de huellas y rostros implementado.
* Sistema de monitoreo y seguridad del SEDIP implementados.

El proveedor deberá conformar un equipo de trabajo de profesionales con la experiencia suficiente en proyectos similares y con resultados exitosos. El equipo del proveedor deberá estar liderado por un profesional con sólida formación académica y experiencia liderando proyectos similares a nivel nacional y/o internacional.

De su parte, la DIGERCIC conformará un equipo de proyecto integrado por funcionarios de sólida formación académica y con experiencia en la emisión de documentos de identidad y pasaportes con los sistemas actuales y en ámbitos de desarrollo de software, infraestructura tecnológica y soporte técnico.

El control de calidad durante la ejecución del proyecto y el aseguramiento de la calidad de los productos y entregables deberá ser una actividad constante de la metodología.

En la planificación del proyecto, especial atención deberá tener la fase de despliegue del sistema, tanto en las agencias de la DIGERCIC a nivel nacional como en la oficina de Quito y los consulados Nueva York y Madrid del MREMH. Esto debido a que, se continuará emitiendo documentos de identidad y pasaportes con los sistemas actuales hasta que finalice el despliegue del nuevo sistema. El proveedor deberá planificar las actividades antes, durante y después del despliegue del sistema en las agencias, considerando lo antes expuesto.

El plan de entrenamiento al personal que designe la DIGERCIC en el ámbito operativo deberá tener un enfoque teórico-práctico. En el ámbito informático, a más del entrenamiento, se deberá involucrar tempranamente al personal de informática designado por la DIGERCIC en las actividades de instalación, configuración, afinamiento, administración y monitoreo de todos los componentes y software del sistema. Esto permitirá garantizar la gestión de soporte de usuario final (nivel 1) y del sistema (nivel 2) por parte del personal informático de la DIGERCIC y del MREMH (en los consulados)

La gestión de las comunicaciones deberá ser proactiva y recurrente. Será necesario mantener reuniones semanales de avance entre las contrapartes designadas; y reuniones mensuales con las autoridades de la DIGERCIC para revisar el avance, desviaciones o retrasos del cronograma y cualquier tema de interés.

En general, la metodología podrá considerar los siguientes lineamientos para garantizar el éxito de la ejecución de los trabajos.

* Conformación de un equipo profesional y con experiencia en proyectos similares
* Entendimiento a profundidad de los requerimientos del sistema a implementar y las expectativas de la DIGERCIC
* Elaboración de un diseño que cumpla con los requerimientos especificados y garantice la capacidad, rendimiento, disponibilidad, continuidad y seguridad del sistema tanto a nivel central como en los puntos de atención.
* Provisión a tiempo y completa de equipos y software conforme el diseño del sistema.
* Solución a tiempo de problemas, controversias o desviaciones del cronograma
* Pruebas exhaustivas, completas y detalladas de toda la funcionalidad del sistema. Se implementará un piloto de pruebas de emisión en paralelo con los sistemas actuales de emisión de cédulas y pasaportes con una duración de al menos 2 semanas en la agencia matriz de Quito, como paso previo a la aceptación del sistema e inicio de operaciones. Los documentos emitidos con el nuevo sistema no serán válidos.
* Implementación progresiva del sistema sin interrumpir la emisión con el sistema actual y otros servicios de la DIGERCIC.
* Elaboración y entrega oportuna de documentación del sistema y sus componentes tanto para usuarios finales como personal de informática. Incluye documentación de la gestión del proyecto.
* Organización y facilitación del plan y documentación para entrenamiento del personal designado por la DIGERCIC en la modalidad “entrenamiento para entrenadores”.
* Régimen del mantenimiento preventivo y correctivo de todos los componentes de hardware y software del sistema.
* Gestión oportuna de incidentes y problemas del sistema en base a los niveles de servicios establecidos por la DIGERCIC. Incluye procedimientos para soporte presencial, telefónico y remoto por parte del proveedor bajo la modalidad 24x7x365 para agencias de la DIGERCIC y consulados del MREMH.
* Actualización tecnológica del sistema durante el tiempo exigido por la DIGERCIC
  1. **HITOS CLAVES Y PLAZOS DE CUMPLIMIENTO**

La siguiente figura presenta el cronograma de referencia con los hitos claves y plazos de cumplimiento, contados a partir de la firma del contrato. El proveedor deberá considerar los hitos del 1 al 4 y sus plazos como obligatorios. El proveedor deberá adecuar la propuesta y plan de trabajo considerando los hitos y plazos señalados.



La implementación del sistema deberá estar finalizada en 12 meses (1 año) después de la suscripción del contrato. Los primeros pasaportes deberán emitirse a partir del primer día del mes 6 en la agencia matriz de Quito y el despliegue en el país y en los consulados de Nueva York (USA) y Madrid (España) deberá tomar hasta 2 meses. Los primeros documentos de identidad deberán emitirse a partir del primer día del mes 8 en la agencia matriz de Quito y el despliegue en el país deberá tomar hasta 4 meses. La entrega-recepción del sistema deberá ocurrir al finalizar el mes 12 de ejecución del contrato. Los servicios post-implementación relacionados a mantenimiento, soporte, gestión de incidentes actualización y gestión del cambio del sistema deberán ser facilitados durante 36 meses (3 años) después de terminada la implementación (a partir el mes 13).

# ESPECIFICACIONES TÉCNICAS

* 1. SISTEMA DE EMISION DE DOCUMENTOS DE IDENTIDAD Y PASAPORTES **ELECTRÓNICOS (SEDIP)**

# DESCRIPCIÓN FUNCIONAL

Para obtener un documento de identidad, un pasaporte, o ambos, el ciudadano deberá presentarse en una estación de captura fija o móvil de la DIGERCIC en el país; o de un consulado del MREMH en el extranjero, previo el pago de la tasa fijada para el documento a solicitar.

El operador de la estación de captura, procederá a ingresar al Sistema Único de Registro Civil e Identidad (SURI) de la DIGERCIC y creará una solicitud de documento según el tipo requerido por el ciudadano. Los tipos de documentos podrán ser:

* Documento de identidad
* Pasaporte

Los tipos de solicitud podrán ser:

* Primera vez
* Renovación
* Duplicado (solo para documentos de identidad)

A continuación, consultará los datos demográficos del ciudadano directamente en la base de datos del Registro Civil ingresando el Número Único de Identidad (NUI) o el nombre; y procederá a validar:

* La existencia de la identidad del solicitante en base a los datos demográficos
* La supervivencia del solicitante
* La unicidad de la identidad del solicitante
* El uso de la identidad por parte del solicitante

Si la validación de los datos demográficos del solicitante presenta inconsistencias la solicitud será cancelada y se comunicará al ciudadano.

Si la validación de identidad es exitosa, se verificará los requisitos y condiciones exigibles por tipo de documento (fechas, vigencia, impedimentos, otros), se escaneará documentos de soporte (opcional), y se generará una solicitud de emisión en estado “por procesar”. De presentarse inconsistencias o novedades durante esta fase, la solicitud será cancelada y se comunicará al solicitante.

Para continuar con el procesamiento de una solicitud, el operador deberá ingresar y autenticarse en el SEDIP. La autenticación se realizará utilizando uno de los siguientes métodos de dos factores:

* ingresando usuario/contraseña y comparando una huella del operador capturada con lector contra el ABIS implementado. Este deberá ser configurado por default.
* ingresando usuario/contraseña y token lógico enviado al operador. Este podrá ser configurado cuando por alguna circunstancia el método default no funcione.

La información para autenticación de operadores en el SEDIP, como son: institución, país/ciudad, agencia/consulado, roles/permisos y usuario/contraseña, deberá previamente ser consultada al Sistema de Administración de Usuarios (SAUREG) de la DIGERCIC. De esta forma el operador utilizará el mismo usuario y contraseña del SURI en el SEDIP.

A continuación, el operador consultará una solicitud precargada en la base de datos del SEDIP ingresando el número único de identidad o el nombre del solicitante. Acto seguido, realizará la captura biométrica de las huellas dactilares, la foto del rostro y la firma manuscrita del solicitante con los equipos instalados en la estación de captura. De esta forma, se completará la solicitud con la información biométrica capturada. Posteriormente, el SEDIP enviará las imágenes de las huellas y del rostro del solicitante al ABIS. Para las solicitudes de documentos por primera vez, la búsqueda de las huellas y el rostro se realizarán contra todas las huellas y rostros previamente registrados en el ABIS. En caso que no exista registros se creará un nuevo registro biométrico en el ABIS y devolverá un resultado exitoso de validación biométrica al SEDIP. Para las solicitudes de renovación de documentos, la búsqueda de las huellas y el rostro se realizará contra las huellas y rostros del solicitante previamente registradas en el ABIS. En caso que la validación biométrica sea exitosa, el ABIS devolverá el resultado al SEDIP para que el operador envíe a producir el documento solicitado.

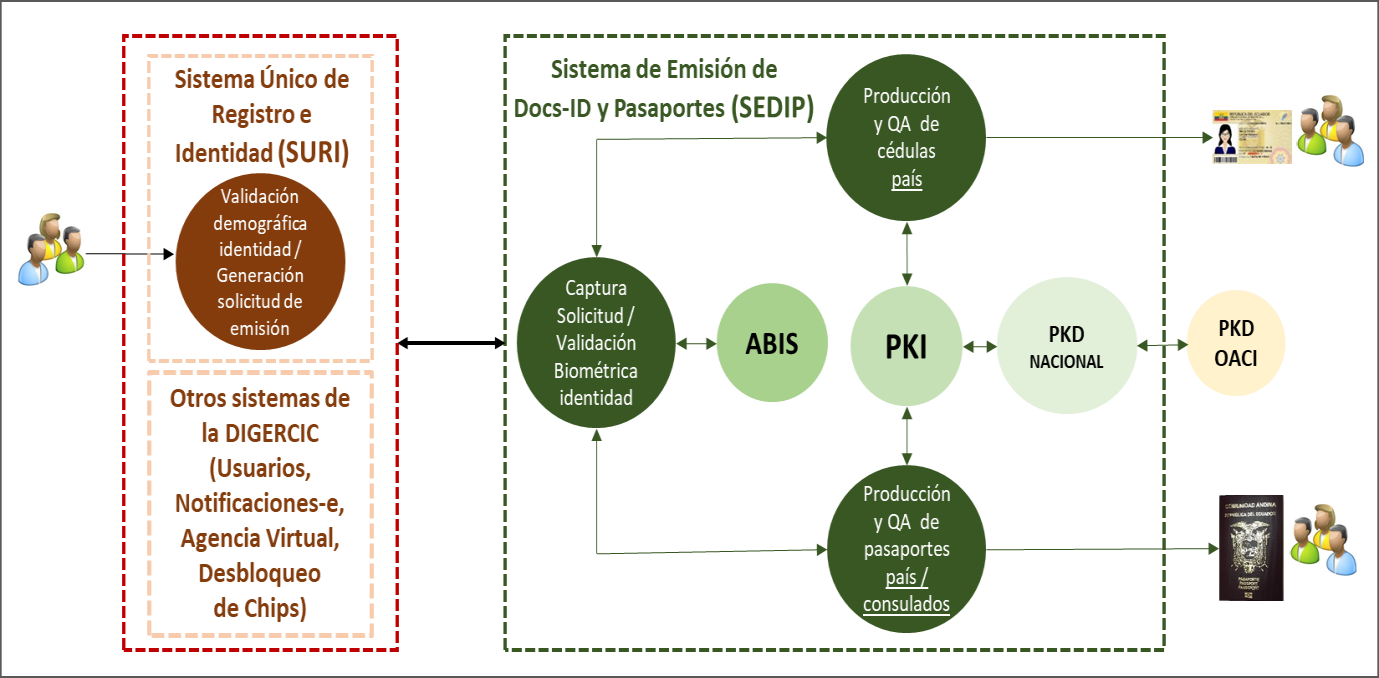
Si la validación de identidad biométrica no es exitosa, el SEDIP deberá permitir que operadores de análisis biométrico analicen y decidan sobre la validez o no de la identidad del solicitante. Si los operadores de análisis biométrico deciden que la validación de identidad biométrica es positiva, el ABIS devolverá un resultado exitoso al SEDIP para que el operador envíe a producir el documento solicitado. Por el contrario, el ABIS deberá devolver un resultado negativo de validación biométrica al SEDIP y el operador deberá cancelar la solicitud del documento y comunicar al solicitante. El SEDIP deberá permitir obtener un reporte del caso de análisis de la validación biométrica negativo, como respaldo de la cancelación de la solicitud, y para otros trámites al interior de la DIGERCIC.

Seguidamente, el SEDIP preparará los datos del documento conforme las recomendaciones vigentes de la OACI. A continuación, los datos preparados serán enviados al centro de producción asignado, donde deberán ser firmados electrónicamente para luego ser grabados (codificados) en el chip RFID del documento utilizando la impresora establecida para el efecto. La impresora realizará el control de calidad automático de la grabación leyendo los datos grabados. En caso de que la lectura sea exitosa, el sistema imprimirá los datos demográficos y biométricos en el documento. Por el contrario, el documento deberá ser registrado como rechazado y permitir la reproducción de uno nuevo. El SEDIP gestionará el inventario de documentos en blanco e insumos que se utilizará para asegurar la trazabilidad de los documentos que se producen correctamente y los rechazados.

A reglón seguido, el documento pasará al aseguramiento de calidad que incluirá la inspección manual/visual del documento producido y la comparación automática de los datos de la solicitud con los leídos del chip e impreso por medio de un lector especializado. Si el documento pasa el aseguramiento de calidad, el operador deberá registrar en el sistema para su posterior entrega. Caso contrario, el operador registrará el motivo por el cual el documento no pasó el aseguramiento de calidad y solicitará la reproducción del documento en el sistema.

En agencias o consulados que cuentan con estaciones de entrega de documentos separadas, el operador deberá entregar el documento al solicitante para su revisión. En caso que el ciudadano este conforme con el documento, el operador deberá tomar una foto del rostro del solicitante para comparar con la foto grabada en el chip del documento y que será recuperada mediante un lector especializado. Si la comparación es exitosa, el sistema activará el documento y registrará como documento entregado, con lo cual terminará el procesamiento de la solicitud de emisión. Si el ciudadano encuentra errores o defectos en el documento entregado para su revisión, el operador deberá registrar en el sistema el error o defecto, imputable a la DIGERCIC, y solicitará la reproducción del documento. La entrega de un documento de identidad (cédula) o de viaje (pasaporte) al solicitante será personal y en la agencia en la que realizó la solicitud. Por excepción y de forma parametrizable y/o con autorización de un supervisor, el sistema deberá permitir realizar la entrega de un documento sin autenticación biométrica del solicitante.

Para los documentos que se deben enviar a las agencias o consulados en los cuales se ingresó la solicitud y se realizó la captura de datos del solicitante, el operador de la estación de producción, deberá clasificar los documentos producidos previo a su envío. El SEDIP deberá permitir generar las guías de remisión o reportes de envío, conforme las cantidades de documento producidos. El SEDIP deberá asignar el estado de la solicitud a “enviado para entrega”. En la agencia de entrega, el operador deberá buscar en el sistema el documento a entregar en base al número de identidad, nombre o número de solicitud, ubicarlo físicamente y seguir el procedimiento especificado anteriormente. El siguiente diagrama representa el diseño lógico de ato nivel del SEDIP y su interrelación con sistemas de la DIGERCIC y de la OACI.



El Anexo D se especifica el diseño físico de alto nivel físico del SEDIP y sus componentes y la topología general de la red extendida de la DIGERCIC que utilizará el sistema.

* + 1. **REQUERIMIENTOS FUNCIONALES**

# CAPTURA DE DATOS DEMOGRÁFICOS Y BIOMÉTRICOS

# 7.1.2.1.1 Importar las solicitudes de emisión de documentos desde el SURI

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá:   * Importar las solicitudes de emisión de documentos (para documentos de identidad y/o pasaportes) ingresadas en Sistema Único de Registro e Identidad (SURI) de la DIGERCIC hacia la base de datos del SEDIP. El SURI se utiliza en las agencias de la DIGERCIC y los consulados del MREMH para registro de las solicitudes y captura/validación de los datos requeridos para la emisión de los documentos. * Las solicitudes contendrán la información necesaria para la emisión de un documento de identidad y/o pasaporte conforme las recomendaciones de la OACI. En general, la información de las solicitudes consistirá de: * Código único de solicitud * Tipo de documento (ej., documento de identidad o pasaporte) * Clase de solicitud (ej., nuevo, renovación o duplicado); * Categoría /ej., ordinario, diplomático) * Fechas (ej., de expedición, de caducidad, oficial) * Información demográfica (ej., nombres, apellidos, sexo, fecha nacimiento, etc.) * Datos de la transacción (ej., fecha, hora, operador, punto de atención, etc.) * Estado de la solicitud (ej., por procesar) * Trámite (ej., normal, prioritario) * Código Hash * Todos los registros de las solicitudes tendrán un código “hash” que deberá ser comprobado previo a confirmar la importación de los registros en la base de datos del SEDIIP. Se deberá asegurar la integridad y no repudio de los registros importados por medio de la comprobación del hash. La información de las solicitudes de emisión de documentos no podrá ser cambiada o editada en el SEDIP por parte de los operadores. En caso de inconsistencias, las solicitudes podrán ser canceladas para que se ingresen nuevamente desde el SURI. * La documentación del proceso para generar y comprobar el código hash será entregada a los proveedores interesados. La documentación del SW para importación de solicitudes de documentos, así como la descripción detallada de los datos se proporcionará a los proveedores interesados. * La importación deberá ser realizada invocando a un SW asíncrono implementado por la DIGERCIC. La frecuencia de importación será parametrizable y definida por la DIGERCIC (ej., cada minuto, cada 5 minutos, cada hora). La disponibilidad y capacidad del SW será responsabilidad de la DIGERCIC. La invocación/llamado del SW será responsabilidad del SEDIP. El proveedor puede considerar que, la DIGERCIC podrá hacer cambios al SW, para cumplir con requerimientos específicos de integración del proveedor. * El campo “Trámite” será utilizado para especificar si una solicitud es prioritaria. Por defecto, todas las solicitudes tendrán un trámite normal. Las solicitudes que tenga un trámite prioritario serán producidas primero que las de trámite normal. Si existieren varias solicitudes prioritarias se procesarán en base al día y hora que fueron priorizadas. El operador deberá solicitar al supervisor de agencia que autorice cada cambio de trámite de normal a prioritario, indicando el motivo. |  |  |

# Autenticar a operadores de captura de datos

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá:   * Autenticar a operadores de captura de datos mediante uno de los siguientes métodos de autenticación:   + Ingreso de usuario/contraseña; y captura de huella dactilar para validación biométrica 1 a 1, que se deberá realizar contra el ABIS, o   + Ingreso de usuario/contraseña; y de un token lógico que se deberá enviar al email y/o teléfono celular del operador. * La información sobre los puntos de atención (agencias o consulados) y operadores para acceso al SEDIP deberá ser precargada en la base de datos del SEDIP. La información será proporcionada por la DIGERCIC en un formato para carga a base de datos (ej., CSV, TXT, XML) conforme petición del proveedor. * La actualización de la información podrá ser realizada a través de un SW implementado por la DIGERCIC. La documentación del SW para consulta de información de puntos de atención y operadores se proporcionará a los proveedores interesados. * La información de puntos de atención y de los operadores no deberá ser editada/cambiada en el SEDIP. Esto para garantizar homogeneidad y consistencia de esa información en el SEDIP y el resto de sistemas de la DIGERCIC. * Alternativamente, el proveedor podrá utilizar directamente la información sobre puntos de atención (agencias o consulados), operadores, roles/permisos y usuarios/contraseñas, a través del Sistema Único de Administración de Usuarios (SAUREG) de la DIGERCIC. Este sistema permite gestionar los usuarios, permiso y roles de las aplicaciones Web de la DIGERCIC. La integración de aplicaciones al SAUREG, se realiza por medio de un SW. La documentación del SW para integración del SAUREG con una aplicación Web se proporcionará a los proveedores interesados. * El envío del token lógico al email y/o celular del operador deberá ser realizado mediante el Sistema de Notificaciones Electrónicas (SNE) de la DIGERCIC por medio de un SW. El SNE permite enviar mensajes a los emails y/o celulares de los operadores de sistemas de la DIGERCIC o a los ciudadanos para información del estado de los trámites. La documentación del SW para envío de notificaciones electrónicas se proporcionará a los proveedores interesados. * La validación biométrica 1 a 1 de una huella dactilar del operador deberá ser realizada desde la interface de acceso al SEDIP a través de un SW que el proveedor deberá implementar. El proveedor deberá documentar y entregar el código fuente del SW para autenticación 1 a 1 de huella dactilar. * La captura de la huella dactilar del operador se realizará mediante un escáner uni dactilar disponible en el kit de captura. |  |  |

* + - * 1. **Consultar/recuperar las solicitudes de emisión**

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá permitir:   * Consultar las solicitudes de emisión de documentos por procesar mediante el ingreso de: * Número Único de Identidad (NUI) del solicitante, o * Nombre del solicitante, o * Número de solicitud de emisión * Validar la información de la solicitud con el solicitante. Si la validación es positiva se procederá a captura la información biométrica.   Si la validación de la solicitud es negativa se deberá cancelar la solicitud de emisión seleccionando la causa. El estado de la solicitud deberá pasar a cancelada. Las causas de cancelación de solicitudes de documentos podrán ser:   * Información inconsistente * Información incompleta * Requerimiento del ciudadano * Otras (que se deberán poder parametrizar) |  |  |

# Capturar información biométrica desde estaciones fijas

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá:   * **Capturar huellas dactilares de los solicitantes** * Captura en-vivo de hasta las 10 huellas dactilares planas del solicitante en base al patrón 4-4-2 (4 dedos de la palma derecha; 4 dedos de la palma izquierda; y 2 dedos pulgares). Se deberá poder recapturar los patrones de huellas en casos que así lo amerite. La captura de huellas en será en escala de grises, a una resolución de al menos 500 dpi y cumpliendo con el estándar ISO/IEC 19794-4:2011. El sistema deberá guiar la captura mediante secuencia de captura, indicadores sonoros y/o visuales. * Registro si el ciudadano no tiene uno o más dedos; o no tiene una o las 2 manos. * Control de la calidad de captura de las huellas por posición incorrecta de los dedos en el escáner, deterioro de las huellas, duplicados, otros. * Segmentación de las imágenes de las huellas (una hasta diez) a partir de los patrones de captura y despliegue como vista previa en el formulario de solicitud desplegado en pantalla. * Valoración de la calidad de cada huella conforme a NIST Fingerprint Image Quality (NFIQ). Solo huellas de buena calidad se deberán almacenar en la base de datos. * Asociación de las huellas al número de dedo de las manos. * Conteo de las huellas efectivas a guardar. * Registro del número de dedo de huellas que no puedan ser capturadas (ej., por edad, por daño, por desgaste/deterioro). * Asignación automática de la clasificación dactilar VUCETICH. Se deberá poder asignar la clasificación de forma manual en caso que una o más huellas no puedan ser clasificadas automáticamente. * Despliegue de vista previa en el formulario del módulo de captura. * Compresión de las imágenes de las huellas en formato JPEG-2000 conforme a normativa y para garantizar la integración con sistemas existentes. * Almacenamiento de imágenes de las huellas conforme ISO/IEC 19794-4:2011. * Conservación del registro histórico de las imágenes de las huellas capturadas en la base de datos del SEDIP. * Configuración de la escala y granularidad de las huellas a capturar. * La captura de las huellas dactilares del solicitante se realizará mediante un escáner deca-dactilar disponible en el kit de captura. * Se deberá conservar el histórico de imágenes capturadas, inclusive si las solicitudes de emisión fuesen canceladas. * **Capturar la fotografía digital del rostro del solicitante** * Captura en-vivo una foto digital del rostro del solicitante, a todo color, con una resolución de al menos 300 dpi y cumpliendo con el estándar ISO/IEC 19794-5:2011. El sistema deberá guiar la captura mediante secuencia de captura, indicadores sonoros y/o visuales. Se deberá poder recapturar la foto en casos que así lo amerite. * Corte automático o asistido de la imagen de la foto capturada * Control de calidad para asegurar el cumplimiento estricto de las especificaciones vigentes de la OACI. Si la imagen no cumple las recomendaciones se deberá recapturar la foto. * Despliegue de vista previa en el formulario de solicitud desplegado en pantalla. * Compresión de las imágenes de las huellas en formato WSQ (Formato que gestiona la DIGERCIC). * Almacenamiento de las imágenes de las fotos en la base de datos del SEDIP conforme ISO/IEC 19794-5:2011. * Conservación del registro histórico de las imágenes de las fotos capturadas en la base de datos del SEDIP. * La captura de foto del solicitante se realizará mediante una cámara digital con telón de fondo disponible en el kit de captura. * Se deberá conservar el histórico de imágenes capturadas, inclusive si las solicitudes de emisión fuesen canceladas. * **Capturar de la firma manuscrita del ciudadano** * Captura en-vivo la firma manuscrita del solicitante en escala de grises a una resolución de al menos 300 dpi cumpliendo el estándar ISO/IEC 19794-7:2011. Se deberá poder recapturar la firma manuscrita en casos que así lo amerite. * Corte automático o asistido de la imagen de la firma capturada * Control de calidad para asegurar el cumplimiento de las especificaciones OACI vigentes. * Despliegue de vista previa en el formulario de solicitud desplegado en pantalla. * Comprimir las imágenes en formato JPEG-2000, conforme a normativa y para garantizar la integración con sistemas existentes. * Almacenar las imágenes de las firmas manuscritas en la base de datos del SEDIP conforme ISO/IEC 19794-7:2011 mínimo. * Conservación del registro histórico de las imágenes de las firmas manuscritas en la base de datos del SEDIP. * La captura de la firma manuscrita del solicitante se realizará mediante una tableta o pad de captura; o un escáner; ambos disponibles en el kit de captura. El sistema deberá permitir escoger con cual dispositivo se realizará la captura. La tableta de firma deberá el equipo por defecto. El escáner será utilizado en caso que por alguna razón el solicitante no pueda firmar directamente en la tableta por lo que deberá firmar en una tarjeta de papel en blanco, misma que será escaneada. El sistema deberá permitir configurar los dos dispositivos para este propósito. |  |  |

# Verificar biométricamente la identidad

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá:   * Enviar las imágenes de las huellas y rostro capturadas a buscar en el ABIS de acuerdo a la clase de solicitud del documento solicitado. * Buscar coincidencias 1 a 1 tanto de huellas como de rostros (bi-modal) si la clase de documento es “renovación”.   + Registro positivo de la verificación de identidad en el SEDIP si la respuesta de la búsqueda encontró 1 coincidencia de huella y 1 de foto. * Cambiar el estado de la solicitud a preparación de datos para producción del documento. * Buscar coincidencias 1 a n tanto de huellas como de rostros (bi-modal) si la clase de documento es “primera vez”.   + Registro positivo de la verificación de identidad en el SEDIP si la respuesta de la búsqueda no encontró 1 coincidencia de huella y 1 coincidencia de foto.   + Cambiar el estado de la solicitud a preparación de datos para producción del documento. * Enviar la solicitud para análisis biométrico por parte de operadores de análisis biométricos cuando la validación de identidad es negativa (falso positivo o falso negativo). |  |  |

# Analizar registros biométricos duplicados en el ABIS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá:   * Autenticar a operadores de análisis biométrico (peritos) mediante autenticación por 2 factores. * Consultar los datos y estados de la solicitud por número único de identidad o nombre del ciudadano o número de solicitud o escoger de una lista presentada al operador en orden de procesamiento. * Desplegar los datos demográficos y biométricos del solicitante y los encontrados por el ABIS * Guiar el analizar de huellas y/o rostros encontrados por el ABIS y demás información asociada. * Marcar/determinar las diferencias en los datos * Liberar la solicitud de emisión de documento al módulo de captura si la validación de identidad por los expertos es positiva. * Cancelar la solicitud de emisión del documento si la validación de identidad por los dactiloscopistas es negativa. * Generar reporte en PDF con el resultado del análisis efectuado. |  |  |

# Capturar información biométrica con kits móviles en-línea

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá:   * Establecer una conexión segura y cifrada mediante VPN entre e kit móvil y el SEDIP. * Verificar de permisos de los equipos de la estación móvil para conexión al SEDIP. * Autenticar al operador en el SURI. * Crear y llenar la solicitud de emisión de documentos en el SURI. * Autenticar al operador en el SEDIP. * Consultar una solicitud de emisión por número de documento de identidad o nombre. * Capturar de las huellas dactilares, rostro y firma manuscrita como se realiza con los kits de captura fijos. * Generar la solicitud de emisión del documento. * Imprimir la solicitud de emisión del documento para constancia del ciudadano. * Cambiar el estado de la solicitud a preparación de datos para producción. |  |  |

# 

# Capturar información biométrica con kits móviles fuera-de-línea

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Preparar el kit móvil para captura fuera de línea previo a su uso. * Actualización de la base de datos del PC del kit móvil mediante descarga de catálogos desde el SEDIP centralizado. * Creación de usuarios de captura * Autenticar al operador de captura móvil * Ingresar datos demográficos de los solicitantes * Generar las solicitudes de los documentos * Capturar huellas dactilares, rostro y firma manuscrita de los solicitantes * Imprimir las solicitudes de documentos para entrega a los solicitantes. * Exportar las solicitudes generadas de forma cifrada * Importar las solicitudes generadas al SEDIP * Analizar las solicitudes cargadas en el SEDIP * Aprobar las solicitudes correctas por el operador de captura y un operador de supervisión * Rechazar las solicitudes incorrectas por un operador de captura y un operador de supervisión * Enviar las solicitudes aprobadas a producción. * El proveedor deberá desarrollar e implementar el programa de software para ingreso y captura de información demográfica y biométrica “fuera-de-línea”, en base a los mismos requerimientos de captura “en-línea”. El programa de software deberá permitir: * Autenticar al operador mediante usuario/contraseñe y huella dactilar * Crear y editar solicitudes de emisión según el tipo: documentos de identidad o pasaportes; tipo de solicitud: primera vez o renovación y los otros datos necesarios según el tipo de documento. * Ingresar la información demográfica del solicitante * Capturar la información biométrica en-vivo: foto digital del rostro, hasta 10 huellas dactilares y la firma manuscrita * Validar automáticamente y generar la solicitud * Exportar las solicitudes en formato interoperable cifrado por operadores de captura autorizados * Importar las solicitudes al SEDIP por operadores de captura autorizados * Validar la información de las solicitudes * Aprobar la solicitud si pasa la validación de información tanto demográfica como biométrica. Se deberá implementar un flujo de aprobación por operadores de captura y supervisores * Rechazar la solicitud si no pasa la validación de información demográfica y/o biométrica. * Enviar las solicitudes aprobadas a producción de los documentos * El proveedor deberá realizar el análisis, diseño, implementación, pruebas del programa. El proveedor deberá entregar todo el código fuente de la aplicación y la documentación técnica y manuales respectivos. El proveedor deberá instalar el programa de captura “fuera-de-línea” en todas los PC’s de los kits móviles. * La DIGERCIC facilitará un documento con los catálogos de datos para uso en la aplicación de captura “fuera-de-línea”. La arquitectura de la aplicación podrá ser Web de 3 capas; o cliente-servidor de dos capas. Se deberá utilizar herramientas de software libre open source tanto para el desarrollo como para el funcionamiento/operación del programa. La información capturada deberá ser encriptada tanto a nivel de bases de datos como de archivos para garantizar su integridad y consistencia. El programa deberá reconocer y utilizar los equipos o periféricos disponibles en el kit móvil. Se deberá capturar todos los datos biométricos en un solo paso, es decir, no se permitirá la captura parcial de datos biométricos, de no ser posible se deberá poder cancelar la captura. |  |  |

* + - * 1. **Solicitudes de duplicados de documentos de identidad**

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá permitir:   * Generar solicitudes de emisión de duplicados de documento de identidad. Para esto, el proveedor deberá implementar un SW para generar solicitudes de emisión de documentos de identidad con la información demográfica y biométrica que conste en la última solicitud de emisión de documentos efectivamente producidos y entregados a los solicitantes. * La comprobación de la identidad del solicitante de un duplicado de documento de identidad se realizará al momento de la entrega del documento. El servicio de emisión de un duplicado será solo para documentos de identidad. Un duplicado de documento de identidad será distinguido del original por medio de una etiqueta en la sección visible del documento de identidad. * El proveedor deberá elaborar la documentación técnica del SW y apoyar en la integración del mismo en los sistemas de la DIGERCIC. El SW será invocado desde dos sistemas de la DIGERCIC:  1. el portal Web de servicios en-línea o la “Agencia Virtual” de la DIGERCIC. Desde la “Agencia Virtual” los ciudadanos deben poder solicitar en-línea duplicados de documentos de identidad; y escoger la agencia en la cual retirarán los mismos. 2. El SURI, para que los ciudadanos puedan solicitar duplicados de documentos de forma presencial en las agencias a las que acudan a solicitar los mismos.  * El SEDIP deberá enviar a producción la solicitud de emisión obviando la validación biométrica del ABIS. Para solicitudes de duplicados desde la “Agencia Virtual”, el SEDIP deberá considerar la agencia en la cual el solicitante retirará el documento de identidad duplicado y por consecuencia el centro de producción asignado. * La producción de documentos de identidad duplicados seguirá el mismo flujo que para los otros tipos de solicitud de emisión de documentos de identidad.   El proveedor deberá considerar que el servicio de emisión de duplicados de documentos de identidad tanto en-línea como presencial se encuentra en plena operación[[14]](#footnote-14). |  |  |

**7.1.2.1.10. Gestionar consultas/reportes y notificaciones**

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá permitir:   * Consultar el estado del avance del procesamiento de las solicitudes por cada paso del flujo o proceso de producción y la información asociada (ej., agencia, operador, fecha, hora, número de solicitud, tipo de documentos, tipos de solicitud, número único de identificación del solicitante, nombre del solicitante, estado, otro). * Consultar las solicitudes de emisión enviadas a producción por: número único de identidad, nombres o número de la solicitud. Se deberá poder exportar al PDF: la información demográfica de las solicitudes, la información demográfica más la información biométrica; o los datos de identificación del solicitante y la información biométrica. Los reportes PDF que contengan las huellas dactilares deberán indicar la escala de las mismas. * Adicionalmente, se deberá poder realizar consultas consolidadas por: país y/o extranjero, por ciudad, por agencia, por operador, por tipo de documento, por tipo de solicitud, por clase de documento, por rangos de fechas, por centro de producción, por impresora de centro de producción. Las consultas deberán desplegarse a pantalla y se podrá generar reportes en formato no editable PDF y en formatos editables (.ODF, .DOCX, .XLSX). * Consultar el estado del avance del procesamiento de las solicitudes por cada paso del flujo o proceso de producción por medio de un SW, que deberá ser implementado por el proveedor. El SW deberá permitir enviar notificaciones electrónicas a los solicitantes de acuerdo al cambio de los estados del proceso de producción de los documentos, especialmente, cuando el documento se encuentre listo para la entrega. Adicionalmente, el SE permitirá implementar una consulta en la “Agencia Virtual” de la DIGERCIC, para que los solicitantes puedan consultar el estado de avance de la producción de los documentos.   El proveedor deberá documentar y entregar el código fuente del SW para consulta de los estados de avance del procesamiento de las solicitudes de emisión de documentos. |  |  |

# PRODUCCIÓN DE DOCUMENTOS

# Preparación de datos y producción del documento

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá**:**   * **Preparar los datos del documento a producir**   + Preparar los datos demográficos y biométricos a ser codificados en el chip en base a la información de solicitudes de emisión recibidas desde las estaciones de captura de datos fijas o móviles. * **Firmar y codificar electrónicamente datos demográficos y biométricos en los chips de los documentos** * Firmar electrónicamente los datos preparados por parte de la PKI. * Enviar los datos firmados al equipo de personalización configurado para la estación de captura. * Posicionar el documento en blanco a utilizar * Escanear el número único del documento, o el código QR o número de serie del documento y verificar que se encuentre asignado a la bodega virtual del centro de producción. Si el número único del documento se encuentra inventariado se deberá asociar el número único a la solicitud caso contrario el proceso de producción se deberá suspender o cancelar. * Leer el número de serie del chip RFID del documento en blanco y verificar que se encuentre asignado a la bodega virtual del centro de producción. Si el número de serie del chip se encuentra inventariado se deberá asociar número de serie del chip a la solicitud caso contrario se deberá suspender o cancelar. * Desbloquear el chip del documento mediante el sistema criptográfico de desbloqueo implementado. * Grabar/codificar los datos en el chip del documento mediante el equipo de codificación/impresión asignado, de conformidad a las recomendaciones vigentes de la OACI. * Leer automáticamente los datos grabados en el chip con el equipo de codificación/impresión asignado. Si el equipo indica que la lectura ha sido exitosa, se continuará con la impresión gráfica; caso contrario, se deberá notificar al operador y se deberá poder reproducir el documento. El documento rechazado deberá ser enviado a la salida o tolva de documentos rechazados de la impresora. El SEDIP deberá actualizar el estado del documento como rechazado especificando la causa para fines estadísticos y de control del inventario. * **Imprimir la información demográfica y biométrica en los documentos** * Desplegar la vista previa de la información que se imprimirá en el documento de identidad o en la página de datos del pasaporte. Modalidad de despliegue “What You See Is What You Get” o WYSIWYG”. * Imprimir la información de acuerdo al tipo de documento y tipo de solicitud con el equipo de personalización/impresión asignado. El proveedor deberá considerar que los datos que se imprimen en los documentos de identidad y pasaportes pueden variar en el tiempo, particularmente, de los documentos de identidad (ej., es posible que se añadan o eliminen datos). El sistema deberá permitir cambiar el diseño o layout de los documentos para su impresión gráfica conforme cambien los datos. * Verificar automáticamente la impresión gráfica en el equipo de codificación/impresión asignado. Si el equipo indica que la verificación ha sido exitosa, se continuará con el proceso aseguramiento de la calidad; caso contrario, el SEDIP rechazará el documento y notificará el operador envíe a reproducir el documento. El documento rechazado deberá ser enviado a la salida o tolva de documentos rechazados de la impresora. El SEDIP deberá actualizar el estado del documento como rechazado especificando la causa para fines estadísticos y de control del inventario. * **Laminar la página de datos de los pasaportes** * Se deberá laminar la página de datos de los pasaportes siempre que superen el control automático de calidad de la lectura del chip y de la impresión gráfica. El SEDIP deberá registrar el número de lámina utilizada por cada pasaporte y conciliar con el inventario. * **Asegurar la calidad de los documentos producidos** * Recuperar la solicitud de emisión del documento producido por medio de escaneo o ingreso del número único del documento. * Realizar control manual y visual del documento producido. Si la calidad es satisfactoria se deberá registrar en el sistema y continuar con el proceso caso contrario se deberá suspender o cancelar el proceso y registrar en el sistema. * Colocar el documento en el lector de documentos OACI Doc 9303 * Escanear los datos impresos, leer la zona de lectura mecánica para recuperar los datos del chip, desplegar la información en pantalla. * Validar automáticamente la información impresa con la información grabada en el chip por medio de la captura de la Zona de Lectura Mecánica (MRZ, por sus siglas en ingles) y la comprobación del control de acceso básico (BAC) y control de acceso suplementario (SAC), y con la información de la solicitud de emisión del documento. * Notificar los resultados de la validación al operador. * Registrar la conformidad de la validación en cuyo caso se actualizará el estado de la solicitud a documento listo para entrega. * Enviar a reproducir el documento en caso de inconformidad entre los datos validados o por imposibilidad de lectura electrónica de los datos del chip. |  |  |

# Control de la producción de documentos

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El sistema deberá permitir al menos:   * Controlar en-línea la producción de los documentos según el tipo y centro de producción. * Desviar la producción de documentos, debido a incidentes o indisponibilidad de equipos del centro de producción predeterminado, a otros centros de producción. * Cambiar la prioridad de impresión de documentos de forma individual o en lotes en base a los números de solicitudes o números únicos de los documentos o de agencias específicas. |  |  |

# Control del inventario de documentos e insumos

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El SEDIP deberá permitir al menos:   * Cargar el inventario de documentos en blanco según su tipo y códigos de identificación únicos tanto impresos (ej., número de serie) como electrónicos (ej., número de serie del chip). Los datos serán provistos por la DIGERCIC en un archivo en formato abierto (CSV, TXT, XML, otro) en coordinación con el proveedor de los documentos en blanco. Los archivos estarán encriptados para garantizar la integridad, consistencia y no repudio de los datos. La DIGERCIC entregará un documento describiendo la estructura de archivo, nombre, campos y formato. Se deberá cargar el inventario de rollos de láminas para laminación de la página de datos de los pasaportes. Los datos deberán ser cargados de un archivo en formato abierto (CSV, TXT, XML, otro) que el proveedor del SEDIP en coordinación con el proveedor de los rollos deberán facilitar. Los archivos deberán ser encriptados para garantizar la integridad, consistencia y no repudio de los datos. El proveedor entregará un documento describiendo la estructura de archivo, nombre, campos y formato. * Controlar la carga de los archivos de inventario manteniendo la historia de las cargas y las cantidades de documentos y/rollos registrados por carga. * Asignar documentos en blanco y rollos a bodegas virtuales por cada centro de producción de agencias o consulados. * Generar órdenes de despacho o transporte de los documentos en blanco y/o rollos de las bodegas virtuales a los centros de producción. * Corregir la asignación de documentos en blanco y/o rollos a bodegas virtuales en caso de envío erróneo de los documentos o rollos. Esto se podrá realizar cuando el proceso de producción se haya suspendido en algún centro de producción y se verifique que los documentos en blanco no corresponden a los de la bodega virtual del centro de producción. Se deberá implementar un flujo de aprobación por un supervisor. * Controlar y conciliar a diario el stock total y parcial (de las bodegas virtuales) de los documentos en blanco y/o rollos * Controlar el inventario de documentos en blanco con los documentos producidos y/o los rechazados. * Emitir alertas de escasez de documentos en blanco y/o rollos tanto a nivel del inventario global como de los centros de producción. Se deberá poder parametrizar el porcentaje o valor de stock mínimo por centro de producción. * Conciliar el inventario en cualquier momento sea total o por tipo de documento en blanco, por rollos o por bodega virtual * Consultar y generar reportes del inventario por diferentes criterios: total, por bodega(s) virtual(es), por agencia, por ciudad, por cortes a fechas específicas. otros. Se deberá generar reportes en PDF o formatos editables (ej., .ODF, .ODT, .XLSX, otros). * Realizar proyecciones de uso de documentos en blanco y/o rollos en base a históricos de producción y rechazo de documentos. |  |  |

# ENTREGA DE DOCUMENTOS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El sistema deberá permitir:   * Autenticar operadores de entrega de documentos por medio de 2 factores. * Escanear o ingresar el número único del documento para consultar los datos de la solicitud de emisión del documento. * Colocar el documento en el lector de documentos OACI Doc 9303. * Capturar la fotografía del solicitante y compararla con la recuperada del documento por medio del lector de documentos. La autenticación de la identidad del solicitante mediante esta modalidad será por defecto. * Registrar el documento como entregado si la identidad del solicitante ha sido comprobada satisfactoriamente. * Enviar a reproducir el documento si el solicitante encuentra un error en la información y/o la calidad del documento. El operador podrá enviar a reproducir el documento siempre que un supervisor autorice. * Para casos particulares, el sistema deberá permitir entregar documentos sin autenticación biométrica del solicitante (modo manual). Para activar esta modalidad, se deberá implementar un flujo de aprobación por parte de un supervisor (ej., persona enferma, persona con discapacidad, recién nacido). Esta modalidad de entrega podrá ser configurada de forma permanente o temporal por estación de entrega. |  |  |

# CONSULTAS Y REPORTES

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El sistema deberá permitir   * Generar automáticamente visores de estadísticas consolidadas de captura, producción y entrega de documentos por años, meses, días, agencias, ciudades, zonas, países, tipos de documentos (documentos de identidad, pasaportes), tipos de solicitudes (primera vez, renovaciones, duplicados). * Generar reportes detallados de captura, producción y entrega de documentos por agencias y rangos de fechas a usuarios con el rol apropiado. Los supervisores de agencias podrán obtener reportes de las agencias que supervisan. Los supervisores regionales de las ciudades o regiones que supervisan y las autoridades. * Generar reportes de cuadre diarios, semanal y mensual del inventario a usuarios con el rol apropiado. Los supervisores de agencias podrán obtener reportes de las agencias que supervisan. Los supervisores regionales de las ciudades o regiones que supervisan y las autoridades. * Generar reportes de uso del sistema por usuario y rangos de fechas para acciones de auditoría a usuarios con el rol apropiado. |  |  |

# REQUERIMIENTOS NO FUNCIONALES

# ARQUITECTURA

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * La arquitectura del SEDIP deberá ser Web, es decir, con al menos capas de presentación, lógica de negocio y de base de datos. La capa de presentación o de usuario deberá ser tipo Web para todas las funcionalidades incluyendo la de captura biométrica. * Las funcionalidades de la capa de presentación deberán correr en programas navegadores o browsers en las versiones existentes a la fecha de puesta en operación. Los programas de navegación a soportar son al menos: Mozilla Firefox, Google Chrome, Microsoft Internet Explorer. * Para captura móvil fuera de línea, la arquitectura del software de la aplicación de captura demográfico y biométrico podrá ser cliente-servidor puro de dos capas o Web de 3 capas (aplicación monolítica). La aplicación deberá poder ser instalada íntegramente en las computadoras portátiles de las estaciones móviles e integrar los periféricos disponibles. |  |  |

# RENDIMIENTO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * La carga del sistema en el browser y el tiempo promedio de transacciones entre el browser y el servidor debe durar hasta 8 segundos desde los kits de captura, producción o entrega de las agencias de la DIGERCIC en el país. Esto debido a que se utilizará la red nacional de datos de la DIGERCIC. Para cumplir este requerimiento el proveedor podrá solicitar la ampliación de la capacidad de los enlaces de forma justificada. * La carga del sistema en el browser y el tiempo promedio de transacciones entre el browser y el servidor debe durar hasta 15 segundos desde los kits de captura, producción o entrega de los consulados del MREMH en el extranjero. Esto debido a que se utilizará conexiones a la Internet para acceso al SEDIP desde los consulados. Para cumplir este requerimiento el proveedor podrá solicitar la ampliación de la capacidad de los enlaces de Internet de forma justificada. * Debe grabar o codificar los datos en los chips de los documentos en un tiempo no mayor de 30 segundos una vez iniciado el proceso de codificación. * La lectura y validación de un documento de identidad o pasaportes terminados, con un lector especializado, debe tomar hasta 8 segundos. |  |  |

# CAPACIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * **Número de operadores** * Deberá soportar al menos 965 operadores concurrentes para captura fija y/o móvil, producción, entrega, supervisión, análisis biométrico y consultas/reportes. * Los operadores deberán poder acceder al SEDIP desde las agencias de la DIGERCIC en el país y los consulados del MREMH en el extranjero; o desde cualquier lugar mediante equipos móviles. * Los operadores podrán tener asignados más de un rol (ej., de captura y entrega). La tabla siguiente especifica la cantidad de usuarios promedio que podrán operar el sistema, conforme los requerimientos establecidos.      * **Producción de documentos de identidad y pasaportes** * Deberá tener la capacidad para procesar los valores máximos o picos de demanda de producción de documentos de identidad y pasaportes. Esos valores corresponden a eventos (ej., elecciones de autoridades nacionales o seccionales, consultas populares, otros); o épocas (ej., matriculas escolares, vacaciones estacionales, otros) en las cuales la demanda crece para luego estabilizarse en valores promedio.   La siguiente tabla especifica la capacidad máxima de producción que el SEDIP deberá soportar. Este valor ha sido obtenido en base al pico de producción histórica de documentos de identidad.   |  |  |  |  | | --- | --- | --- | --- | | **TIPO DE DOCUMENTO** | **CANTIDAD DE**  **PRODUCCION PICO POR HORA** | **CANTIDAD DE**  **PRODUCCION PICO REDONDEADA POR HORA** | **PROYECCION DE**  **PRODUCCION MAXIMA 8 HORAS** | | DOCUMENTO DE IDENTIDAD | 3.854 | 4.000 | 32.000 |   Por otra parte, la tabla a continuación especifica la capacidad promedio habitual de producción de documentos de identidad y pasaportes a la fecha.   |  |  |  |  | | --- | --- | --- | --- | | **TIPO DE DOCUMENTO** | **PRODUCCION**  **PROMEDIO HORA** | **PRODUCCION PROMEDIO DIA** | **PRODUCCION PROMEDIO AÑO** | | DOCUMENTO DE IDENTIDAD | 1.229 | 9.832 | 2.654.640 | | PASAPORTE | 215 | 1.720 | 464.400 | | **TOTAL** | **1.444** | **11.552** | **3.119.040** |   Por lo que el SEDIP deberá tener la capacidad de procesar un promedio habitual de 1.444 solicitudes por hora de documentos de identidad y/o pasaportes pudiendo alcanzar picos de 4.000 documentos de identidad y/o pasaportes por hora en promedio (en periodos de alta demanda). El proveedor deberá considerar el valor pico de solicitudes de emisión de documentos de identidad y pasaportes, es decir 4000, para el dimensionamiento de la capacidad de procesamiento que el SEDIP y todos los componentes de hardware y software deberán soportar.  La captura, producción y entrega de documentos de identidad y pasaportes en el país se realiza de lunes a viernes en horario de 08h00 a 17h00. Excepcionalmente se trabaja los sábados y/o domingos o en horarios extendidos, por ejemplo, durante los periodos electorales; o cuando se realizan campañas de emisión de documentos de identidad con equipos móviles.  La captura de datos para pasaportes, producción de pasaportes y entrega de pasaportes o documentos de identidad en los consultados se realizará de lunes a viernes en horario laboral de los países donde están localizados los consulados. Se deberá considerar que los consulados podrán trabajar también fines de semana u horarios extendidos.   * El proveedor deberá dimensionar la capacidad de la base de datos del SEDIP tomando como línea base, el tamaño de la base de datos demográficos y biométricos actual, que se deberá migrar al SEDIP. La base de datos actual esta implementada en un clúster de 2 nodos y el tamaño de cada nodo bordea los 5,223 TB con un crecimiento mensual promedio de 42 GB por nodo. Al presente, la trama de datos de cada captura o enrolamiento está compuesta por: datos demográficos en formato alfanumérico (ej., nombre, fecha de nacimiento, sexo, otros) y datos biométricos en formato binario (foto, firma y hasta 10 huellas dactilares). El tamaño promedio de cada dato biométrico binario es menor a 15 Kb. La tabla a continuación especifica el tamaño actual de la base de datos del sistema que se encuentra en operación.  |  |  | | --- | --- | | **CAPACIDAD BASE DE DATOS ACTUAL** | **TAMAÑO (GB)** | | Nodo 1 | 5.223,43 | | Nodo 2 | 5.223,43 | | Espacio para respaldos completos, incrementales y archive de logs. | 10.056,57 | | **TOTAL** | 20.503,43 |  * El proveedor deberá mantener o mejorar los tiempos para producción y entrega de documentos de identidad y pasaportes en las agencias que cuentan con centro de producción, sea en el país o el extranjero. Esos tiempos se medirán desde la captura de la solicitud de emisión hasta el registro de la entrega al solicitante. Los tiempos esperados se especifican en la siguiente tabla.  |  |  |  | | --- | --- | --- | | **TIPO DE AGENCIA** | **TIPO DE DOCUMENTO** | **TIEMPO PARA PRODUCCION Y ENTREGA** | | DIGERCIC CON CENTRO DE IMPRESION | CEDULA DE IDENTIDAD | HASTA 60 MINUTOS DESPUES DE LA CAPTURA DE LA SOLICITUD | | DIGERCIC/MREMH CON CENTRO DE IMPRESION | PASAPORTE | HASTA 60 MINUTOS DESPUES DE LA CAPTURA DE LA SOLICITUD | |  |  |

# DISPONIBILIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá tener una disponibilidad del 99,5% en un esquema de operación 24x7x365. Se imputarán para el cálculo, la disponibilidad de todos los componentes suministrados por el proveedor sin considerar indisponibilidad por mantenimientos planificados o de componentes que no dependen del proveedor (ej., la red datos de la DIGERCIC). El SEDIP deberá estar disponible para uso desde los puntos de atención en el país y del extranjero. * Deberá estar garantizada por medio de la implementación de un clúster, de al menos 2 nodos para las capas de base de datos, de lógica de negocio y de presentación respectivamente, en el centro de datos principal ubicado en la ciudad de Quito. Cada nodo del clúster deberá tener la capacidad suficiente para procesar toda la carga del sistema en caso de fallo de un nodo. Otros componentes, que sean críticos para la operación del sistema deberán ser implementados también en redundancia, por ejemplo, los HSM para desbloquear los chips de las tarjetas y pasaportes en blanco. * Se deberá implementar una base de datos de réplica (stand-by) para ejecución de consultas/reportes y analítica de datos, de forma que estos procesos no afecten la disponibilidad y rendimiento del sistema. |  |  |

# CONTINUIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá ser garantizada mediante la implementación del SEDIP en el centro de datos secundario o de contingencia de la DIGERCIC, ubicado en la ciudad de Guayaquil. El nodo de contingencia deberá tener la capacidad suficiente para procesar toda la carga del sistema en caso de contingencia del centro de datos principal. * Deberá soportar switch-over al SEDIP de contingencia en Guayaquil por mantenimientos planificados u otros eventos previstos que afecten la continuidad del SEDIP en el centro de cómputo principal. * Deberá soportar fail-over al SEDIP de contingencia en Guayaquil por incidentes o problemas imprevistos que afecten total o parcialmente la continuidad del SEDIP en el centro de datos principal. * Se deberá implementar equipos para obtención y restauración de respaldos a/desde disco y a/desde cintas magnéticas digitales de alta velocidad y capacidad. Los respaldos deberán ser incrementales y completos (full) en base a política de respaldos del SEDIP que recomiende e implemente el proveedor en coordinación con la DIGERCIC. El proveedor deberá suministrar equipos que soporten el formato abierto "Linear-Tape Open" (LTO, por sus siglas en inglés) en su generación estable más actual. El proceso de backup/restauración no deberá afectar el rendimiento del sistema. |  |  |

# INTEGRACIÓN CON SISTEMAS LEGADOS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * El SEDIP deberá integrarse con los siguientes sistemas de la DIGERCIC tanto para recibir como para enviar información.   + **Sistema Único de Registro e Identificación (SURI)**   El SURI es utilizado por la DIGERCIC y el MREMH para generar las solicitudes de emisión de documentos de identidad. El SEDIP deberá importar las solicitudes de emisión a su base de datos para continuar con el proceso.  Desde el SURI se deberá poder consultar los estados de avance del proceso de producción de los documentos, para actividades de conciliación y control. También se enviarán solicitudes de emisión de duplicados de documentos de identidad de forma presencial.   * + **Sistema Administración de Usuarios (SAUREG)**   El SAUREG es utilizado para administrar entidades, agencias, usuarios, roles y permisos para los sistemas de la DIGERCIC. El SEDIP deberá importar la información respectiva para gestionar la seguridad del SEDIP.   * + **Sistema de Notificaciones Electrónicas (SNE)**   El SNE se utiliza para enviar notificaciones a los operadores de sistemas y a los ciudadanos mediante emails o SMS. El SEDIP deberá permitir al SURI consultar los estados de avance del proceso de producción de los documentos, para enviar notificaciones a los ciudadanos. De igual forma, se deberá enviar notificaciones a los operadores respecto de la creación de usuarios, cambios de contraseñas, entre otros.   * + **Agencia Virtual Web de la DIGERCIC**   La Agencia Virtual es utilizada para solicitar la emisión de duplicados de documentos de identidad. El SEDIP deberá permitir producir los duplicados obviando el proceso de captura y validación de datos biométricos4   * + **Esquema de interoperabilidad de la DIGERCIC (INTDB)**   Es una base de datos interna de la DIGERCIC que es utilizada para interoperabilidad con entidades externas por medio de conexiones de base de datos (ej., vistas materializadas) o mediante SW que la DIGERCIC ha implementado (ej., SW para consultar la fecha de expedición de un documento de identidad). El esquema de interoperabilidad es utilizado por entidades públicas externas de forma permanente. Bajo este esquema, el proveedor deberá implementar programas de software de base de datos para enviar la información de los documentos producidos en el SEDIP a la base de datos de interoperabilidad de la DIGERCIC.   * + **Sistema criptográfico de desbloqueo de chips**   Es un proceso criptográfico que se deberá ejecutar para desbloquear los chips RFID de los documentos en blanco como paso previo a la personalización electrónica. Si los chips no son desbloqueados no se podrá codificar electrónicamente los documentos.  El proveedor deberá implementar programas de software para leer las llaves almacenadas en los chips de los documentos y validarlas contra las claves maestras que estarán almacenadas en equipos HSM y desbloquear el chip. Las llaves maestras serán entregadas por la DIGERCIC al proveedor para la carga en los HSM tanto de documentos de identidad como de pasaportes, que funcionarán por separado.   * + **Esquema de inventario de documentos en blanco**   El inventario de documentos en blanco con información que identifica unívocamente a los documentos y los chips se entregará al proveedor en un archivo cifrado en formato abierto (CVS, TXT, XML), previo a la distribución a los centros de producción en el país y en el extranjero.  El proveedor deberá desarrollar una interface para cargar el archivo de inventario al SEDIP con el objeto de gestionar el inventario y la trazabilidad del uso de los documentos en blanco, documentos producidos y documentos rechazados.  La DIGERCIC facilitará la documentación necesaria para los componentes de integración y el apoyo técnico que corresponda para su implementación.  De requerirse otras integraciones para el funcionamiento correcto del SEDIP el proveedor deberá documentar e implementar las mismas.   * + **Directorio de Claves Públicas de la OACI**   El proveedor deberá integrar la infraestructura del Directorio de Claves Públicas Nacional de la PKI al Directorio de Claves Públicas de la OACI. Se deberá aplicar las políticas, procedimiento y tecnologías que especifique la OACI para ese fin. El proveedor deberá implementar, probar y poner en operación el esquema de integración. La DIGERCIC facilitará el apoyo técnico y logístico a su alcance.   * Se deberá utilizar SW tipo SOAP para integración de sistemas. Se podrá implementar interfaces de base de datos para integración de sistemas como mecanismo de contingencia a los SW. * Se deberá especificar en la documentación de arquitectura lógica y física de la integración en caso que se utilice interfaces de base de datos, por ejemplo, vistas materializadas, conexiones directas, etc., |  |  |

# USABILIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá disponer de menús, opciones e interfaces de usuario que faciliten el uso y entendimiento del sistema * Las interfaces deberán disponer de opciones de ayuda en línea, tips o mensajes de ayuda * Deberá desplegar mensajes de información, alerta o error claros y entendibles * El idioma de las interfaces deberá ser español * Deberá permitir customizar las interfaces de usuario con información institucional. Al menos el nombre y/o el logotipo de la DIGERCIC. |  |  |

# SEGURIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El sistema deberá permitir:   * Gestionar roles y permisos para asignación a operadores. * Gestionar usuarios y asignar roles. Los roles de operador serán al menos: de captura para documentos de identidad y/o pasaportes, de producción, de entrega de documentos de identidad y/o pasaportes, pudiendo un operador tener hasta los 3 roles (ej., en agencia pequeñas o en estaciones de captura y entrega). Adicionalmente se podrá asignar roles de supervisor para funcionarios que aprueban o autorizan ciertas transacciones o son jefes de agencia. De igual forma el rol de operador de análisis biométrico para análisis de solicitudes que terminan en el ABIS. Se crearán roles adicionales para consultas y reportes por agencia(s), ciudades, provincias, zonas y a nivel nacional que se asignarás a directivos locales, provinciales, zonales y nacionales. * Resetear las contraseñas de los usuarios por olvido. Las contraseñas deberán ser fuertes de al menos 10 caracteres. Se deberá obligar el ingreso de al menos una letra en mayúscula, un número entero y un carácter especial permitido. El sistema deberá enviar el link del formulario en el cual se registrarán o reestablecer las contraseñas. El sistema no deberá enviar contraseñas por email o SMS, salvo que sean temporales para obligar al operador a cambiar la contraseña cuando acceda al sistema. El algoritmo de cifrado de las contraseñas deberá utilizar claves de tamaño apropiado que eviten ataques al cifrado. Se deberá registrar las veces que un usuario cambia de contraseña incluyen la fecha y hora. * Cancelar/suspender o desactivar cuentas de usuarios. No se deberá poder eliminar cuentas de usuarios después que hayan ejecutado transacciones. * Importar datos personales y para creación de usuarios. La DIGERCIC proporcionará la información de los usuarios incluyendo la foto. * Asignar uno de métodos de autenticación que deberán utilizar los usuarios: usuario/contraseña; usuario/contraseña y token lógico; o, usuario/contraseña y validación biométrica de huella. * Crear una o más organizaciones (multi-organización) y crear usuarios por cada institución. Se deberán poder crear usuarios separados de la DIGERCIC y del MREMH. Los usuarios podrán tener uno o más permisos y/o roles. * Consultar las actividades de un usuario en el sistema por: número único de identidad o nombres. Se deberá poder consultar las actividades por rangos de fechas; por rangos de hora; por kit de captura, producción o entrega. * Controlar el tiempo de sesiones inactivas y bloquear el acceso. * Bloquear el acceso al sistema de forma temporal por intentos fallidos de acceso. El número de intentos fallidos por defecto será 3 y el tiempo de bloqueo por defecto será 5 minutos. * Obligar a que las contraseñas caduquen cada cierto periodo de tiempo configurable en el SEDIP. El tiempo por default será de 90 días. Los usuarios deberán registrar una nueva contraseña cuando caduquen las utilizadas. * Garantizar que el formulario de acceso (o login) mitigue vectores de vulneración más conocidos (ej., SQL/XML-injection, man in the middle, de fuerza bruta/diccionario o los que especifica la OWASP. * Informar al usuario que se encuentra conectado, el nombre del usuario, la foto del usuario, el rol, la fecha y hora, la agencia. * Desplegar una opción permanente para consultar los “Términos de uso del sistema”. La DIGERCIC proporcionará el archivo de texto a ser desplegado. Todo usuario que acceda por primera vez a utilizar el sistema deberá registrar que ha leído y entendido los “Términos de uso del sistema”. * Obtener consultas a pantalla de la actividad de los usuarios por rangos de fechas, por tipo de acción, por módulo utilizado. La información podrá ser generada como reporte o informe en PDF. * Deberá implementar uno de los siguientes esquemas de autenticación para acceso al sistema:   + Usuario/contraseña y Token lógico enviado al email del operador sea en el país o en el extranjero; y/o enviado al teléfono celular del operador del sistema (mediante un SMS) solo en el país.   + Autenticación biométrica por comparación de una huella dactilar o del rostro del operador contra los elementos similares registrados en el ABIS de la DIGERCIC. * Deberá generar logs detallados para trazabilidad de las actividades de los usuarios en el sistema. Toda transacción deberá establecer al menos: la fecha/hora, usuario, acción, rol, equipo, agencia, entre otros. No se deberá borrar lógica- o físicamente ningún dato de las bases de datos. Las transacciones de actualización deberán respaldar el registro a cambiar como paso previo a la actualización correspondiente. Se deberá llevar un registro histórico de todas las transacciones de las bases de datos por día, mes y año. Esto facilitará el respaldo y/o restauración de esos datos frente auditorías internas o externas. * Se deberán encriptar las conexiones remotas a través de la Internet entre los kits de captura, centros de producción y kits de entrega con el SEDIP para minimizar riesgos de seguridad. * La DIGERCIC cuenta con un sistema único de creación de usuarios, permisos y roles para la autenticación en todas las aplicaciones Web internas. La interfaz de integración es un SW tipo SOAP que es invocado por las aplicaciones internas. Este SW podrá ser utilizado por el proveedor para integrarlo al SEDIP y de esa forma utilizar el esquema de autenticación único de la DIGERCIC en lugar del que se provea. * Soportar TLS y HTTPS. Todo URL de aplicación o Servicio Web deberá ser invocado mediante HTTPS. |  |  |

# ESTÁNDARES Y BUENAS PRATICAS APLICABLES

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Recomendaciones de la OACI Doc 9303 versión 2015 para emisión de documentos de viaje de lectura por máquinas, donde corresponda. * Normas de la Organización de Estándares Internacional (ISO)[[15]](#footnote-15), por sus siglas en inglés) aplicables que deben ser especificadas por el proveedor. |  |  |

# SOFTWARE A SER UTILIZADO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * El software base, para implementar el SEDIP, deberá ser de preferencia software libre open source o de tecnología abierta; y por excepción podrá ser privativo. Se deberá suministrar todas las suscripciones de uso perpetuo a nombre de la DIGECIC. El software base deberá estar basado o correr en Linux y comprenderá, pero sin estar limitado a:   + Sistemas operativos   + Sistemas de virtualización   + Gestores de base de datos   + Servidores Web   + Servidores de aplicaciones Web   + Herramientas de programación   + Software de respaldo/restauración   + Sistemas de email   + Servicios Web   + Software de monitoreo * Los sistemas, subsistemas, componentes o herramientas/programas de software privativos, que se utilicen para implementar el SEDIP, deberán ser especificados detalladamente por el proveedor, y se deberá suministrar todas las licencias de uso perpetuo a nombre de la DIGERCIC. * Cualquier componente de software que sea programado conforme los requerimientos establecidos por la DIGERCIC deberá ser libre y su código fuente deberá ser entregado a la DIGERCIC. |  |  |

# IMPLEMENTACIÓN

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá poder ser implementado en ambientes virtuales o deberá poder operar en servidores virtuales. * Se deberá proveer el hardware necesario para implementación del sistema en ambientes virtualizados de acuerdo con las consideraciones de capacidad, disponibilidad, continuidad y rendimiento antes especificadas. * La virtualización aplicará a la instalación de alta disponibilidad en el centro de datos principal; y a la instalación de contingencia en el centro de datos secundario. * En caso de que el SEDIP no pueda ser implementado en ambientes virtuales, deberá ser así especificado por el proveedor. * Se deberá proveer un (1) ambiente de pruebas del SEDIP que tenga una capacidad de hasta el 1% de la producción anual proyectada de documentos identidad y pasaportes. La implementación podrá ser completamente virtual en el centro de datos principal de la DIGERCIC en la ciudad de Quito. Se deberá proveer el equipamiento y licencias/suscripciones de software necesarias. Incluye un ABIS y PKI de pruebas integrados al SEDIP de pruebas. * La DIGERCIC requiere que los equipos a ser provistos sean hiperconvergentes. * El proveedor deberá especificar los requerimientos de conectividad, de energía, de enfriamiento, de espacio, de cantidad y tipo de tomas eléctricas, y cual información necesaria para instalación de los equipos en los centros de datos principal y secundario. * La DIGERCIC entregará la documentación de los procedimientos que el proveedor deberá tomar en cuenta para la puesta en operación de los equipos en los centros de cómputo. El proveedor deberá suministrar todos los accesorios, materiales, partes y piezas necesarios para la puesta en operación de los equipos. La puesta en operación de los equipos en los centros de cómputo es en la modalidad “llave en mano”. * El proveedor deberá documentar como quedan los equipos instalados conforme la arquitectura lógica y física que haya propuesto. La documentación deberá incluir los diagramas lógicos y físicos de detalles que especifiquen el lugar y función de cada componente de hardware y el software instalado. Se deberá anexar un registro fotográfico y un video de la instalación de los equipos en los centros de cómputo. * El proveedor deberá proponer un plan de entrenamiento a personal técnico de la DIGERCIC en temas relacionados a: la arquitectura lógica y física, configuración, afinamiento, monitoreo, “troubleshooting” de los componentes de hardware y software del SEDIP. El plan será ejecutado, previa aprobación y en coordinación con la DIGERCIC. |  |  |

# ADMINISTRACIÓN/PARAMETRIZACION Y MONITOREO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * **Administrar/Parametrizar las diferentes funcionalidades del sistema** * Configuración de entidades (DIGERCIC, MREMH), agencias/ consulados, países, ciudades, usuarios * Inventario de kits de captura, kits de producción, kits de entrega de documentos autorizados para acceder al sistema * Configuración de agencias y consulados de captura y entrega; y de captura producción y entrega. * Configurar la producción de documentos en determinadas impresoras para estaciones de captura específicas. * Configuración de roles, permisos y usuarios * **Parametrizar la operación del sistema para, al menos:** * Captura de datos demográficos y biométricos. * Producción de documentos. Asignación de kits de captura a sus kits de producción por default. * Codificación/personalización electrónica * Entrega de documentos. * Inventario de documentos en blanco y rollos de laminas * Otros a juicio del proveedor. * Se deberá poder monitorear de forma centralizada el funcionamiento del SEDIP desde la captura de datos, pasando por la producción de documentos y la entrega de estos a los ciudadanos en las agencias de la DIGERCIC en el país y en los consulados del MREMH en el extranjero.   Se deberá poder monitorear de forma centralizada el funcionamiento de la infraestructura del SEDIP implementada en los centros de cómputo principal y de contingencia para verificar la capacidad, disponibilidad y rendimiento. La herramienta de monitoreo deberá de arquitectura Web accesible mediante un programa navegador o browser. La herramienta será utilizada solo por administradores del sistema designados por la DIGERCIC. La herramienta de monitoreo podrá ser de software libre open source. |  |  |

# SISTEMA AUTOMATIZADO DE IDENTIFICACIÓN BIOMÉTRICA (ABIS)

# DESCRIPCIÓN FUNCIONAL

Una vez que el operador ha capturado los datos biométricos del solicitante en la estación de captura, el SEDIP deberá ejecutar la validación biométrica de la identidad interactuando con el ABIS.

Para el tipo de solicitudes de documentos por primera vez, el ABIS deberá comparar las huellas dactilares y/o el rostro del solicitante contra todas las huellas dactilares y rostros almacenados en el ABIS (comparación 1 a n). Si la comparación no encuentra coincidencias, el ABIS insertará (enrolará) las huellas y el rostro del solicitante en la base de datos. El ABIS deberá devolver un resultado de la validación biométrica de la identidad al SEDIP, para que el proceso de emisión pueda continuar.

Para el caso de solicitudes de documentos por renovación, el ABIS deberá comparar las huellas dactilares y/o el rostro del solicitante contra las huellas dactilares y el rostro del solicitante almacenadas previamente en el ABIS (comparación 1 a 1). Si la comparación encuentra una y solo una coincidencia, el ABIS actualizará las huellas y rostro existentes del solicitante con las actuales en la base de datos. El ABIS deberá devolver un resultado positivo de la validación biométrica de la identidad al SEDIP, indicando que el proceso de emisión puede continuar.

Si la comparación de huellas y/o rostros encuentra más de una coincidencia, el ABIS deberá devolver un resultado negativo de la validación biométrica de la identidad al SEDIP; y suspender el proceso de emisión hasta que un operador de análisis biométrico realice el análisis respectivo. El ABIS deberá generar un caso de análisis biométrico y bloquear la solicitud y cualquier cambio de información demográfica y biométrica de los casos por analizar, hasta que se realice el análisis respectivo.

Para realizar el análisis biométrico, un operador, con rol de analista biométrico, se autenticará en el SEDIP y deberá poder seleccionar o buscar el caso de análisis de una lista presentada por el sistema. El sistema deberá permitir buscar el caso por: número único de identidad del solicitante, nombre del solicitante, número de solicitud, agencia de captura, o número de caso. El sistema deberá permitir enviar notificaciones a los operadores con rol de analista biométrico, tanto al email como al celular del operador, cada vez que el ABIS genere un caso de análisis.

Luego de seleccionar el caso de análisis, el sistema deberá desplegar simultáneamente la información demográfica y biométrica de los duplicados identificados. Si el operador confirma (adjudica) la identidad del solicitante automáticamente se levantará el bloqueo para que el proceso de emisión pueda continuar. Si el operador no confirma (no adjudica) la identidad del solicitante automáticamente se cancelará el proceso de emisión y el sistema notificará al operador para que a su vez informe al solicitante.

El SEDIP deberá permitir consultar los estados por los que ha pasado la solicitud bloqueada, así como el histórico de solicitudes de documentos, según el tipo, realizada por el solicitante.

El sistema deberá permitir a los operadores de análisis biométrico obtener el reporte correspondiente del análisis realizado en PDF. El operador de análisis biométrico deberá aplicar el procedimiento operativo establecido por la DIGERCIC, para estos casos.

* **Sistema de SW de Autenticación e Identificación**

El ABIS deberá permitir realizar consultas 1 a 1 y 1 a n de huellas dactilares y rostros por medio de SW, que podrán ser invocados por sistemas internos de la DIGERCIC, para facilitar a su vez, servicios a entidades externas.

# REQUERIMIENTOS FUNCIONALES

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El ABIS deberá permitir:   * Identificar personas por comparación 1 a n de huellas dactilares planas y/o de rostros capturados en-vivo mediante el SEDIP en las agencias de la DIGERCIC en el país y de consulados del MREMH en el extranjero. * Autenticar personas por comparación 1 a 1 de huellas dactilares planas y/o de rostros capturados en-vivo mediante el SEDIP en las agencias de la DIGERCIC en el país y de consulados del MREMH en el extranjero. * Identificación 1 a n por comparación de huellas dactilares y rostros por medio de SW. Los datos biométricos para identificación deberán ser enviados a los SW desde sistemas internos de la DIGERCIC. El SW biométrico no será expuesto directamente a entidades externas por norma de seguridad. * Autenticación 1 a 1 por comparación de huellas dactilares y/o de rostros por medio de SW. Los datos biométricos para autenticación deberán ser enviados a los SW desde sistemas internos de la DIGERCIC. El SW biométrico no será expuesto directamente a entidades externas por norma de seguridad. * Identificación 1 a n por comparación de huellas deca-dactilares, fragmentos de huellas, huellas latentes y huellas necro-dactilares por medio de SW asíncronos. El ABIS deberá responder al SW con hasta 10 candidatos, ordenados por precisión de la búsqueda. Se deberá implementar un SW adicional para consultar los datos de identidad del candidato seleccionado. Los datos biométricos para identificación deberán ser enviados a los SW en formato NIST estándar para intercambio de información biométrica. La respuesta deberá ser generada también en archivos NIST estándar. Ningún SW biométrico será expuesto directamente a entidades externas por norma de seguridad. Estas búsquedas deberán poder ser calendarizadas para que sean ejecutadas en horarios fuera de oficina de Ecuador. Es decir, de 19h00 a 07h00.   El proveedor deberá desarrollar una aplicación Web para consumir los SW de autenticación e identificación de huellas y/o rostros implementados. La aplicación deberá permitir al menos:   * **Autenticar personas por huella o rostro en imagen** * Capturar el número de identidad del ciudadano * Capturar una huella o la foto del ciudadano * Validar la calidad de la huella o de la foto * Registrar la fecha y hora * Buscar una coincidencia invocando al SW de autenticación 1 a 1 por huella o por foto * Registrar el resultado de la búsqueda * Si existe una coincidencia se deberá desplegar en pantalla y generar en PDF reporte con los datos de la consulta, el número de identidad y el nombre de la persona encontrada y la precisión de la consulta. * Si no existe una coincidencia se deberá desplegar el mensaje en pantalla o el error correspondiente. * **Identificar personas por huella o rostro en imagen** * Crear y llenar una solicitud para identificación * Capturar una huella o la foto del usuario * Validar la calidad de la huella o de la foto * Registrar la fecha y hora * Buscar una coincidencia de la huella o la foto invocando al SW de identificación 1 a n por huella o por foto * Registrar el resultado de la búsqueda * Si existe una coincidencia se deberá desplegar en pantalla y/o generar en PDF reporte con los datos de la transacción de consulta, número de caso, número de identidad, nombre de la persona encontrada, foto de la persona y precisión de la consulta. * Si no existe una coincidencia se deberá desplegar el mensaje en pantalla o el error correspondiente. * **Identificar personas mediante huellas dactilares, fragmentos, latentes y necro-dactilares en archivos NIST** * Crear un caso de identificación * Cargar el archivo NIST * Parametrizar, priorizar y calendarizar la búsqueda por tipo de huellas * Registrar la fecha y hora de la parametrización * Ejecutar automáticamente la consulta de acuerdo al calendario * Registrar el resultado de la búsqueda por orden de precisión y los archivos NIST con las huellas resultantes de hasta 10 candidatos * Descargar los archivos NIST para análisis por expertos * Consultar información demográfica y la foto correspondiente a un candidato * Registrar el resultado de la consulta demográfica y la foto * Generar en PDF reporte del caso de identificación. |  |  |

# REQUERIMIENTOS NO FUNCIONALES

# MIGRACIÓN Y SINCRONIZACIÒN DE HUELLAS Y ROSTROS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Se deberá migrar todas las imágenes de las huellas deca-dactilares, fotos de rostros y firmas manuscritas de los ciudadanos y la información demográfica necesaria registrada en la base de datos del sistema actual de cedulación a la base de datos del SEDIP. Se deberá considerar que los solicitantes tendrán tantos registros de datos biométricos como tantas veces haya solicitado un documento de identidad. * Se deberá enrolar las huellas y rostros más actualizados en el ABIS y se deberá ejecutar un proceso de de-duplicación de las huellas dactilares para asegurar la unicidad de cada identidad que inserte en el ABIS durante el proceso de migración. Adicionalmente, se deberá implementar al menos 5 estaciones de análisis biométrico, por cuenta del proveedor, para análisis biométrico de casos de doble identidad, que pudieren resultar del proceso de de-duplicación de huellas del ABIS. El proveedor deberá entrenar al personal designado por la DIGERCIC para esa actividad para garantizar la integridad, eficacia y completitud del proceso de migración.   La DIGERCIC tiene completo acceso a la base de datos de datos biométricos del sistema actual de cedulación y podrá apoyar al proveedor en el proceso de migración y posterior enrolamiento en el ABIS.   * A la fecha, la base de datos biométrica tiene aproximadamente 12 millones de registros biométricos de huellas deca-dactilares únicas, fotos y firmas de ciudadanos mayores de 12 años. Adicionalmente, se cuenta con registros biométricos de ciudadanos menores a 12 años distribuidos como señala la siguiente tabla:  |  |  | | --- | --- | | **RANGOS DE EDADES** | **CANTIDAD DE REGISTROS BIOMETRICO** | | MENORES A 6 AÑOS | 1’044.606 | | ENTRE 6 y 12 AÑOS | 1’940.432 | | MAYORES A 12 AÑOS | 12’042.545 | | **TOTAL** | **15’027.583** |   En base a la tabla anterior, el proveedor deberá insertar los datos de los ciudadanos entre 6 a 12 años, que suman 1’940.000, registros a la fecha. De esta forma, la base de datos del SEDIP y del ABIS tendría de partida 13’982.977 registros.   * Las imágenes de las huellas tienen una resolución de 500 dpi en escala de grises en formato WSQ. Todas las huellas han sido capturadas en-vivo utilizando escáneres deca-dactilares y han pasado filtros de control de calidad. Cabe acotar que no se han capturado ni registrado huellas dactilares desde otros soportes (ej., papel o cartolas). El proveedor deberá asumir que la calidad de las huellas capturadas es muy buena. En caso que, se encontraren imágenes de huellas de calidad deficiente, el proveedor deberá procesar las mismas para lograr una calidad aceptable según las recomendaciones internacionales. * Las imágenes de las fotos tienen una resolución de al menos 96 dpi a color en formato JPG. Las fotos han sido capturadas en-vivo con cámaras digitales, sus dimensiones son 360 x 480 pixeles aproximadamente y tienen un peso de hasta 20Kb. Las fotos son a color y han pasado un filtro de cumplimiento de los requerimientos exigidos por la OACI. No se han capturado ni registrado fotos desde otros soportes (ej., papel o cartolas). Por esta razón, el proveedor deberá asumir que la calidad de las fotos capturadas es muy buena. En caso que, se encontraren imágenes de rostros de calidad deficiente, el proveedor deberá procesar las mismas para lograr una calidad aceptable según las recomendaciones internacionales. * El proveedor deberá implementar un proceso de sincronización bidireccional entre la base de datos y el AFIS del sistema actual de cedulación con la base de datos y el ABIS del SEDIP. Esto para garantizar la integridad, igualdad y completitud de la información en los dos sistemas una vez que comience el despliegue progresivo del SEDIP. La DIGERCIC continuará utilizando el sistema de cedulación actual hasta que termine la implantación completa del SEDIP.   Los datos biométricos de un solicitante procesados con el sistema actual deberán ser sincronizados con el SEDIP, y viceversa, tanto para solicitudes de nuevos documentos como para renovaciones. De esta forma, las búsquedas de huellas 1 a n, que se ejecutan para solicitudes de nuevos documentos, así como las búsquedas de huellas 1 a 1, que se realizan para solicitudes de renovación de documentos, deberán efectuarse tanto en el AFIS como el ABIS, o viceversa; e insertar o actualizar los datos en ambos sistemas, según corresponda.  La base de datos del SEDIP y del ABIS deberán estar completas y sincronizadas con las del sistema actual de cedulación previo a cualquier prueba funcional del SEDIP. |  |  |

# ARQUITECTURA

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * La arquitectura del ABIS podrá ser cliente-servidor de 3 capas: presentación, lógica de negocio y base de datos. En ese caso, la capa de presentación o de usuario deberá ser tipo Web y correr en programas navegadores o browsers (por ejemplo, Mozilla Firefox y/o Google Chrome y/o Microsoft Internet Explorer) en sus últimas versiones. El proveedor deberá especificar la arquitectura del ABIS a implementar en caso que sea diferente a la señalada en el párrafo anterior. * El diseño arquitectónico de los flujos de búsquedas 1 a 1 y 1 a n para el sistema de SW, deberá considerar evitar afectaciones de cualquier tipo a las búsquedas biométricas 1 a 1 y 1 a n solicitadas desde los kits de captura, producción y entrega de documentos, tanto en el país como en el extranjero. De esta forma se evitará degradar el servicio de emisión de documentos de identidad y pasaportes. * La arquitectura no deberá contemplar componentes de hardware privativos para realizar las comparaciones biométricas o acelerar las mismas. |  |  |

# RENDIMIENTO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * El ABIS debe soportar mínimo 965 operadores concurrentes para autenticación biométrica de huella para acceso al sistema durante las horas laborables. * Las búsquedas 1 a n de huellas dactilares o de rostros desde kits de captura podrá durar hasta 8 segundos. El tiempo se medirá desde que llegan los datos al ABIS. El ABIS deberá utilizar las mejores 4 huellas del set deca-dactilar para la búsqueda 1 a n. * Las búsquedas 1 a 1 de huellas dactilares o de rostros para el SEDIP podrá durar hasta 3 segundos. El tiempo se medirá desde que llegan los datos al ABIS. * Las búsquedas 1 a n de huellas dactilares o de rostros mediante SW podrá durar hasta 10 segundos. El tiempo se medirá desde que llegan los datos al ABIS. * Las búsquedas 1 a n de fragmentos de huellas, huellas latentes y huellas necro-dactilares mediante SW podrán durar hasta 48 horas. El tiempo se medirá desde que llegan los archivos NIST al ABIS. Estas búsquedas deberán ser ejecutadas entre las 19h00 y las 07h00 del día siguiente. Salvo excepción, estas búsquedas podrán ser priorizadas para que se ejecuten fuera de ese horario. |  |  |

# CAPACIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá tener capacidad para buscar en 160 millones de huellas y 16 millones de rostros. Estas cantidades corresponden al número de licencias solicitado para el ABIS, es decir, 16’000.000 de licencias (1 licencia biométrica por individuo). * Para la validación biométrica de identidad a realizase en el proceso de emisión de un documento, el ABIS deberá permitir realizar consultas de identificación 1 a n, y de autenticación 1 a1 de huellas dactilares y rostros según el tipo de solicitud: primera vez o renovación. Cada validación de identidad demandará hasta 2 consultas al ABIS. * El proveedor deberá considerar que a la fecha un promedio del 85% de solicitudes de documentos de identidad son renovaciones y en promedio del 15% corresponde a nuevos documentos de identidad. De acuerdo a estos porcentajes, la siguiente tabla indica las cantidades pico de solicitudes de documentos según el tipo de solicitud.      * Dado que la producción promedio usual por hora de documentos a la fecha bordea 1.444 documentos; el resto de la capacidad del ABIS deberá ser utilizada para consultas 1 a 1 y 1 a n, en los porcentajes especificados. * Se deberá implementar un SW específico para ejecutar hasta 50 consultas diarias de identificación 1 a n de fragmentos de huellas, huellas latentes y huellas necro-dactilares. Estas búsquedas deberán ser parametrizables para ser ejecutadas en horas no laborables de Ecuador. Por ejemplo, de 19h00 a 07h00 del día siguiente. Por excepción, las búsquedas pueden ser enviadas durante el día. Cabe anotar, que el ABIS será utilizado en los consulados, pero la demanda de producción de documentos es menor. |  |  |

# DISPONIBILIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá tener una disponibilidad del 99,5% en un esquema de operación 24x7x365. Se imputarán para el cálculo, la disponibilidad de todos los componentes suministrados por el proveedor sin considerar indisponibilidad por mantenimientos planificados o de componentes que no dependen del proveedor (ej., la red datos de la DIGERCIC). El ABIS deberá estar disponible para uso desde los puntos de atención en el país y del extranjero. * Deberá estar garantizada por medio de la implementación de un clúster, de al menos 2 nodos para las capas de base de datos, de lógica de negocio y de presentación respectivamente, en el centro de datos principal ubicado en la ciudad de Quito. Cada nodo del clúster deberá tener la capacidad suficiente para procesar toda la carga del sistema en caso de fallo de un nodo. Otros componentes, que sean críticos para la operación del sistema deberán ser implementados también en redundancia. |  |  |

# CONTINUIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá ser garantizada mediante la implementación del ABIS en el centro de datos secundario o de contingencia de la DIGERCIC, ubicado en la ciudad de Guayaquil. El nodo de contingencia deberá tener la capacidad suficiente para procesar toda la carga del sistema en caso de contingencia del centro de datos principal. * Deberá soportar switch-over al ABIS de contingencia en Guayaquil por mantenimientos planificados u otros eventos previstos que afecten la continuidad del SEDIP y/o el ABIS en el centro de cómputo principal. * Deberá soportar fail-over al ABIS de contingencia en Guayaquil por incidentes o problemas imprevistos que afecten total o parcialmente la continuidad del SEDIP y/o el ABBIS en el centro de datos principal. * Se deberá implementar equipos para obtención y restauración de respaldos a/desde disco y a/desde cintas magnéticas digitales de alta velocidad y capacidad. Los respaldos deberán ser incrementales y completos (full) en base a política de respaldos del SEDIP que recomiende e implemente el proveedor en coordinación con la DIGERCIC. El proveedor deberá suministrar equipos que soporten el formato abierto "Linear-Tape Open" (LTO, por sus siglas en inglés) en su generación estable más actual. El proceso de backup/restauración no deberá afectar el rendimiento del sistema. |  |  |

# INTEGRACIÓN DEL ABIS CON EL SISTEMA DE EMISION

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * De preferencia, la integración se deberá realizar por medio de SW tipo SOAP o REST. De utilizarse otro tipo de interfaces, por ejemplo, a través de sistemas de email o de base de datos, se deberá especificar en la documentación de la arquitectura lógica y física del ABIS. |  |  |

# USABILIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá disponer de menús, opciones e interfaces de usuario que faciliten el uso y entendimiento del ABIS * Las interfaces deberán disponer de opciones de ayuda en línea, tips o mensajes de ayuda * Deberá desplegar mensajes de información, alerta o error claros y entendibles * El idioma de las interfaces deberá ser español. |  |  |

# SEGURIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * De ser posible, se deberá implementar uno de los siguientes esquemas de autenticación para acceso al sistema por parte de administradores y operadores de análisis biométrica, de ser necesario:   + Usuario/contraseña y Token lógico enviado al email del operador sea en el país o en el extranjero; y/o enviado al teléfono celular del operador del sistema (mediante un SMS) solo en el país   + Autenticación biométrica por comparación de una huella dactilar o del rostro del administrador/operador contra los elementos similares registrados en el ABIS. * Deberá generar logs detallados para trazabilidad de las actividades de los administradores del ABIS. * Se deberá especificar como se protegen los archivos y datos de la base de datos del ABIS, para evitar actividades no autorizadas. |  |  |

# ESTÁNDARES Y BUENAS PRÁCTICAS APLICABLES

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Recomendaciones de la OACI Doc 9303 versión 2015 para emisión de documentos de viaje de lectura por máquinas, donde corresponda. * Normas de la ISO que deben ser especificadas por el proveedor. * Normas o recomendaciones de la NIST[[16]](#footnote-16) en cuanto a la velocidad y precisión de algoritmos de comparación biométrica. * El ABIS a proveer deberá haber participado en evaluaciones recientes de proveedores de biometría dactilar organizadas por el NIST y cuyos resultados hayan sido publicados oficialmente, denominadas Fingerprint Vendor Technology Evaluation (FpVTE)[[17]](#footnote-17); y de proveedores de biometría facial, llamadas Face Recogntion Vendor Test (FrVT)[[18]](#footnote-18). * El proveedor deberá especificar la velocidad y precisión de los algoritmos de comparación dactilar y facial del ABIS que proponga, así como la Tasa de Aceptación Falsa (del inglés False Acceptance Rate o FAR) y la Tasa de Rechazo Falsa (False Rejection Rate o FRR). tanto para huellas como para rostros. Para especificación de los parámetros solicitados, se deberá considerar una base de datos compuesta de 160.000 millones de huellas dactilares planas y de 16.000 millones de rostros. Esas cantidades son los máximos de registros biométricos que tendrá la base de datos biométrica. |  |  |

# SOFTWARE A SER UTILIZADO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * El software base, para implementar el ABIS, deberá ser de preferencia software libre open source o de tecnología abierta; y por excepción podrá ser privativo. Se deberá suministrar todas las suscripciones de uso perpetuo a nombre de la DIGERCIC. El software base deberá estar basado o correr en Linux y comprenderá, pero sin estar limitado a:   + Sistemas operativos   + Sistemas de virtualización   + Gestores de base de datos   + Servidores Web   + Servidores de aplicaciones Web   + Herramientas de programación   + Sistemas de email   + Software de respaldo/restauración   + Servicios Web   + Software de monitoreo * Los sistemas, subsistemas, componentes o herramientas/programas de software privativos, que se utilicen para implementar el ABIS, deberán ser especificados detalladamente por el proveedor, y se deberá suministrar todas las licencias de uso perpetuo a nombre de la DIGERCIC. * Cualquier componente de software que sea programado conforme los requerimientos establecidos por la DIGERCIC deberá ser libre y su código fuente deberá ser entregado a la DIGERCIC. |  |  |

# IMPLEMENTACIÓN

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * De preferencia, el ABIS deberá poder ser implementado en ambientes virtuales o deberá poder operar en servidores virtuales siempre que la capacidad, disponibilidad, continuidad y rendimiento no sean afectados. * Se deberá proveer el hardware necesario para implementación del sistema virtualizado de acuerdo con las consideraciones de capacidad, disponibilidad, continuidad y rendimiento antes señaladas. * La virtualización aplica a la instalación de alta disponibilidad en el centro de datos principal; y a la instalación de contingencia en el centro de datos secundario. El software base de virtualización deberá cumplir lo señalado en la sección anterior. * En caso de que el ABIS no pueda ser implementado en ambientes virtuales, debe ser así especificado por el proveedor. * La escalabilidad (crecimiento) horizontal y vertical debe estar garantizada en cualquier implementación. * Se deberá proveer un (1) ambiente de pruebas del ABIS que tenga una capacidad de hasta el 1% de la capacidad anual solicitada para el ambiente de producción tanto para búsqueda 1 a 1 y 1 a n desde kits de captura o mediante SW. El ambiente de pruebas del ABIS deberá ser integrado al ambiente de pruebas del SEDIP. La implementación podrá ser completamente virtual en el centro de datos principal de la DIGERCIC en la ciudad de Quito. Se deberá proveer el equipamiento y licencias/suscripciones de software necesarias. * La DIGERCIC requiere que los equipos a proveer para implementación del ABIS sean hiperconvergentes. * El proveedor deberá especificar los requerimientos de conectividad, de energía, de enfriamiento, de espacio, de cantidad y tipo de tomas eléctricas, y cual información necesaria para instalación de los equipos en los centros de datos principal y secundario. * La DIGERCIC entregará la documentación de los procedimientos que el proveedor deberá tomar en cuenta para la puesta en operación de los equipos en los centros de cómputo. El proveedor deberá suministrar todos los accesorios, materiales, partes y piezas necesarios para la puesta en operación de los equipos. La puesta en operación de los equipos en los centros de cómputo es en la modalidad “llave en mano”. * El proveedor deberá documentar como quedan los equipos instalados conforme la arquitectura lógica y física que haya propuesto. La documentación deberá incluir los diagramas lógicos y físicos de detalles que especifiquen el lugar y función de cada componente de hardware y el software instalado. Se deberá anexar un registro fotográfico y un video de la instalación de los equipos en los centros de cómputo. * El proveedor deberá proponer un plan de entrenamiento a personal técnico de la DIGERCIC en temas relacionados a: la arquitectura lógica y física, configuración, afinamiento, monitoreo, “troubleshooting” de los componentes de hardware y software del ABIS. El plan será ejecutado, previa aprobación y en coordinación con la DIGERCIC. |  |  |

# ADMINISTRACIÓN/PARAMETRIZACION Y MONITOREO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Se deberá poder administrar y/o parametrizar las diferentes funcionalidades del sistema para las búsquedas 1 a 1 y 1 a n de huellas y rostros, dentro de límites razonables. * Se deberá poder administrar y monitorear de forma centralizada el ABIS. * Se deberá poder monitorear de forma centralizada el funcionamiento de la infraestructura del SEDIP implementada en los centros de cómputo principal y de contingencia para verificar la capacidad, disponibilidad y rendimiento. La herramienta de medición podrá ser de software libre open source accesible mediante un programa navegador o browser. La herramienta será utilizada solo por administradores del sistema nombrados por la DIGERCIC. * Se deberá poder parametrizar o configurar la edad a la cual se podrá enrollar huellas dactilares y rostros en el ABIS (por default será a partir de los 7 años). * Otros a juicio del proveedor. |  |  |

# INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

# DESCRIPCIÓN FUNCIONAL

Durante el proceso de emisión, los datos que se deben codificar/grabar en el chip de un documento son preparados de conformidad a las recomendaciones del Doc 9303 versión 2015 de la OACI. A continuación, los datos preparados son enviados a la PKI para que sean firmados y cifrados y posteriormente enviados de vuelta al SEDIP, el cual a su vez los envía al centro de producción para la codificación respectiva en el chip RFID del documento. Para lo cual, se utiliza una impresora de documentos de identidad o pasaportes con equipo codificador.

Para grabar los datos el chip, este debe ser desbloqueado, debido a que está cerrado (protegido) por una clave criptográfica acordada entre el proveedor de los documentos y la DIGERCIC, y cuya llave maestra es almacenada en un equipo modular de seguridad por hardware (HSM). Por tanto, el SEDIP debe solicitar el desbloqueo de chip y una vez desbloqueado proceder a cotejar automáticamente el número del chip contra el inventario de tarjetas o libretas en blanco (previamente cargado). Si el chip esta inventariado, se procede a grabar los datos. Para verificar la correcta grabación de los datos, el dispositivo de codificación de la impresora realiza una lectura automática de comprobación de los mismos.

Una vez que el chip del documento ha sido codificado, se procede a la impresión de la sección gráfica, que incluye la zona de lectura mecánica (Machine Readable Zone o MRZ), que es utiliza posteriormente para la lectura electrónica del chip del documento.

# REQUERIMIENTOS FUNCIONALES

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| La PKI deberá permitir:   * Expedir y autofirmar el certificado de autoridad de certificación de firma de país * Expedir, firmar y validar el certificado de firmante de documentos de identidad y el certificado de firmante de pasaportes, con el certificado de autoridad de certificación de firma de país. * Expedir, firmar y validar los certificados de firmante de lista maestra, firmante de lista de desviaciones y la lista de certificados revocados (CRL) con el certificado de autoridad de certificación de firma de país. * Enviar los certificados al Director de Claves Públicas Nacional (nPKD) * Distribuir los certificados de la PKD nacional a la PKD de la OACI para asegurar la lectura del documento a nivel mundial. * Generar periódicamente certificados de Firmantes de Documentos conforme recomienda OACI 9303 * Firmar y validar los datos (objetos de seguridad) para los documentos de identidad y pasaportes con el certificado de firmantes de documentos que corresponda. |  |  |

# REQUERIMIENTOS NO FUNCIONALES

# ARQUITECTURA

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Puede ser cliente-servidor de 3 capas: presentación, lógica de negocio y base de datos. La capa de presentación o de usuario debe ser tipo Web y correr en programas navegadores o browsers (por ejemplo, Mozilla Firefox y/o Google Chrome y/o Microsoft Internet Explorer) en sus últimas versiones. Caso contrario, el proveedor deberá especificar la arquitectura del ABIS a implementar. * Debe contemplar al menos:   + La Autoridad de Certificación Firmante del País (CSCA, por sus siglas en inglés) conforme OACI 9303   + El firmante de Documentos de documentos de identidad   + El Firmante de Documentos de pasaportes   + El Directorio de Claves Públicas Nacional (NPKD) y su integración informática al PKD de la OACI   + Los gestores de lista maestra y de revocación de certificados   + Un gestor o administrador de la PKI * Los firmantes de documentos de pasaportes deberán ser diferentes de los de documentos de identidad. |  |  |

# RENDIMIENTO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá firmar objetos de seguridad de documentos de identidad en hasta 5 segundos desde que es enviado a ser firmado por la PKI. |  |  |

# CAPACIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Los firmantes de documentos, deberán tener la capacidad para firmar el pico de documentos para el cual estará dimensionado el SEDIP. La siguiente tabla especifica la cantidad máxima de documentos de identidad y pasaportes que se deberán firmar por hora; y por minuto y segundo (valores redondeados). |  |  |

# DISPONIBILIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá tener una disponibilidad del 99,5% en un esquema de operación 24x7x365. Se imputarán para el cálculo, la disponibilidad de todos los componentes suministrados por el proveedor sin considerar indisponibilidad por mantenimientos planificados o de componentes que no dependen del proveedor (ej., la red datos de la DIGERCIC). La PKI deberá estar disponible para uso desde los puntos de atención en el país y del extranjero. * La disponibilidad del sistema de gestión de la PKI podrá estar garantizada por medio de la implementación de un clúster, de al menos 2 nodos para la capa de base de datos y para la capa de lógica de negocio respectivamente, en el centro de datos principal ubicado en la ciudad de Quito. Cada nodo del clúster deberá tener la capacidad suficiente para procesar toda la carga del sistema en caso de fallo de un nodo. * Los equipos o Módulos de Seguridad por Hardware (HSM)[[19]](#footnote-19), deberán estar configurados también en alta-disponibilidad. |  |  |

# CONTINUIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Debe ser garantizada mediante la implementación de la PKI en el centro de datos secundario o de contingencia de la DIGERCIC, ubicado en la ciudad de Guayaquil. El nodo de contingencia deberá tener la capacidad suficiente para procesar toda la carga del sistema en caso de contingencia del centro de datos principal. * Deberá soportar switch-over a la PKI de contingencia en Guayaquil por mantenimientos planificados u otros eventos previstos que afecten la continuidad del SEDIP y/o la PKI en el centro de cómputo principal. * Debe soportar fail-over a la PKI de contingencia en Guayaquil por incidentes o problemas imprevistos que afecten total o parcialmente la continuidad del SEDIP y/o la PKI en el centro de datos principal. * Se deberá implementar equipos para obtención y restauración de respaldos a/desde disco y a/desde cintas magnéticas digitales de alta velocidad y capacidad. Los respaldos deberán ser incrementales y completos (full) en base a política de respaldos del SEDIP que recomiende e implemente el proveedor en coordinación con la DIGERCIC. El proveedor deberá suministrar equipos que soporten el formato abierto "Linear-Tape Open" (LTO, por sus siglas en inglés) en su generación estable más actual. El proceso de backup/restauración no deberá afectar el rendimiento del sistema. |  |  |

# INTEGRACIÓN CON EL SISTEMA DE EMISION

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * De preferencia, la integración se debe realizar por medio de SW tipo SOAP o REST. De utilizarse otro tipo de interfaces se deberá especificar en la documentación de arquitectura lógica y física de la PKI. |  |  |

# USABILIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Deberá disponer de menús, opciones e interfaces de usuario que faciliten el uso y entendimiento de la PKI. * Las interfaces deberán disponer de opciones de ayuda en línea, tips o mensajes de ayuda * Deberá desplegar mensajes de información, alerta o error claros y entendibles * El idioma de las interfaces deberá ser español, de preferencia. |  |  |

# SEGURIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * De ser posible, se deberá implementar uno de los siguientes esquemas de autenticación para acceso al sistema por parte de administradores:   + Usuario/contraseña y Token lógico enviado al email del operador sea en el país o en el extranjero; y/o enviado al teléfono celular del operador del sistema (mediante un SMS) solo en el país   + Autenticación biométrica por comparación de una huella dactilar o del rostro del administrador/operador contra los elementos similares registrados en el ABIS. * Deberá generar logs detallados para trazabilidad de las actividades de los administradores de la PKI. * Se deberá especificar como se protegen los archivos y datos de la base de datos de la PKI, para evitar actividades no autorizadas. |  |  |

# ESTÁNDARES Y BUENAS PRÁCTICAS APLICABLES

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Recomendaciones de la OACI Doc 9303 aplicables a la PKI   + Aseguramiento de la emisión correcta de los Certificados conforme OACI 9303   + Cambio de los Certificados de los Firmantes de Documentos cada 6 meses o menos para evitar riesgos de seguridad a la PKI o desconfianza.   + Aseguramiento de la vigencia de los Certificados de los Firmantes de documentos durante del tiempo de vigencia de los documentos que haya firmado. * Normas de la ISO aplicables que deberán ser especificadas por el proveedor. |  |  |

# SOFTWARE A SER UTILIZADO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * El software base y de la PKI deberá ser de preferencia software libre open source o de tecnología abierta; y por excepción podrá ser privativo. Se deberá proveer todas las suscripciones de uso perpetuo a nombre de la DIGECIC. El software base deberá estar basado o correr en Linux y comprenderá, pero sin estar limitado a:   + Sistemas operativos   + Sistemas de virtualización   + Gestores de base de datos   + Servidores Web   + Servidores de aplicaciones Web   + Herramientas de programación   + Sistemas de email   + Software de respaldo/restauración   + Servicios Web   + Software de monitoreo * Los sistemas, subsistemas, componentes o herramientas/programas de software privativos, que se utilicen para implementar la PKI, deberán ser especificados detalladamente por el proveedor, y se deberá suministrar todas las licencias de uso perpetuo a nombre de la DIGERCIC. |  |  |

# IMPLEMENTACIÓN

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * De preferencia, la PKI deberá poder ser implementado en ambientes virtuales o deberá poder operar en servidores virtuales siempre que la capacidad, disponibilidad, continuidad y rendimiento no sean afectados. * La virtualización aplica a la instalación de alta disponibilidad en el centro de datos principal; y a la instalación de contingencia en el centro de datos secundario. El software base de virtualización deberá cumplir lo señalado en la sección anterior * En caso de que la PKI no pueda ser implementada en ambientes virtuales, debe ser así especificado por el proveedor. * Se debe implementar adicionalmente equipos modulares de seguridad por hardware (HSM) y el software de gestión respectivo para almacenamiento de las claves maestra criptográficas que permitirán la apertura del chip de un documento previo al proceso de personalización electrónica. * Se debe documentar detalladamente los procedimientos para ceremonias para gestión de las claves criptográficas de la PKI. Los roles que se deben asignar a funcionarios de la DIGERCIC y las funciones deben ser plenamente documentados. Los procedimientos operativos deben establecer las entradas, proceso y salidas de cada ceremonial. Las plantillas de documentos deben ser estándares y entregadas como parte de la documentación, en caso que no las pueda generar el software de gestión de la PKI. * Se deberá proveer un (1) ambiente de pruebas de la PKI que tenga una capacidad de hasta el 1% de la capacidad de firmado solicitada para el ambiente de producción. El ambiente de pruebas deberá ser integrado al SEDIP. La implementación podrá ser completamente virtual en el centro de datos principal de la DIGERCIC en la ciudad de Quito. Se deberá proveer el equipamiento y licencias/suscripciones de software necesarias. En caso que sea factible, la PKD de ese ambiente debe ser conectado a un ambiente de pruebas de la PKD de la OACI. * La DIGERCIC requiere que los equipos a proveer para implementación del ABIS sean, de ser factible, hiperconvergentes. * El proveedor deberá especificar los requerimientos de conectividad, de energía, de enfriamiento, de espacio, de cantidad y tipo de tomas eléctricas, y cual información necesaria para instalación de los equipos en los centros de datos principal y secundario. * La DIGERCIC entregará la documentación de los procedimientos que el proveedor deberá tomar en cuenta para la puesta en operación de los equipos en los centros de cómputo. El proveedor deberá suministrar todos los accesorios, materiales, partes y piezas necesarios para la puesta en operación de los equipos. La puesta en operación de los equipos en los centros de cómputo es en la modalidad “llave en mano”. * El proveedor deberá documentar como quedan los equipos instalados conforme la arquitectura lógica y física que haya propuesto. La documentación deberá incluir los diagramas lógicos y físicos de detalles que especifiquen el lugar y función de cada componente de hardware y el software instalado. Se deberá anexar un registro fotográfico y un video de la instalación de los equipos en los centros de cómputo. * El proveedor deberá proponer un plan de entrenamiento a personal técnico de la DIGERCIC en temas relacionados a: la arquitectura lógica y física, configuración, afinamiento, monitoreo, “troubleshooting” de los componentes de hardware y software de la PKI. El plan será ejecutado, previa aprobación y en coordinación con la DIGERCIC. |  |  |

# ADMINISTRACIÓN/PARAMETRIZACION Y MONITOREO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Se deberá poder administrar/parametrizar las diferentes funcionalidades de la PKI para la gestión de las claves criptográficas, certificados emitidos y listas o elementos necesario para el funcionamiento correcto del AFIS. * Se deberá poder administrar y monitorear de forma centralizada todos los componentes de la PKI. * Se deberá poder monitorear de forma centralizada el funcionamiento de la PKI implementada en los centros de cómputo principal y de contingencia para verificar la capacidad, disponibilidad y rendimiento. La herramienta de medición podrá ser de software libre open source accesible mediante un programa navegador o browser. La herramienta será utilizada solo por administradores del sistema nombrados por la DIGERCIC. |  |  |

# SISTEMA DE MONITOREO DE LA OPERACIÓN Y SEGURIDAD

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El proveedor deberá implementar un sistema de monitoreo de la operación y seguridad del SEDIP. El monitoreo deberá comprender desde la captura de solicitudes y datos biométricos, la producción y la entrega de documentos.  Se requiere monitorear el funcionamiento de la infraestructura informática de los centros de datos, así como de los kits de captura, kits de producción y kits de entrega. Las variables a monitorear son al menos: la capacidad, disponibilidad y rendimiento de los componentes de hardware y del software del SEDIP, el ABIS, la PKI, los HSMs para desbloqueo de chips, entre otros.  Todo el proceso de producción de los documentos desde la captura de solicitudes hasta la entrega de los documentos, así como el funcionamiento de las impresoras tanto de documentos de identidad como de pasaportes deberá ser monitoreada desde el sistema de monitoreo.  Adicionalmente, se deberá monitorear la seguridad de la información que procesa el sistema por lo que se requiere la implementación de una herramienta de gestión de eventos de la seguridad de la información (SIEM, por sus siglas en inglés)[[20]](#footnote-20), basada en software libre open source. El SIEM deberá colectar y correlacionar datos de los logs de los componentes de software y hardware del sistema tanto de los centros de cómputo como de los puntos de atención y gestionar eventos de seguridad de la información, que se pudieren presentar.  Se deberá implementar un solo aplicativo o programa de monitoreo que se pueda desplegar en monitores tipo “Wall-panel” y en estaciones de trabajo de monitoreo. La tabla a continuación indica los tipos de equipos y función que deben cumplir en sistema de monitoreo. El proveedor puede proponer variantes equipos y/o accesorios o añadir otros mientras sirvan para el propósito de monitoreo.   |  |  |  |  | | --- | --- | --- | --- | | **Nro**. | **EQUIPO** | **CANTIDAD** | **ROL** | | 1 | COMPUTADORA PERSONAL “ALL-IN-ONE” con doble monitor. | Mínimo 3 | Monitoreo de los sistemas y control de los monitores, Se debe proveer con suscripciones o licencias de software base del software de monitoreo de la infraestructura de centro de cómputo y equipamiento de puntos de atención | | 2 | MONITORES WALL-PANEL | Mínimo 4 | Despliegue de la información del monitoreo y alertas de ser el caso. |   Los equipos deberán ser nuevos de fábrica, no remanufacturados y fabricados el año en los que sean entregados.  Debido a la normativa legal ecuatoriana, se deberá proveer equipos y software que funcionen en sistemas operativos privativos (ej., de Microsoft) y/o de preferencia sistemas operativos open source o libres (ej., basados en Linux). Se debe proveer las licencias o suscripciones de software respectivas.  El oferente deberá proveer e instalar software antivirus en los PC de los kits de impresión, así como las suscripciones o licencias respectivas.  El oferente deberá proveer e instalar en cada PC para monitoreo una herramienta de seguridad de punto final (endpoint security tool) que tenga la característica para prevenir la fuga de datos (data loss prevention) así como protección contra spam/virus, bloqueo de actividad maliciosa, control de navegación Web.    Ese software particularmente deberá permitir controlar los puertos de entrada-salida (ej., USB), dispositivo de lectura/escritura de CD/DVD, puertos infrarrojos, bluetooh, Wifi, RJ45, para evitar la copia/transmisión de información no autorizada. El oferente deberá suministra las suscripciones o licencias respectivas del software de seguridad de punto final.  La garantía técnica de los equipos y la vigencia de las licencias o suscripciones con mantenimiento/actualización incluido deberá ser de al menos 3 años. Durante la vigencia del contrato se deberá proveer mantenimientos preventivos con frecuencia semestrales para garantizar su operatividad. El cambio de equipos, piezas y accesorios deberá ser contemplado como parte de los mantenimientos preventivos y correctivos.  El proveedor deberá instalar y poner en operación los monitores y estaciones de trabajo en el espacio físico y muebles que asigne la DIGERCIC. Todos los materiales, accesorios, partes y piezas para la instalación correrán por cuenta del proveedor. Esto incluye, de ser necesario, la instalación de puntos de tomas eléctricas y/o de datos, que cumplan estándares de la industria.  El proveedor deberá entregar todos los equipos del sistema de monitoreo a la DIGERCIC. De igual forma, se deberá coordinar el entrenamiento al personal técnico que la DIGERIC delegue.  Para los eventos de entrenamiento se deberá proveer la documentación técnica y de usuario respectiva, así como manuales, drivers, y cualquier rubro necesario para la instalación y uso correcto de los equipos y las herramientas de monitoreo. |  |  |

# EQUIPAMIENTO PARA AGENCIAS/CONSULADOS

# KITS FIJOS PARA CAPTURA DE DATOS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| Los kits fijos de captura de datos para documentos de identidad y pasaportes estarán conformados por un conjunto de equipos y programas de software que permitirán acceder y utilizar el SURI y el SEDIP para procesar las solicitudes de documentos de identidad y/o pasaportes tanto las agencias de la DIGERCIC como en los consulados del MREMH.  En las agencias de la DIGERCIC, la captura de datos para solicitudes de documentos de identidad y pasaportes se realiza en estaciones de trabajo diferentes y separadas. En los consulados del MREMH, la captura de datos para solicitudes de documentos de identidad y pasaportes se realiza en las mismas estaciones de trabajo. La tabla a continuación especifica la cantidad de kits de captura que deberán ser provistos.   |  |  |  |  | | --- | --- | --- | --- | | **ENTIDAD** | **CANTIDAD** | **TIPO DOCUMENTO** | **KITS DE CAPTURA** | | **DIGERCIC AGENCIAS** | 183 | CEDULA | 485 | | PASAPORTE | 39 | | **MREMH CONSULADDOS** | 80 | CEDULA / PASAPORTE | 97 | | **Stock de backup** | | | 14 | | **TOTAL** | | | **635** |   La siguiente tabla indica los tipos de equipos y rol de los mismos en los kits fijos de captura. El proveedor podrá proponer variantes de equipos y/o accesorios o añadir otros mientras sirvan para el propósito de la captura de datos de forma fácil, rápida y segura.   |  |  |  |  | | --- | --- | --- | --- | | **Nro**. | **EQUIPO** | **CANTIDAD** | **ROL** | | 1 | COMPUTADORA PERSONAL FACTOR “ULTRA-SIM” | 1 | Acceso al SURI, SEDIP, software utilitario (email, ofimática) y conexión/control de equipos del kit | | 2 | ESCANER DE HUELLAS UNIDACTILAR | 1 | Captura de huella dactilar para autenticación del operador en el SEDIP. | | 2 | ESCANER DE HUELLAS DECADACTILAR | 1 | Captura de hasta 10 huellas dactilares del solicitante para validación biométrica de la identidad | | 4 | CAMARA FOTOGRAFICA DIGITAL, TRIPODE Y TELON DE FONDO | 1 | Captura de foto del rostro del solicitante (conforme OACI) para validación biométrica de la identidad | | 5 | TABLETA DIGITALIZADORA DE FIRMAS MANUSCRITAS | 1 | Captura de firma manuscrita del solicitante con lápiz digital para posterior impresión en los documentos | | 7 | ESCANER DE DOCUMENTOS | 1 | Captura de documentos de soporte de la solicitud de documentos; y captura de firmas manuscritas desde papel para posterior impresión en los documentos. |   Las especificaciones técnicas mínimas de los equipos de los kits fijos de captura se encuentran en el Anexo E. Los equipos deben ser nuevos de fábrica, no re-manufacturados y fabricados el año en los que sean entregados.  Debido a la normativa legal ecuatoriana, el sistema operativo de la PC del kit podrá ser preferencia libre open source (ej., Linux); o privativo (ej., de Microsoft) en sus versiones recientes. Los controladores (drivers) y kits de desarrollo de software de los equipos periféricos deberán ser compatibles con el sistema operativo que se proporcione. El proveedor deberá proveer las licencias o suscripciones de software respectivas para los sistemas operativos y los programas de software que se solicitan. Todas las licencias o suscripciones deberán estar a nombre de la DIGERCIC.  El oferente deberá proveer e instalar software antivirus en los PC de los kits de captura, así como las suscripciones o licencias respectivas para cada PC del kit de captura; y para la consola centralizada de administración del software antivirus.  El proveedor deberá implementar una herramienta o funcionalidad para controlar y garantizar que solo equipos inventariados y autorizados puedan acceder y utilizar el SEDIP para la funcionalidad de captura de datos.  El oferente deberá proveer e instalar en cada PC del kit una herramienta de seguridad de punto final (endpoint security tool) que tenga la característica para prevenir la fuga de datos (data loss prevention) así como protección contra spam/virus, bloqueo de actividad maliciosa, control de navegación Web  Ese software particularmente deberá permitir controlar los puertos de entrada-salida (ej., USB), dispositivo de lectura/escritura de CD/DVD, puertos infrarrojos, bluetooh, Wifi, RJ45, para evitar la copia/transmisión de información no autorizada. El oferente deberá facilitará las suscripciones o licencias respectivas para cada PC del kit de captura; así como para la consola centralizada de administración del software de seguridad de punto final.  El oferente deberá proveer e instalar software monitoreo y administración remota del PC (incluso el encendido y apagado). El oferente deberá facilitar las suscripciones o licencias respectivas para cada PC del kit de captura; así como para la consola centralizada de administración del software de monitoreo y administración.  La DIGERCIC podrá instalar o facilitar el acceso a herramientas de software y/o sistemas/aplicaciones informáticas en las PC’s de los kits, siempre que sea compatible con el hardware y software base de las mismas. El software a instalar por parte de la DIGERCIC consistirá al menos de: cliente para llamar turnos, cliente de email, herramienta de ofimática, lector de archivos PDF, cliente de control remoto de la PC, navegadores Web (browsers): Mozilla Firefox, Google Chrome y Microsoft Internet Explorer, manejador de impresora de red.  La garantía técnica de los equipos y la vigencia de las licencias o suscripciones de software con mantenimiento/actualización incluidos deberá ser de al menos 3 años. La vigencia del soporte y mantenimiento/actualización de licencias suscripciones regirá partir de la fecha de la entrada en producción del SEDIP y así aceptado por la DIGERCIC mediante acta de entrega-recepción.  Durante la vigencia del soporte y mantenimiento/actualización se deberá realizar mantenimientos preventivos con frecuencia semestrales para garantizar la operatividad de los kits de captura. Para mantenimientos correctivos se deberá aplicar la garantía técnica solicitada. El cambio de equipos, piezas y accesorios deberá estar contemplado como parte de los mantenimientos preventivos y correctivos sin costo adicional para la DIGERCIC.   * **Implementación de kits de captura**   El proveedor deberá entregar todos los kits de captura en la bodega de la DIGERCIC.  El proveedor deberá proponer un plan y cronograma de despliegue de kits de captura para aprobación de la DIGERCIC. El plan deberá considerar primero el despliegue de kits de captura para emisión de pasaportes; y posteriormente el despliegue de kits de captura para emisión de documentos de identidad. El primer servicio a implementar deberá ser el de pasaportes electrónicos y a continuación el de emisión de documentos de identidad.  El plan deberá considerar actividades previas, durante y después de la implementación de los kits. La instalación y puesta en operación deberá considerar horarios de trabajo a partir de las 17h30, fines de semana o feriados, es decir, horarios fuera de oficina, para no interrumpir los servicios de emisión de documentos de pasaportes y documentos de identidad en las agencias.  El proveedor deberá contemplar las actividades previas a realizar para el despliegue de los kits de captura en las agencias y consulados. Actividades previas a considerar serán: Instalación/configuración de los kits, entrenamiento a usuarios designados por la DIGERCIC (operadores de captura, de validación biométrica, supervisores), creación de usuarios, roles y permisos para acceso al SEDIP, preparación y envío de equipos a las agencias, entre otras.  El proveedor deberá facilitar el entrenamiento al personal técnico que la DIGERIC delegue para la instalación, configuración, puesta en operación, pruebas, aseguramiento y soporte de primer nivel de los equipos y software de los kits de captura. Se deberá entregar la documentación técnica y de usuario respectivas, así como manuales, drivers, y cualquier ítem necesario para el entrenamiento del personal designado.   * **Alcance de la implementación de kits de captura**   El proveedor deberá tomar en cuenta que el servicio de despliegue de kits de captura estará limitado a:   1. **ECUADOR**  * 25 agencias de la DIGERCIC de emisión de pasaportes * 1 oficina del MREMH de emisión de pasaportes * 183 agencias de la DIGERCIC de emisión de documentos de identidad  1. **EXTRANJERO**  * 1 consulado del MREMH en Nueva York (USA) de emisión de pasaportes y documentos de identidad * 1 consulado del MREMH en Madrid (España) de emisión de pasaportes y documentos de identidad   El proveedor deberá considerar que la instalación de los kits de captura en el resto de consulados estará a cargo del MREMH. El proveedor deberá facilitar el entrenamiento necesario y suficiente al personal que designe el MREMH bajo coordinación de la DIGERCIC.   * **Implementación de kits de captura para emisión de pasaportes** * **Implementación de piloto de emisión de pasaportes de prueba**   El proveedor deberá implementar un piloto de emisión de pasaportes electrónicos de prueba. El piloto deberá implementarse en la agencia matriz de la DIGERCIC en Quito con una duración de al menos 2 semanas previo al despliegue de los kits de captura en esa agencia para el comienzo de operaciones.  El proveedor deberá implementar al menos 1 kit de captura en 1 estación de trabajo del área de pasaportes con el objeto de realizar emisión en paralelo de pasaportes de lectura mecánica y pasaportes electrónicos –de prueba- a los solicitantes.  El proveedor deberá asegurar que para la emisión de los pasaportes -de prueba- el operador siga el procedimiento definido en los requerimientos funcionales. Esto comprende desde la generación de una solicitud de pasaporte en el SURI, la captura de esa solicitud en el SEDIP, la autenticación por huella del operador en el SEDIP, la captura de datos biométricos, la validación de identidad biométrica con el ABIS, la producción y verificación de calidad, y la entrega del pasaporte al solicitante mediante la autenticación biométrica de rostro contra la foto almacenada en el pasaporte. Para evitar molestias a los solicitantes, personal de la DIGERCIC informará de la prueba a realizar. Así mismo, para no alargar los tiempos de atención en la estación de pruebas, se realizará al menos 2 emisiones por día de pasaportes -de prueba-. Esta cantidad podrá aumentar previa aprobación de la DIGERCIC. Al finalizar las 2 semanas del piloto se deberán haber capturado datos de al menos 20 pasaportes -de prueba-.  El proveedor deberá considerar que un kit de producción (equipo de impresión y QA) y un kit de entrega de pasaportes estarán también implementados en la agencia Matriz de la DIGERCIC en Quito, previo a la ejecución del piloto.  El proveedor deberá elaborar un informe de la ejecución de la emisión de pasaportes -de prueba- al finalizar el mismo. Deberá anexar los pasaportes –de prueba- emitidos.   * **Implementación de kits de captura para pasaportes en el país**   El proveedor deberá ejecutar la implementación de los kits de captura para pasaportes conforme el plan y cronograma de trabajo que la DIGERCIC apruebe. La primera agencia en la cual se deberá desplegar el servicio de emisión de pasaportes electrónicos será la agencia matriz de la DIGERCIC en Quito. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días de anticipación al proveedor.  El proveedor deberá retirar los kits de captura de la bodega de la DIGERCIC ubicada en el edificio matriz en Quito, en coordinación con la DIGERCIC. Posteriormente, procederá a preparar cada kit, previo al envío, por su cuenta, a la(s) agencia(s) correspondiente(s) según el cronograma de trabajo.  Una vez en sitio y conforme el cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por la DIGERCIC deberán retirar los equipos de captura actuales de las estaciones de trabajo, y proceder a instalar, configurar y probar cada kit de captura con el SEDIP. Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de captura con el SEDIP y los sistemas propios de la DIGERCIC.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de emisión de pasaportes en cada agencia según el cronograma de trabajo y hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico de la DIGERCIC prestará también el apoyo y soporte necesarios. Una vez instalados los kits de captura el inicio de operaciones será el siguiente día laborable.  La DIGERCIC en coordinación con el proveedor activará el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de emisión de pasaportes en la(s) agencia(s) en las cuales se haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por la DIGERCIC un acta de entrega-recepción con los datos de cada kit implementado. Además, deberá elaborar un informe por agencia que detalle los trabajos realizados, la cantidad de kits implementados, la evidencia de la operatividad de los kits con el SEDIP, los usuarios, roles y permisos creados para uso de los kits de captura, registro fotográfico de cada kit de captura instalado, anexos y cualquier información adicional que se considere necesario.   * **Implementación de kits de captura en el extranjero**   Conforme el alcance especificado anteriormente, el proveedor deberá implementar kits de captura en los consulados de Nueva York (USA) y Madrid (España), conforme el plan y cronograma de trabajo que la DIGERCIC apruebe.  El primer consulado en el cual se deberá desplegar el servicio de emisión de pasaportes electrónicos será el de Nueva York. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días calendario de anticipación al proveedor.  El proveedor deberá retirar los kits de la bodega matriz de la DIGERCIC en Quito y realizar la preparación respectiva. Posteriormente, deberá devolver los kits listos a la DIGERCIC, la cual a su vez entregará al MREMH para el envío al consulado. Los costos del envío deberán ser asumidos por el proveedor, salvo que la DIGERCIC notifique por escrito lo contrario, con una anticipación de 7 días calendario.  Una vez en sitio y conforme cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por el MREMH y/o la DIGERCIC deberá retirar los equipos de captura actuales de las estaciones de trabajo, y proceder a instalar, configurar y probar cada kit de captura con el SEDIP. Cada estación de trabajo cuenta con puntos de energía eléctrica y de datos para conexión de kit de captura. Personal del proveedor y de la DIGERCIC deberá facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de captura con el SEDIP y los sistemas propios de la DIGERCIC. Las pruebas de los kits de captura comprenderán también la captura para emisión de documentos de identidad considerando que se implementará primero la emisión de pasaportes.  El proveedor deberá considerar que el kit de captura deberá ser conectado a la red de área local del consulado por medio de la interface RJ45 del PC y el punto de datos disponible en la estación de trabajo. El proveedor deberá conectar el kit de captura al centro de datos principal y alterno por medio de una red privada virtual (VPN, por las siglas en inglés) implementada en equipo gateway de seguridad principal. La VPN será del tipo punto a punto y encriptará el tráfico entre el kit de captura y los centros de datos de la DIGERIC que se transmitirá por la Internet. Se deberá implementar un gateway secundario para uso en caso de falla del principal.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de emisión de pasaportes hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico del MREMH y/o de la DIGERCIC prestarán también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el MREMH y el proveedor activarán el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de emisión de pasaportes en el consulado una vez que haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por el MREMH y/o por la DIGERCIC un acta de entrega-recepción con los datos de cada kit implementado. Además, deberá elaborar un informe que, al menos contenga: detalle los trabajos realizados; la cantidad de kits implementados; la evidencia de la operatividad de los kits con el SEDIP; los usuarios entrenados para operar los kits de captura y el SEDIP; el registro fotográfico de cada kit de captura instalado y anexos. El informe podrá incluir cualquier información adicional que el proveedor o la DIGERCIC consideren necesario.  Para la implementación de los kits de captura en el consulado de Madrid en España regirán los mismos requerimientos que para el consulado de Nueva York en Estados Unidos (USA).   * **Implementación de kits de captura para emisión de documentos de identidad** * **Implementación de piloto de emisión de documentos de identidad de prueba** * El proveedor deberá implementar un piloto de emisión de documentos de identidad de prueba. El piloto deberá implementarse en la agencia matriz de la DIGERCIC en Quito con una duración de al menos 2 semanas previo al despliegue de los kits de captura en esa agencia para el comienzo de operaciones de emisión de documentos de identidad.   El proveedor deberá implementar al menos 2 kit de captura en 2 estaciones de trabajo del área de emisión de documentos de identidad con el objeto de realizar emisión en paralelo de documentos de identidad con el formato actual y documentos de identidad –de prueba- con el nuevo formato a los solicitantes.  El proveedor deberá asegurar que para la emisión de los documentos de identidad -de prueba- el operador siga el procedimiento definido en los requerimientos funcionales. Esto comprende desde la generación de una solicitud de documentos de identidad en el SURI, la captura de esa solicitud en el SEDIP, la autenticación por huella del operador en el SEDIP, la captura de datos biométricos, la validación de identidad biométrica con el ABIS, la producción y verificación de calidad, y la entrega del documento de identidad al solicitante mediante la autenticación biométrica de rostro contra la foto almacenada en el documento de identidad. Para evitar molestias a los solicitantes, personal de la DIGERCIC informará de la prueba a realizar. Así mismo, para no alargar los tiempos de atención en la estación de pruebas, se realizará al menos 10 emisiones por día de documentos de identidad -de prueba. Esta cantidad podrá aumentar previa aprobación de la DIGERCIC. Al finalizar las 2 semanas del piloto se deberán haber capturado datos de al menos 100 documentos de identidad -de prueba-. Cada estación de pruebas emitirá 25 documentos de identidad –de prueba- por semana.  El proveedor deberá considerar que un kit de producción (equipo de impresión y QA) y un kit de entrega de documentos de identidad estarán también implementados en la agencia Matriz de la DIGERCIC en Quito, previo a la ejecución del piloto.  El proveedor deberá elaborar un informe de la ejecución de la emisión de documentos de identidad -de prueba- al finalizar la prueba. Deberá anexar los documentos de identidad –de prueba- emitidos.   * **Implementación de kits de captura para documentos de identidad en el país**   El proveedor deberá ejecutar la implementación de los kits de captura para documentos de identidad conforme el plan y cronograma de trabajo que la DIGERCIC apruebe. La primera agencia en la cual se deberá desplegar el servicio de emisión de documentos de identidad será la agencia matriz de la DIGERCIC en Quito. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días de anticipación al proveedor.  El proveedor deberá retirar los kits de captura de la bodega de la DIGERCIC ubicada en el edificio matriz en Quito, en coordinación con la DIGERCIC. Posteriormente, procederá a preparar cada kit, previo al envío, por su cuenta, a la(s) agencia(s) correspondiente(s) según el cronograma de trabajo.  Una vez que los kits de captura se encuentren en sitio y conforme el cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por la DIGERCIC deberán retirar los equipos de captura actuales de las estaciones de trabajo, y proceder a instalar, configurar y probar cada kit de captura con el SEDIP. Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de captura con el SEDIP y los sistemas propios de la DIGERCIC.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de emisión de documentos de identidad en cada agencia según el cronograma de trabajo y hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico de la DIGERCIC prestará también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el proveedor activará el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de emisión de documentos de identidad en la(s) agencia(s) en las cuales se haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por la DIGERCIC un acta de entrega-recepción con los datos de cada kit implementado. Además, deberá elaborar un informe por agencia que detalle los trabajos realizados, la cantidad de kits implementados, la evidencia de la operatividad de los kits con el SEDIP, los usuarios, roles y permisos creados para uso de los kits de captura, registro fotográfico de cada kit de captura instalado, anexos y cualquier información adicional que se considere necesario. |  |  |

# KITS DE PRODUCCION DE PASAPORTES

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| Los kits de producción de pasaportes estarán conformados por un conjunto de equipos y programas de software que permitirán acceder y utilizar el SEDIP para: grabar/codificar los datos de solicitante en el chip del pasaporte, imprimir la página de datos y asegurar la calidad del pasaporte, de conformidad a las recomendaciones de la OACI vigentes.  El proveedor deberá facilitar kits para reemplazar los equipos actuales de impresión de los 3 centros de producción de pasaportes ordinarios que actualmente se encuentran en operación en 3 agencias de la DIGERCIC. Adicionalmente, se deberá proveer kits de impresión para 3 centros de producción de pasaportes ordinarios, diplomáticos, oficiales y especiales en 3 locaciones del MREMH.  La tabla a continuación indica la distribución de kits de impresión y equipos de control de calidad de pasaportes que deberán ser implementados.   |  |  |  | | --- | --- | --- | | **ENTIDAD** | **CENTRO DE PRODUCCION** | **KITS DE IMPRESION** | | DIGERCIC | QUITO | 3 | | GUAYAQUIL | 2 | | CUENCA | 2 | | MREHMH | NUEVA YORK | 2 | | MADRID | 2 | | QUITO | 1 | | Stock de backup | | 1 | | **TOTAL** | | **13** |   El proveedor deberá ofertar impresoras del tipo “todo en uno” (“all-in-one”)/modulares. Esto para minimizar la intervención de operadores durante el proceso de producción, la manipulación de libretas y varios dispositivos, optimizar el tiempo de producción y minimizar riesgos de seguridad en el centro de producción.  La siguiente tabla indica los tipos y cantidad de equipos por cada kit de impresión de pasaportes y el rol que cumplirán:   |  |  |  |  | | --- | --- | --- | --- | | **Nro**. | **EQUIPO** | **CANTIDAD** | **ROL** | | 1 | COMPUTADORA PERSONAL TIPO “ULTRA-SLIM”. INCLUYE MONITOR, TECLADO Y MOUSE. | 1 | Acceso al SURI, SEDIP, software utilitario (email, ofimática, etc.) y conexión/control de equipos del kit. | | 2 | IMPRESORA DE TRASFERENCIA DE TINTA TIPO “ALL-IN-ONE” / MODULAR | 1 | Codificación/grabado/verificación automática de los datos demográficos y biométricos en el chip RFID conforme OACI 9303 versión 2015. Impresión de la sección visual del pasaporte; y laminado de la página de datos del pasaporte. | | 3 | ESCANER DE HUELLAS UNIDACTILAR | 1 | Captura de huella dactilar para autenticación del operador en el SEDIP. | | 4 | LECTOR DE DOCUMENTOS OACI 9303 Y CHIP RFID | 1 | Lectura del pasaporte mediante MRZ, BAC/SAC y verificación visual de seguridades del pasaporte para luz blanca, ultravioleta o infrarroja. | | 5 | MESA DE SOPORTE (SOLO SI LA IMPRESORA NO VIENE MONTADA) | 1 | Instalación y soporte de la impresora conforme su peso, en caso que la impresora no venga montada en su propio gabinete. |   La tecnología de impresión de la página de datos del pasaporte será de transferencia de tinta debido que el material de la página de datos es de papel. La impresión de la fotografía del ciudadano en la página de datos del pasaporte deberá ser a color. En la página 3 se deberá imprimir nuevamente la fotografía en blanco y negro para comparación visual contra la impresa en la página de datos como medida de seguridad adicional. La DIGERCIC podrá cambiar o eliminar este requerimiento previa notificación y acuerdo con el proveedor.  Los chips de las libretas en blanco estarán bloqueados contra escritura mediante un esquema de criptografía simétrica acordado entre el IGM y la DIGERCIC. Es un mecanismo de seguridad establecido para evitar el mal uso de las libretas e impedir su utilización en caso de pérdida o robo. En proveedor deberá implementar la funcionalidad para desbloquear los chips durante del proceso de personalización. Para tal efecto, el proveedor deberá validar las llaves instanciadas en el chip de las libretas contra las llaves maestras almacenadas en un módulo de seguridad de hardware principal (HSM, por sus siglas en inglés); o en un HSM de contingencia, en caso de falla del principal. Previamente, el proveedor en coordinación con la DIGERCIC y el IGM deberán transportar las llaves maestras generadas por el IGM a los HSM principal y de contingencia, que el proveedor deberá suministrar e implementar para el efecto. La generación y grabación de llaves tanto maestras como las de las tarjetas seguirán estándares y buenas prácticas de la industria privilegiando la seguridad y confiabilidad del proceso. La DIGERCIC facilitará el procedimiento de generación y transporte de claves al proveedor que resulte adjudicado.  El proveedor deberá suministrar impresoras de pasaportes del tipo “todo-en-uno” (“all-in-one”) con las siguientes características mínimas:   * Lector para reconocimiento óptico de caracteres para captura automática del número de serie del pasaporte * Cámara para ubicación exacta del pasaporte y datos a imprimir * Codificador electrónico RFID para grabación por no contacto; y comprobación automática de la codificación. * Indicadores sonoros y/o gráficos del proceso de producción. * Seguridades físicas (por ejemplo, candados) y/o lógicas (por ejemplo, contraseñas). * Bandejas para carga automática de libretas en blanco y para salida de pasaportes producidos y rechazados. * SDK para diferentes sistemas operativos y lenguajes de programación. * Software para monitoreo centralizado del funcionamiento la impresora.   El proveedor deberá suministrar lectores de documentos OACI 9303 para asegurar la calidad del pasaporte producido. El lector deberá recuperar la información de la solicitud de pasaporte producido por medio de la lectura de la zona de lectura mecánica. El aseguramiento de la calidad deberá comprobar que el pasaporte ha sido correctamente producido por medio de una inspección manual y visual que se registrará en el sistema. Adicionalmente, el sistema deberá permitir realizar la comparación automática de la información impresa, escaneada de la página de datos por medio del lector, con la información de la solitud del pasaporte procesado. El sistema deberá permitir también realizar la lectura y comparación automática de la información codificada en el chip, leída por medio del lector, con la información de la solicitud del pasaporte procesado. Se deberán verificar los controles de acceso básico y suplementario implementados en el chip, conforme recomienda la OACI.  Todo el proceso de producción, incluido el de aseguramiento de la calidad, deberá ser controlado paso a paso y registrado en el SEDIP previo a la salida del pasaporte del centro de producción para entrega al solicitante.  Las especificaciones técnicas mínimas de los equipos de los kits de producción de pasaportes se encuentran en el Anexo E. Los equipos deberán ser nuevos de fábrica, no re-manufacturados y fabricados el año en que sean entregados a la DIGERCIC.  Debido a la normativa legal ecuatoriana, el sistema operativo de la PC del kit podrá ser preferencia libre open source (ej., Linux); o privativo (ej., de Microsoft) en sus versiones recientes. Los controladores (drivers) y kits de desarrollo de software de los equipos periféricos deberán ser compatibles con el sistema operativo que se proporcione. El proveedor deberá suministrar las licencias o suscripciones de software respectivas para el sistema operativo y los programas de software que se solicitan. Todas las licencias o suscripciones deberán estar a nombre de la DIGERCIC.  El oferente deberá proveer e instalar software antivirus en los PC de los kits de impresión, así como las suscripciones o licencias respectivas.  El proveedor deberá implementar una herramienta o funcionalidad para controlar y garantizar que solo los equipos inventariados y autorizados para cada kit de producción puedan acceder y utilizar el SEDIP para la funcionalidad de producción.  El oferente deberá entregar toda la información técnica del módulo de laminación que propone en sus impresoras de pasaportes electrónicos, para poder probar oportunamente las láminas de seguridad holográficas provistas por el IGM en sus equipos y garantizar que no existan problema de operación. Adicionalmente, se requiere que el oferente trabaje conjuntamente con el IGM para garantizar que la laminación del documento de viaje cumpla los estándares exigidos por la OACI en el Doc. 9303.  El oferente deberá proveer e instalar en cada PC del kit una herramienta de seguridad de punto final (endpoint security tool) que tenga la característica para prevenir la fuga de datos (data loss prevention) así como protección contra spam/virus, bloqueo de actividad maliciosa, control de navegación Web  Ese software particularmente deberá permitir controlar los puertos de entrada-salida (ej., USB), dispositivo de lectura/escritura de CD/DVD, puertos infrarrojos, bluetooh, Wifi, RJ45, para evitar la copia/transmisión de información no autorizada. El oferente deberá suministra las suscripciones o licencias respectivas para cada PC del kit de producción del software de seguridad de punto final.  El oferente deberá proveer e instalar software monitoreo y administración centralizada del PC (incluso el encendido y apagado) y de la impresora del kit. El oferente deberá facilitar las suscripciones o licencias respectivas para cada PC del kit de producción y para la impresora; así de la consola centralizada de administración del software centralizado de monitoreo y administración.  La DIGERCIC podrá instalar o facilitar el acceso a herramientas de software y/o sistemas/aplicaciones informáticas en los PC’s de los kits, siempre que sea compatible con el hardware y software base de las mismas. El software a instalar por parte de la DIGERCIC consistirá al menos de: cliente de email, herramienta de ofimática, lector de archivos PDF, cliente de control remoto de la PC, navegadores Web (browsers): Mozilla Firefox, Google Chrome y Microsoft Internet Explorer, manejador de impresora de red.  La garantía técnica de los equipos y la vigencia de las licencias o suscripciones de software con mantenimiento/actualización incluidos deberá ser de al menos 3 años. La vigencia del soporte y mantenimiento/actualización de licencias suscripciones regirá partir de la fecha de la entrada en producción del SEDIP y así aceptado por la DIGERCIC mediante de acta entrega-recepción.  Durante la vigencia del contrato se deberá realizar mantenimientos preventivos con frecuencia semestrales para garantizar la operatividad de los kits de producción. Para mantenimientos correctivos se deberá aplicar la garantía técnica solicitada. El cambio de equipos, piezas y accesorios deberá estar contemplado como parte de los mantenimientos preventivos y correctivos sin costo adicional para la DIGERCIC.   * **Implementación de los kits de producción de pasaportes**   El proveedor deberá entregar todos los kits de producción a la bodega de la DIGERCIC.  El proveedor deberá proponer un plan y cronograma de despliegue de los kits de producción para aprobación de la DIGERCIC. El plan deberá considerar actividades previas, durante y después de la implementación de los kits. La instalación y puesta en operación deberá considerar horarios de trabajo a partir de las 17h30, fines de semana o feriados, es decir, horarios fuera de oficina, para no interrumpir los servicios de emisión de documentos de pasaportes en las agencias y consulados.  El proveedor deberá entregar a la DIGERCIC un documento especificando los requerimientos para la instalación de los kits de producción, específicamente de las impresoras. Se deberá especificar al menos: dimensiones del espacio apropiado para ubicación de la impresora y circulación del personal, peso, tipo/cantidad de tomas eléctricas, voltaje requerido, punto (s) de red datos y cualquier otro dato necesario para verificar los requisitos para instalación y operación óptima, de los equipos del kit de producción (PC’s, impresoras, lectores y cajas fuertes)  El proveedor deberá realizar por su cuenta cualquier instalación eléctrica, de datos o de seguridad, u otra, así como suministrar cualquier material, pieza o equipo adicional necesarios para la instalación y puesta en operación de los kits en los centros de producción designados. La DIGERCIC y el MREMH proporcionarán el espacio físico requerido en los centros de producción para instalación de los kits, así como, tomas de energía eléctrica y puntos de red de datos existentes y acceso a la red de datos local de la agencia o consulado donde estén ubicados. Adicionalmente, las dos entidades asignarán personal y facilitarán apoyo para la instalación, configuración, pruebas y puesta en operación de los kits de producción.  El proveedor deberá contemplar las actividades previas a realizar para el despliegue de los kits de producción en las agencias y consulados. Actividades previas a considerar serán: visita a los centros de producción establecidos y levantamiento de información, instalaciones eléctricas o de datos o de otra índole de ser necesarias, preparación y movilización de los kits a los centros de producción, entrenamiento a usuarios designados por la DIGERCIC (operadores de producción, de control de calidad, supervisores), creación de usuarios, roles y permisos para acceso al SEDIP, entre otras.  El proveedor deberá facilitar el entrenamiento al personal técnico que la DIGERIC delegue para la instalación, configuración, puesta en operación, pruebas, aseguramiento y soporte de primer nivel de los equipos y software de los kits de producción. Se deberá entregar la documentación técnica y de usuario respectiva, así como manuales, drivers, y cualquier ítem necesario para el entrenamiento del personal designado.   * **Alcance de la implementación de kits de producción**   El proveedor deberá tomar en cuenta que el despliegue de los kits de producción estará limitado a:   1. **ECUADOR**    * 3 agencias de la DIGERCIC    * 1 oficina del MREMH 2. **EXTRANJERO**    * 1 consulado del MREMH en Nueva York (USA)    * 1 consulado del MREMH en Madrid (España)  * **Implementación de kits de producción de pasaportes** * **Implementación de piloto de producción de pasaportes de prueba**   El proveedor deberá implementar un piloto de producción de pasaportes de prueba. El piloto deberá implementarse en la agencia matriz de la DIGERCIC en Quito con una duración de al menos 2 semanas en paralelo al despliegue de los kits de captura en esa agencia, previo al comienzo de operaciones.  El proveedor deberá implementar al menos 1 kit de producción en el centro de producción de la agencia con el objeto de producir en paralelo pasaportes de lectura mecánica y pasaportes electrónicos –de prueba- para los solicitantes.  El proveedor deberá asegurar que para la emisión de los pasaportes -de prueba- el operador siga el procedimiento definido en los requerimientos funcionales para la producción de pasaportes. Esto comprende desde la autenticación por huella del operador en el SEDIP, el desbloqueo contra escritura del chip del pasaporte, la validación de inventario de las libretas, el monitoreo de la codificación electrónica y la validación automática, la impresión gráfica de la página de datos, el aseguramiento de la calidad del pasaporte tanto manual como electrónica (con el lector) y preparación para entrega del pasaporte. Al finalizar las 2 semanas del piloto se deberán haber producido al menos 20 pasaportes -de prueba-. Esta cantidad podrá ser cambiada por la DIGERCIC previo aviso al proveedor.   * **Implementación de kits de producción para pasaportes en el país**   El proveedor deberá ejecutar la implementación de los kits de producción para pasaportes conforme el plan y cronograma de trabajo que la DIGERCIC apruebe. La primera agencia en la cual se deberá desplegar el servicio de emisión de pasaportes electrónicos será la agencia matriz de la DIGERCIC en Quito. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días de anticipación al proveedor.  El proveedor deberá retirar los kits de producción de la bodega de la DIGERCIC ubicada en el edificio matriz en Quito, en coordinación con la DIGERCIC. Posteriormente, procederá a preparar cada kit, previo al envío, por su cuenta, a la(s) agencia(s) correspondiente(s) según el cronograma de trabajo.  Una vez en sitio y conforme el cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por la DIGERCIC deberán proceder a instalar, configurar y probar cada kit de producción con el SEDIP.  Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de producción con el SEDIP y los sistemas propios de la DIGERCIC. El proveedor deberá considerar que, los kits de producción del sistema anterior continuarán en operación atendiendo la producción de pasaportes de lectura mecánica, hasta la finalización del despliegue del sistema e emisión o hasta que la DIGERCIC notifique otra directriz al proveedor.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de producción de pasaportes en cada centro de producción según el cronograma de trabajo y hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico de la DIGERCIC prestará también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el proveedor activará el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de emisión de pasaportes en la(s) agencia(s) en las cuales se haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por la DIGERCIC un acta de entrega-recepción con los datos de cada kit de producción implementado. Además, deberá elaborar un informe por agencia que detalle los trabajos realizados, la cantidad de kits implementados, la evidencia de la operatividad de los kits con el SEDIP, los usuarios, roles y permisos creados para uso de los kits, registro fotográfico de cada kit instalado, anexos y cualquier información adicional que se considere necesario.   * **Implementación de kits de producción en el extranjero**   Conforme el alcance especificado anteriormente, el proveedor deberá implementar kits de producción en los consulados de Nueva York (USA) y Madrid (España), conforme el plan y cronograma de trabajo que la DIGERCIC apruebe.  El primer consulado en el cual se deberá desplegar el servicio de emisión de pasaportes electrónicos será el de Nueva York. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días calendario de anticipación al proveedor.  El proveedor deberá retirar los kits de la bodega matriz de la DIGERCIC en Quito y realizar la preparación respectiva. Posteriormente, deberá devolver los kits listos a la DIGERCIC, la cual a su vez entregará al MREMH para el envío al consulado. Los costos del envío deberán ser asumidos por el proveedor, salvo que la DIGERCIC notifique por escrito lo contrario, con una anticipación de 7 días calendario.  Una vez en sitio y conforme cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por el MREMH y/o la DIGERCIC deberá proceder a instalar, configurar y probar cada kit de producción con el SEDIP. Cada centro de producción cuenta con puntos de energía eléctrica y de datos para conexión de kit de producción, sin embargo, el proveedor, por su cuenta, deberá realizar cualquier instalación adicional, de ser necesario para puesta en operación del kit de producción. Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de producción con el SEDIP y los sistemas propios de la DIGERCIC.  El proveedor deberá considerar que el kit de producción deberá ser conectado a la red de área local del consulado, la cual deberá conectarse al centro de datos principal y alterno por medio de una red privada virtual (VPN, por las siglas en inglés) implementado en un gateway de seguridad principal. La VPN será del tipo punto a punto y encriptará el tráfico entre el kit de captura y los centros de datos de la DIGERIC que se transmitirá por la Internet. Se deberá implementar un gateway secundario para uso en caso de falla del principal.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de emisión de pasaportes hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico del MREMH y/o de la DIGERCIC prestará también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el MREMH y el proveedor activarán el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de emisión de pasaportes en el consulado una vez que haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por el MREMH y/o por la DIGERCIC un acta de entrega-recepción con los datos de cada kit implementado. Además, deberá elaborar un informe que, al menos contenga: detalle los trabajos realizados; la cantidad de kits implementados; la evidencia de la operatividad de los kits con el SEDIP; los usuarios entrenados para operar los kits de producción y el SEDIP; el registro fotográfico de cada kit de producción instalado y anexos. El informe podrá incluir cualquier información adicional que el proveedor o a DIGECIC considere necesario  Para la implementación del kit de producción en el consulado de Madrid en España regirán los mismos requerimientos que para el consulado de Nueva York en Estados Unidos (USA). |  |  |

# KITS DE ENTREGA DE DOCUMENTOS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| Los kits de entrega de documentos de identidad y pasaportes estarán conformados por un conjunto de equipos y programas de software que permitirán acceder y utilizar el SEDIP para autenticar biométricamente la identidad del solicitante y registrar la entrega del pasaporte, o solicitar reprocesamiento en caso que el solicitante encuentre alguna física o de información. El operador deberá recuperar la solicitud de emisión del documento a entregar escaneando el número único del documento, o el código QR o el número de serie del documento con el lector de documentos OACI. De no ser posible la lectura, el operador podrá ingresar manualmente el número de identidad o el número del documento. A continuación, el operador deberá entregar el documento al solicitante para su revisión. En caso que el solicitante no tenga objeciones deberá colocar el documento en el lector de documentos OACI para leer la foto almacenada y compararla con una foto tomada con la cámara de la estación de trabajo. En caso que la autenticación sea positiva, el sistema solicitará registrar la entrega del documento en el SEDIP con lo cual finalizará el proceso de emisión.  En la mayoría de agencias de la DIGERCIC y consulados del MREMH, la entrega de pasaportes se realizará en las estaciones de captura. En esos casos, el kit de captura será parcial. En el resto de agencias de la DIGERCIC y los consulados de Nueva York y Madrid, la entrega de pasaportes se realizará en estaciones de trabajo separadas de las de captura. En esos casos, el kit de captura será completo. La siguiente tabla especifica las cantidades de kits parciales y completos a suministrar.   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **ENTIDAD** | **CANTIDAD** | **TIPO DOCUMENTO** | **KITS PARCIALES DE ENTREGA** |  | **KITS COMPLETOS DE ENTREGA** | | **DIGERCIC AGENCIAS** | 183 | CEDULA | 142 | 62 | | | 25 | PASAPORTE | 22 | 5 | | | **MREMH CONSULADDOS** | 80 | CEDULA / PASAPORTE | 81 | 7 | | | Stock de backup | | | 45 | 14 | | | **TOTALES** | | | **290** | **88** | |   Un kit parcial de entrega de documentos estará compuesto únicamente por un lector de documentos OACI 9303 que podrá leer/capturar información de documentos de identidad y pasaportes. El proveedor deberá instalar y conectar el lector en cada estación de captura.  Un kit completo de entrega de documentos estará compuesto por los equipos especificados en la siguiente tabla.   |  |  |  |  | | --- | --- | --- | --- | | **Nro**. | **EQUIPO** | **CANTIDAD** | **ROL** | | 1 | COMPUTADORA PERSONAL FACTOR “ULTRA-SIM” | 1 | Acceso al SURI, SEDIP, software utilitario (email, ofimática) y conexión/control de equipos del kit. | | 2 | ESCANER DE HUELLAS UNIDACTILAR | 1 | Captura de huella dactilar para autenticación del operador en el SEDIP. | | 4 | CAMARA FOTOGRAFICA DIGITAL Y TRIPODE | 1 | Captura de foto del rostro del solicitante (conforme OACI) para validación biométrica facial de la identidad del solicitante. | | 7 | LECTOR DE DOCUMENTOS OACI 9303 | 1 | Lectura electrónica del documento mediante la MRZ y de la foto almacenada en el chip del documento para validación biométrica facial de la identidad del solicitante. |   Las especificaciones técnicas mínimas de los equipos de los kits de entrega de pasaportes se encuentran en el Anexo E. Los equipos deberán ser nuevos de fábrica, no re-manufacturados y fabricados el año en que sean entregados a la DIGERCIC.  Debido a la normativa legal ecuatoriana, el sistema operativo de la PC del kit podrá ser preferencia libre open source (ej., Linux); o privativo (ej., de Microsoft) en sus versiones recientes. Los controladores (drivers) y kits de desarrollo de software de los equipos periféricos deberán ser compatibles con el sistema operativo que se proporcione. El proveedor deberá suministrar las licencias o suscripciones de software respectivas para el sistema operativo y los programas de software que se solicitan. Todas las licencias o suscripciones deberán estar a nombre de la DIGERCIC.  El oferente deberá proveer e instalar software antivirus en los PC de los kits de entrega, así como las suscripciones o licencias respectivas.  El proveedor deberá implementar una herramienta o funcionalidad para controlar y garantizar que solo los equipos inventariados y autorizados para cada kit de entrega puedan acceder y utilizar el SEDIP para la funcionalidad de entrega de pasaportes.  El oferente deberá proveer e instalar en cada PC del kit una herramienta de seguridad de punto final (endpoint security tool) que tenga la característica para prevenir la fuga de datos (data loss prevention) así como protección contra spam/virus, bloqueo de actividad maliciosa, control de navegación Web  Ese software particularmente deberá permitir controlar los puertos de entrada-salida (ej., USB), dispositivo de lectura/escritura de CD/DVD, puertos infrarrojos, bluetooh, Wifi, RJ45, para evitar la copia/transmisión de información no autorizada. El oferente deberá suministra las suscripciones o licencias respectivas para cada PC del kit de producción del software de seguridad de punto final.  El oferente deberá proveer e instalar software monitoreo y administración centralizada del PC (incluso el encendido y apagado) del kit. El oferente deberá facilitar las suscripciones o licencias respectivas para cada PC del kit de entrega; así de la consola centralizada de administración del software centralizado de monitoreo y administración.  La DIGERCIC podrá instalar o facilitar el acceso a herramientas de software y/o sistemas/aplicaciones informáticas en los PC’s de los kits, siempre que sea compatible con el hardware y software base de las mismas. El software a instalar por parte de la DIGERCIC consistirá al menos de: cliente de email, herramienta de ofimática, lector de archivos PDF, cliente de control remoto de la PC, navegadores Web (browsers): Mozilla Firefox, Google Chrome y Microsoft Internet Explorer, manejador de impresora de red.  La garantía técnica de los equipos y la vigencia de las licencias o suscripciones de software con mantenimiento/actualización incluidos deberá ser de al menos 3 años. La vigencia del soporte y mantenimiento/actualización de licencias suscripciones regirá partir de la fecha de la entrada en producción del SEDIP y así aceptado por la DIGERCIC mediante de acta entrega-recepción.  Durante la vigencia del contrato se deberá realizar mantenimientos preventivos con frecuencia semestral para garantizar la operatividad de los kits de entrega. Para mantenimientos correctivos se deberá aplicar la garantía técnica solicitada. El cambio de equipos, piezas y accesorios deberá estar contemplado como parte de los mantenimientos preventivos y correctivos sin costo adicional para la DIGERCIC.   * **Implementación de kits de entrega**   El proveedor deberá suministrar todos los kits parciales y completos de entrega en la bodega de la DIGERCIC.  El proveedor deberá instalar los kits parciales de entrega junto con las estaciones de captura de datos tanto para documentos de identidad y pasaportes en las agencias de la DIGERCIC como en los consulados del MREMH.  El proveedor deberá proponer un plan y cronograma de despliegue de kits completos de entrega para aprobación de la DIGERCIC. El plan deberá considerar actividades previas, durante y después de la implementación de los kits completos. La instalación y puesta en operación deberá considerar horarios de trabajo a partir de las 17h30, fines de semana o feriados, es decir, horarios fuera de oficina, para no interrumpir los servicios de emisión de documentos de pasaportes.  El proveedor deberá contemplar las actividades previas a realizar para el despliegue de los kits de entrega en las agencias y consulados. Actividades previas a considerar serán: Instalación/configuración de los kits, entrenamiento a usuarios designados por la DIGERCIC (operadores de entrega, supervisores), creación de usuarios, roles y permisos para acceso al SEDIP, preparación y envío de equipos a las agencias, entre otras.  El proveedor deberá facilitar el entrenamiento al personal técnico que la DIGERIC delegue para la instalación, configuración, puesta en operación, pruebas, aseguramiento y soporte de primer nivel de los equipos y software de los kits de entrega. Se deberá entregar la documentación técnica y de usuario respectiva, así como manuales, drivers, y cualquier ítem necesario para el entrenamiento del personal designado.   * **Alcance de la implementación de kits de entrega**   El proveedor deberá tomar en cuenta que el servicio de despliegue de kits completos de entrega de documento estará limitado a:   1. **ECUADOR**    * 41 agencias de la DIGERCIC de emisión de documentos de identidad    * 25 agencias de la DIGERCIC de emisión de pasaportes    * 1 oficina del MREMH de emisión de pasaportes 2. **EXTRANJERO**    * 1 consulado del MREMH en Nueva York (USA) de emisión de documentos de identidad y pasaportes    * 1 consulado del MREMH en Madrid (España) de emisión de documentos de identidad y pasaportes   El proveedor deberá considerar que la instalación de los kits completos de entrega en el resto de consulados estará a cargo del MREMH. El proveedor deberá facilitar el entrenamiento necesario y suficiente al personal que designe el MREMH en coordinación de la DIGERCIC.   * **Implementación de kits de entrega de pasaportes** * **Implementación de piloto de entrega de pasaportes de prueba**   El proveedor deberá implementar un piloto de entrega de pasaportes electrónicos de prueba. El piloto deberá implementarse en la agencia matriz de la DIGERCIC en Quito con una duración de al menos 2 semanas previo al comienzo de operaciones.  El proveedor deberá implementar al menos 1 kit de entrega en 1 estación de trabajo del área de pasaportes con el objeto de realizar la entrega en paralelo de pasaportes de lectura mecánica y pasaportes electrónicos –de prueba- a los solicitantes.  El proveedor deberá asegurar que para la emisión de los pasaportes -de prueba- el operador siga el procedimiento definido en los requerimientos funcionales. Al finalizar las 2 semanas del piloto se deberán haber probado la entrega de al menos 20 pasaportes -de prueba-.  El proveedor deberá considerar que un kit de captura y un kit de producción de pasaportes estarán también implementados en la agencia Matriz de la DIGERCIC en Quito, para la ejecución del piloto.  El proveedor deberá elaborar un informe de la ejecución de la entrega de pasaportes -de prueba- al finalizar el mismo.   * **Implementación de kits de entrega de pasaportes en el país**   El proveedor deberá ejecutar la implementación de los kits de entrega para pasaportes conforme el plan y cronograma de trabajo que la DIGERCIC apruebe. La primera agencia en la cual se deberá desplegar el servicio de entrega de pasaportes electrónicos será la agencia matriz de la DIGERCIC en Quito. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días de anticipación al proveedor.  El proveedor deberá retirar los kits de entrega de la bodega de la DIGERCIC ubicada en el edificio matriz en Quito, en coordinación con la DIGERCIC. Posteriormente, procederá a preparar cada kit, previo al envío, por su cuenta, a la(s) agencia(s) correspondiente(s) según el cronograma de trabajo.  Una vez en sitio y conforme el cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por la DIGERCIC deberán proceder a instalar, configurar y probar cada kit de entrega con el SEDIP. Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de entrega con el SEDIP y los sistemas propios de la DIGERCIC.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de entrega de pasaportes en cada agencia según el cronograma de trabajo y hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico de la DIGERCIC prestará también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el proveedor activará el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de entrega de pasaportes en la(s) agencia(s) en las cuales se haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por la DIGERCIC un acta de entrega-recepción con los datos de cada kit implementado. Además, deberá elaborar un informe por agencia que detalle los trabajos realizados, la cantidad de kits implementados, la evidencia de la operatividad de los kits con el SEDIP, los usuarios, roles y permisos creados para uso de los kits de captura, registro fotográfico de cada kit de captura instalado, anexos y cualquier información adicional que se considere necesario.   * **Implementación de kits de entrega de pasaportes en el extranjero**   Conforme el alcance especificado anteriormente, el proveedor deberá implementar kits de entrega en los consulados de Nueva York (USA) y Madrid (España), conforme el plan y cronograma de trabajo que la DIGERCIC apruebe.  El primer consulado en el cual se deberá desplegar el servicio de entrega de pasaportes electrónicos será el de Nueva York. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días calendario de anticipación al proveedor.  El proveedor deberá retirar los kits de la bodega matriz de la DIGERCIC en Quito y realizar la preparación respectiva. Posteriormente, deberá devolver los kits listos a la DIGERCIC, la cual a su vez entregará al MREMH para el envío al consulado. Los costos del envío deberán ser asumidos por el proveedor, salvo que la DIGERCIC notifique por escrito lo contrario, con una anticipación de 7 días calendario.  Una vez en sitio y conforme cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por el MREMH y/o la DIGERCIC deberá instalar, configurar y probar cada kit de entrega con el SEDIP. Cada estación de entrega cuenta con puntos de energía eléctrica y de datos para conexión de kit de entrega. Personal del proveedor y de la DIGERCIC facilitarán apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de entrega con el SEDIP y los sistemas propios de la DIGERCIC. Las pruebas de los kits de entrega comprenderán también la captura para emisión de documentos de identidad considerando que se implementará primero la emisión de pasaportes.  El proveedor deberá considerar que el kit de entrega deberá ser conectado a la red de área local del consulado por medio de la interface RJ45 del PC y el punto de datos disponible en la estación de trabajo. El proveedor deberá conectar el kit de captura al centro de datos principal por medio de una red privada virtual (VPN, por las siglas en inglés) implementada en equipo gateway de seguridad principal.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de entrega de pasaportes hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico del MREMH y/o de la DIGERCIC prestará también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el MREMH y el proveedor activarán el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de entrega de pasaportes en el consulado una vez que haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por el MREMH y/o por la DIGERCIC un acta de entrega-recepción con los datos de cada kit implementado. Además, deberá elaborar un informe que, al menos contenga: detalle los trabajos realizados; la cantidad de kits implementados; la evidencia de la operatividad de los kits con el SEDIP; los usuarios entrenados para operar los kits de captura y el SEDIP; el registro fotográfico de cada kit de entrega instalado y anexos. El informe podrá incluir cualquier información adicional que el proveedor o a DIGECIC considere necesario  Para la implementación de los kits de entrega en el consulado de Madrid en España regirán los mismos requerimientos que para el consulado de Nueva York en Estados Unidos (USA).   * **Implementación de kits de entrega de documentos de identidad** * **Implementación de piloto de entrega de documentos de identidad de prueba**   El proveedor deberá implementar un piloto de entrega de los documentos de identidad -de prueba-. El piloto deberá implementarse en la agencia matriz de la DIGERCIC en Quito con una duración de al menos 2 semanas previo al comienzo de operaciones.  El proveedor deberá implementar al menos 1 kit de entrega en 1 estación de trabajo del área de entrega de documentos de identidad con el objeto de realizar la entrega en paralelo de documentos de identidad con el sistema actual y documentos de identidad –de prueba- con el nuevo sistema.  El proveedor deberá asegurar que para la emisión de los pasaportes -de prueba- el operador siga el procedimiento definido en los requerimientos funcionales. Al finalizar las 2 semanas del piloto se deberá haber probado la entrega de al menos 100 documentos de identidad -de prueba-.  El proveedor deberá considerar que dos kits de captura y un kit de producción de documentos de identidad para pruebas estarán también implementados en la agencia Matriz de la DIGERCIC en Quito, para la ejecución del piloto.  El proveedor deberá elaborar un informe de la ejecución de la entrega de documentos de identidad -de prueba- al finalizar el mismo.   * **Implementación de kits completos de entrega de documentos de identidad en el país**   El proveedor deberá ejecutar la implementación de los kits completo de entrega de pasaportes conforme el plan y cronograma de trabajo que la DIGERCIC apruebe. La primera agencia en la cual se deberá desplegar el servicio de entrega de documentos de identidad será la agencia matriz de la DIGERCIC en Quito. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días de anticipación al proveedor.  El proveedor deberá retirar los kits de entrega de la bodega de la DIGERCIC ubicada en el edificio matriz en Quito, en coordinación con la DIGERCIC. Posteriormente, procederá a preparar cada kit, previo al envío, por su cuenta, a la(s) agencia(s) correspondiente(s) según el cronograma de trabajo.  Una vez en sitio y conforme el cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por la DIGERCIC deberán proceder a instalar, configurar y probar cada kit de entrega con el SEDIP. Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de entrega con el SEDIP y los sistemas propios de la DIGERCIC.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de entrega de pasaportes en cada agencia según el cronograma de trabajo y hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico de la DIGERCIC prestará también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el proveedor activará el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de entrega de pasaportes en la(s) agencia(s) en las cuales se haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por la DIGERCIC un acta de entrega-recepción con los datos de cada kit implementado. Además, deberá elaborar un informe por agencia que detalle los trabajos realizados, la cantidad de kits implementados, la evidencia de la operatividad de los kits con el SEDIP, los usuarios, roles y permisos creados para uso de los kits de captura, registro fotográfico de cada kit de captura instalado, anexos y cualquier información adicional que se considere necesario. |  |  |

# GATEWAYS DE SEGURIDAD PARA CONSULADOS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El acceso y uso de los kits fijos de captura, kits de producción y kits de entrega desde los consulados del MREMH del extranjero al SEDIP en Quito, será por medio de enlaces de Internet a cargo del MREMH.  El proveedor deberá establecer conexiones seguras y cifradas entre cada consulado y el SEDIP en Quito implementando Redes Privadas Virtuales (VPN’s por sus siglas en inglés) del tipo punto a punto.   * **Conexión de los consulados de Nueva York y Madrid**   El proveedor deberá suministrar equipos físicos para gateways de seguridad para implementación de VPN’s sitio a sitio desde los consulados de Nueva York y Madrid al sistema central en Quito. Estos equipos deberán ser implementados en alta disponibilidad para garantizar que las conexiones sean permanentes y tolerantes a fallos. La distribución de los equipos Gateway se muestra en la siguiente tabla.   |  |  |  |  | | --- | --- | --- | --- | | **ENTIDAD** | **CONSULADOS CON CENTRO DE PRODUCCION** | **CANTIDAD GATEWAYS** | **SUBTOTAL** | | MREMH | 2 | 2 | 4 | | **Total** | | | **4** |   El proveedor deberá establecer conexiones seguras y cifradas entre cada consulado y el sistema central implementando Redes Privadas Virtuales (VPN’s por sus siglas en inglés) del tipo punto a punto, desde los consulados de Nueva York y Madrid, conforme el alcance de implementación en el extranjero solicitado a proveedor.  La DIGERCIC en coordinación con el MREMH facilitarán la información necesaria de las redes locales y de los enlaces de Internet que estarán disponibles en los consulados de Nueva York y Madrid. El proveedor de su parte deberá elaborar un informe de requerimientos de red para implementación de las VPN’s solicitadas. Esto comprenderá: IP’s públicas, puntos de datos, tomas de energía eléctrica, espacio de racks, entre otros. De ser necesario, el proveedor deberá realizará las instalaciones de datos o eléctrica o de otro tipo necesarias para la instalación y puesta en marcha de los gateways.  El proveedor deberá establecer conexiones seguras y cifradas entre cada consulado y el sistema central implementando Redes Privadas Virtuales (VPN’s por sus siglas en inglés) del tipo punto a punto, desde los consulados de Nueva York y Madrid, conforme el alcance de implementación en el extranjero solicitado a proveedor.  El proveedor deberá suministrar equipos físicos para gateways de seguridad. Estos equipos deberán ser implementados en alta disponibilidad para garantizar que las conexiones de los equipos desde los dos consulados al SEDIP en Quito sean permanente y tolerante a fallos. Para el diseño, pruebas y operatividad de este requerimiento, la DIGERCIC y el MREMH facilitarán la información necesaria de la red y de los equipos en operación en los consulados de Nueva York y Madrid. La distribución de los equipos Gateway se muestra en la siguiente tabla.  Las especificaciones técnicas mínimas de los equipos de los gateways de seguridad se encuentran en el Anexo E. Los equipos deberán ser nuevos de fábrica, no re-manufacturados y fabricados el año que sean entregados a la DIGERCIC.  La garantía técnica de los equipos y la vigencia de las licencias o suscripciones de software con mantenimiento/actualización incluidos deberá ser de al menos 3 años. La vigencia del soporte y mantenimiento/actualización de licencias suscripciones regirá partir de la fecha de la entrada en producción del SEDIP y así aceptado por la DIGERCIC mediante de acta entrega-recepción.  Durante la vigencia del contrato se deberá realizar mantenimientos preventivos con frecuencia semestral para garantizar la operatividad de los gateways. Para mantenimientos correctivos se deberá aplicar la garantía técnica solicitada. El cambio de equipos, piezas y accesorios deberá estar contemplado como parte de los mantenimientos preventivos y correctivos sin costo adicional para la DIGERCIC.   * **Implementación de los gateways**   El proveedor deberá entregar los gateways a la bodega de la DIGERCIC. El proveedor deberá considerar la instalación y puesta en operación de los gateways en el plan de implementación de equipos y sistema en los consulados de Nueva York y Madrid.  El proveedor deberá entregar a la DIGERCIC un documento especificando los requerimientos para la instalación de los gateways. Se deberá especificar al menos: direcciones IP’s públicas, tipo/cantidad de tomas eléctricas, voltaje requerido, punto(s) de red datos, espacio para rack y cualquier otro dato necesario para verificar los requisitos para instalación y operación óptima de los gateways.  El proveedor deberá realizar por su cuenta cualquier instalación eléctrica, de datos o de seguridad, u otra, así como suministrar cualquier material (ej., cables, etc.), pieza (ej., bandejas para rack o para pared) o equipo adicional necesarios para la instalación y puesta en operación de los gateways en los consulados mencionados. El MREMH proporcionará el espacio físico requerido en los consulados para instalación de los gateways así como, tomas de energía eléctrica y puntos de red de datos existentes. Adicionalmente, las dos entidades asignarán personal y facilitarán apoyo para la instalación, configuración, pruebas y puesta en operación de los gateways  El proveedor deberá contemplar las actividades previas a realizar para el despliegue de los gateways en los consulados. Actividades previas a considerar serán: análisis de la red local, propuesta de conexión, revisión de instalaciones eléctricas o de datos de ser necesario, entre otras.  El proveedor deberá facilitar el entrenamiento al personal técnico que la DIGERIC y/o el MREMH delegue para la instalación, configuración, puesta en operación, pruebas, aseguramiento y soporte de primer nivel de los gateways. Se deberá entregar la documentación técnica y de usuario respectiva, así como manuales, drivers, y cualquier ítem necesario para el entrenamiento del personal designado.   * **Implementación de gateways de seguridad en el extranjero**   El proveedor deberá retirar los gateways de la bodega matriz de la DIGERCIC en Quito y realizar la preparación respectiva, de ser necesario. Posteriormente, deberá devolver los gateways listos a la DIGERCIC, la cual a su vez entregará al MREMH para el envío al consulado. Los costos del envío deberán ser asumidos por el proveedor, salvo que la DIGERCIC notifique por escrito lo contrario, con una anticipación de 7 días calendario.  Una vez en sitio y conforme cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por el MREMH y/o la DIGERCIC deberá proceder a instalar, configurar y probar los gateways. Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de los gateways desde los consulados al SEDIP en Quito.  El proveedor deberá suscribir con un funcionario designado por el MREMH y/o por la DIGERCIC un acta de entrega-recepción con los datos de gateways implementados. Además, deberá elaborar un informe que, al menos contenga: detalle los trabajos realizados; la cantidad de gateways implementados; la evidencia de la operatividad de los gateways; los usuarios entrenados para administrar los gateways; el registro fotográfico de gateway instalado y anexos.  El informe podrá incluir cualquier información adicional que el proveedor o a DIGECIC considere necesario  Para la implementación los gateways (principal y secundario) en el consulado de Madrid en España regirán los mismos requerimientos que para el consulado de Nueva York en Estados Unidos (USA). |  |  |

# INSUMOS PARA IMPRESION DE PASAPORTES

|  |  |  |
| --- | --- | --- |
| **ESPECIFICACIÓN TÉCNICA** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| El proveedor deberá entregar los insumos necesarios para la impresión gráfica de la página de datos de los pasaportes. Los insumos deberán permitir imprimir mínimo 1’000.000 de pasaportes. Estos insumos serán, pero no están limitados a: cartuchos de tinta negra y a colores, unidades de purga, cabezales de impresión y kits de limpieza, según la marca y modelo de impresora de pasaportes que suministre el proveedor.  Los plazos de entrega y cantidad de insumos requerido se especifican en la tabla a continuación.   |  |  |  | | --- | --- | --- | | **TIPO INSUMO** | **CANTIDAD** | **PLAZO** | | CARTUCHOS DE TINTA, CABEZALES, KITS DE LIMPIEZA, ETC. | Lote 1: Para imprimir 300.000 pasaportes | Hasta 15 días calendario antes de la fecha de inicio de operaciones de la agencia matriz de Quito. | | Lote 2: Para imprimir 200.000 pasaportes | Hasta 100 días calendario después de la firma de acta de entrega-recepción del lote 1. | | Lote 3: Para imprimir 500.000 pasaportes | Hasta 100 días calendario después de la firma de acta de entrega-recepción del lote 2. |   El proveedor deberá detallar las cantidades de insumos para impresión que entregará para cubrir la impresión de mínimo 1’000.000 de pasaportes. Los insumos para impresión deberán ser entregados en la bodega matriz de la DIGERCIC en la ciudad de Quito. Los costos hasta la entrega correrán por parte del proveedor. Los insumos deberán ser fabricados el año que se entreguen a la DIGERCIC con una durabilidad de al menos 2 años, bajo las condiciones de conservación que especifique el proveedor. El proveedor deberá entregar un informe señalando las condiciones que deberá cumplir la bodega de la DGERCIC para el almacenamiento y conservación de los insumos para impresión.  La DIGERCIC será la entidad encargada de enviar los insumos a los 3 centros de producción de pasaportes en el país; y entregará directamente los insumos al MREMH para el envío a los 3 centros de producción de pasaportes a cargo de esa entidad (1 en el país y 2 en el extranjero).  El proveedor deberá facilitar a la DIGERCIC toda la documentación y soporte técnico, presencial o remoto, para implementación de otra lámina de seguridad para los pasaportes luego que se emita el primer millón de pasaportes electrónicos y el contrato esté vigente. En caso que la DIGERCIC así lo decida, comunicará el cambio al proveedor con al menos 90 días de anticipación. |  |  |

# KITS DE PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD

|  |  |  |
| --- | --- | --- |
| **ESPECIFICACIÓN TÉCNICA** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Los kits de producción de documentos de identidad estarán conformados por un conjunto de equipos y programas de software, que permitirán acceder y utilizar el SEDIP para: grabar/codificar los datos del solicitante en el chip del documento de identidad, imprimir los datos del solicitante en el documento de identidad y asegurar la calidad del documento de identidad, de conformidad a las recomendaciones de la OACI vigentes.  El proveedor deberá considerar que, los kits a ser provistos funcionarán en paralelo con las impresoras que actualmente se utilizan para la producción de documentos de identidad hasta que termine el despliegue del SEDIP, se cancele la impresión de documentos con las impresoras actuales o la DIGERCIC notifique otra directriz al respecto. Esto debido a que, la puesta en operación del nuevo SEDIP será progresiva, por tanto, la DIGECIC deberá seguir produciendo documentos con el sistema hasta que finalice la implementación del nuevo sistema.  El proveedor deberá suministrar kits para 41 centros de impresión de producción de documentos de identidad que cuenta actualmente la DIGERCIC en 41 agencias del país. El número de impresoras a ser provistos, está en función de la producción de documentos de identidad de cada centro. La siguiente tabla especifica la distribución de centros de impresión y la cantidad de impresoras que debe ser tomado como referencia. El número de lectores para aseguramiento de calidad de los documentos de identidad está ligado al número de impresoras.   |  |  |  |  | | --- | --- | --- | --- | | **AGENCIAS**  **DIGERCIC** | **NUMERO DE CENTROS DE PRODUCCION** | **CANTIDAD DE KITS DE PRODUCCION** | **SUBTOTAL DE KITS DE PRODUCCION** | | TIPO 1 | 22 | 1 | 22 | | TIPO 2 | 16 | 2 | 32 | | TIPO 3 | 1 | 3 | 3 | | TIPO 3 | 2 | 4 | 8 | | Stock de Backup | | | 2 | | **TOTAL** | | | **67** |   La siguiente tabla indica los tipos y cantidad de equipos por cada kit de impresión y el rol que cumplirán:     |  |  |  |  | | --- | --- | --- | --- | | **Nro**. | **EQUIPO** | **CANTIDAD** | **ROL** | | 1 | COMPUTADORA PERSONAL “ULTRA-SLIM” | 1 | Acceso al SURI, SEDIP, software utilitario (email, ofimática, etc.) y conexión/control de equipos del kit. | | 2 | IMPRESORA DE GRABADO POR LÁSER | 1 | Codificación/grabado/verificación automática de los datos demográficos y biométricos en el chip RFID conforme OACI 9303 versión 2015. Impresión de la sección visual del documento de identidad. | | 3 | ESCANER DE HUELLAS UNIDACTILAR | 1 | Captura de huella dactilar para autenticación del operador en el SEDIP. | | 4 | LECTOR DE DOCUMENTOS OACI DOC 9303 | 1 | Lectura de los datos del documento de identidad mediante MRZ, BAC/SAC y verificación visual de seguridades del documento para luz blanca, ultravioleta o infrarroja. |   La tecnología de impresión de las tarjetas deberá ser de grabado rayo láser en tarjetas de policarbonato. Las tarjetas en blanco tendrán incorporado un chip RFID con la antena respectiva y cumplirán las normas/recomendaciones aplicables tanto de lSO como de la OACI. El proveedor de las tarjetas en blanco de policarbonato para emisión de documentos de identidad será el Instituto Geográfico Militar (IGM).  El proveedor deberá suministrar impresoras de grabado por láser que eviten o disminuya: la intervención de operadores durante el proceso de producción, la manipulación de libretas y varios dispositivos, el tiempo de producción y riesgos de seguridad en el centro de producción.  Los chips de las tarjetas en blanco estarán bloqueados contra escritura mediante un esquema de criptografía simétrica acordado entre el IGM y la DIGERCIC. Es un mecanismo de seguridad establecido para evitar el mal uso de las tarjetas e impedir su utilización en caso de pérdida o robo. En proveedor deberá implementar la funcionalidad para desbloquear los chips durante del proceso de personalización. Para tal efecto, el proveedor deberá validar las llaves instanciadas en el chip de las tarjetas contra las llaves maestras almacenadas en un módulo de seguridad de hardware principal (HSM, por sus siglas en inglés); o en un HSM de contingencia, en caso de falla del principal. Previamente, el proveedor en coordinación con la DIGERCIC y el IGM deberán transportar las llaves maestras generadas por el IGM a los HSM principal y de contingencia, que el proveedor deberá suministrar e implementar para el efecto. La generación y grabación de llaves tanto maestras como las de las tarjetas seguirán estándares y buenas prácticas de la industria privilegiando la seguridad y confiabilidad del proceso. La DIGERCIC facilitará el procedimiento de generación y transporte de claves al proveedor que resulte adjudicado.  Debido al modelo descentralizado de producción de documentos de identidad, las impresoras de engravado láser deberán ser apropiadas para montaje en oficinas, es decir del tipo para escritorio o de rango medio en cuanto a capacidad de personalización e impresión. Las impresoras deberán tener las siguientes especificaciones mínimas:   * Lector para reconocimiento óptico de caracteres para captura automática del número de serie de la tarjeta * Cámara para ubicación exacta de la tarjeta y datos a imprimir * Láser de precisión que permita producir Imágenes Láser Múltiples (MLI, por sus siglas en ingles), Imágenes Láser Cambiables (CLI, por sus siglas en ingles), imágenes tipo fantasma y/o relieves (positivos/negativos) * Codificador electrónico RFID que permita grabación por no contacto; y comprobación automática de la codificación * Indicadores sonoros y/o gráficos del proceso de producción * Seguridades físicas (por ejemplo, candados) y/o lógicas (por ejemplo, contraseñas) * Bandejas para carga automática de tarjetas en blanco y para salida de tarjetas producidas y rechazadas * SDK para diferentes sistemas operativos y lenguajes de programación * Software para monitoreo centralizado del funcionamiento de cada impresora   El sistema deberá permitir también realizar la lectura y comparación automática de la información codificada en el chip, leída por medio del lector, con la información de la solicitud de emisión del documento de identidad. Se deberán verificar los controles de acceso básico (BAC) y suplementario (SAC/PACE) implementados en el chip, conforme recomienda la OACI.  Todo el proceso de producción, incluido el de aseguramiento de la calidad, deberá ser controlado paso a paso y registrado en el SEDIP previo a la salida del documento de identidad del centro de producción para entrega al solicitante.  Las especificaciones técnicas mínimas de los equipos de los kits de producción de documentos de identidad se encuentran en el Anexo E. Los equipos deberán ser nuevos de fábrica, no re-manufacturados y fabricados el año en que sean entregados a la DIGERCIC.  Debido a la normativa legal ecuatoriana, el sistema operativo de la PC del kit podrá ser preferencia libre open source (ej., Linux); o privativo (ej., de Microsoft) en sus versiones recientes. Los controladores (drivers) y kits de desarrollo de software de los equipos periféricos deberán ser compatibles con el sistema operativo que se proporcione. El proveedor deberá suministrar las licencias o suscripciones de software respectivas para el sistema operativo y los programas de software que se solicitan. Todas las licencias o suscripciones deberán estar a nombre de la DIGERCIC.  El oferente deberá proveer e instalar software antivirus en los PC de los kits de impresión, así como las suscripciones o licencias respectivas.  El proveedor deberá implementar una herramienta o funcionalidad para controlar y garantizar que solo los equipos inventariados y autorizados para cada kit de producción puedan acceder y utilizar el SEDIP para la funcionalidad de producción.  El oferente deberá proveer e instalar en cada PC del kit una herramienta de seguridad de punto final (endpoint security tool) que tenga la característica para prevenir la fuga de datos (data loss prevention) así como protección contra spam/virus, bloqueo de actividad maliciosa, control de navegación Web  Ese software particularmente deberá permitir controlar los puertos de entrada-salida (ej., USB), dispositivo de lectura/escritura de CD/DVD, puertos infrarrojos, bluetooth, Wifi, RJ45, para evitar la copia/transmisión de información no autorizada. El oferente deberá suministra las suscripciones o licencias respectivas para cada PC del kit de producción del software de seguridad de punto final.  El oferente deberá proveer e instalar software monitoreo y administración centralizada del PC (incluso el encendido y apagado) y de la impresora del kit. El oferente deberá facilitar las suscripciones o licencias respectivas para cada PC del kit de producción y para la impresora; así de la consola centralizada de administración del software centralizado de monitoreo y administración.  La DIGERCIC podrá instalar o facilitar el acceso a herramientas de software y/o sistemas/aplicaciones informáticas en los PC’s de los kits, siempre que sea compatible con el hardware y software base de las mismas. El software a instalar por parte de la DIGERCIC consistirá al menos de: cliente de email, herramienta de ofimática, lector de archivos PDF, cliente de control remoto de la PC, navegadores Web (browsers): Mozilla Firefox, Google Chrome y Microsoft Internet Explorer, manejador de impresora de red.  La garantía técnica de los equipos y la vigencia de las licencias o suscripciones de software con mantenimiento/actualización incluidos deberá ser de al menos 3 años. La vigencia del soporte y mantenimiento/actualización de licencias suscripciones regirá partir de la fecha de la entrada en producción del SEDIP y así aceptado por la DIGERCIC mediante de acta entrega-recepción.  Durante la vigencia del contrato se deberá realizar mantenimientos preventivos con frecuencia semestral para garantizar la operatividad de los kits de producción. Para mantenimientos correctivos se deberá aplicar la garantía técnica solicitada. El cambio de equipos, piezas y accesorios deberá estar contemplado como parte de los mantenimientos preventivos y correctivos sin costo adicional para la DIGERCIC.   * **Implementación de los kits de producción de documentos de identidad**   El proveedor deberá entregar todos los kits de producción a la bodega de la DIGERCIC. El proveedor deberá proponer un plan y cronograma de despliegue de los kits de producción para aprobación de la DIGERCIC. El plan deberá considerar actividades previas, durante y después de la implementación de los kits. La instalación y puesta en operación deberá considerar horarios de trabajo a partir de las 17h30, fines de semana o feriados, es decir, horarios fuera de oficina, para no interrumpir los servicios de emisión de documentos de identidad en las agencias y consulados.  El proveedor deberá entregar a la DIGERCIC un informe especificando los requerimientos para la instalación de los kits de producción, específicamente de las impresoras. Se deberá detallar al menos: dimensiones del espacio apropiado para ubicación de la impresora/mesa de soporte y circulación del personal, peso, tipo/cantidad de tomas eléctricas, voltaje requerido, punto (s) de red datos y cualquier otro dato necesario para verificar los requisitos para instalación y operación óptima, de los equipos del kit de producción.  El proveedor deberá realizar por su cuenta cualquier instalación eléctrica, de datos o de seguridad, u otra, así como suministrar cualquier material, pieza o equipo adicional necesarios para la instalación y puesta en operación de los kits en los centros de producción designados. La DIGERCIC proporcionará el espacio físico requerido en los centros de producción para instalación de los kits, así como, tomas de energía eléctrica y puntos de red de datos existentes y acceso a la red de datos local de la agencia donde estén ubicados. Adicionalmente, la DIGERCIC asignará personal técnico y facilitará apoyo para la instalación, configuración, pruebas y puesta en operación de los kits de producción de documentos de identidad.  El proveedor deberá contemplar las actividades previas a realizar para el despliegue de los kits de producción en las agencias. Actividades previas a considerar serán: visita a los centros de producción establecidos y levantamiento de información, instalaciones eléctricas o de datos o de otra índole de ser necesarias, preparación y movilización de los kits a los centros de producción, entrenamiento a usuarios designados por la DIGERCIC (operadores de producción, de control de calidad, supervisores), creación de usuarios, roles y permisos para acceso al SEDIP, entre otras.  El proveedor deberá facilitar el entrenamiento al personal técnico que la DIGERIC delegue para la instalación, configuración, puesta en operación, pruebas, aseguramiento y soporte de primer nivel de los equipos y software de los kits de producción. Se deberá entregar la documentación técnica y de usuario respectiva, así como manuales, drivers, y cualquier ítem necesario para el entrenamiento del personal designado.   * **Alcance de la implementación de kits de producción de documentos de identidad**   El proveedor deberá tomar en cuenta que el despliegue de los kits de producción estará limitado a: 41 agencias de la DIGERCIC   * **Implementación de kits de producción de documentos de identidad** * **Implementación de piloto de producción de documentos e identidad de prueba**   El proveedor deberá implementar un piloto de producción de documentos de identidad –de prueba-. El piloto deberá implementarse en la agencia matriz de la DIGERCIC en Quito con una duración de al menos 2 semanas en paralelo al despliegue de los kits de captura en esa agencia, previo al comienzo de operaciones.  El proveedor deberá implementar al menos 1 kit de producción en el centro de producción de la agencia con el objeto de producir en paralelo documentos de identidad en el formato actual y documentos de identidad en el nuevo formato –de prueba- para los solicitantes.  El proveedor deberá asegurar que para la emisión de los documentos de identidad -de prueba- el operador siga el procedimiento definido en los requerimientos funcionales para la producción de documentos de identidad. Esto comprende desde la autenticación por huella del operador en el SEDIP, el desbloqueo contra escritura del chip del pasaporte, la validación de inventario de las tarjetas, el monitoreo de la codificación electrónica y la validación automática, la impresión gráfica del documento de identidad, el aseguramiento de la calidad del documento de identidad tanto manual como electrónica (con el lector) y preparación para entrega del documento de identidad. Al finalizar las 2 semanas del piloto se deberán haber producido al menos 100 documentos de identidad -de prueba-. Esta cantidad podrá ser cambiada por la DIGERCIC previo aviso al proveedor.   * **Implementación de kits de producción para documentos de identidad en el país**   El proveedor deberá ejecutar la implementación de los kits de producción para documentos de identidad conforme el plan y cronograma de trabajo que la DIGERCIC apruebe. La primera agencia en la cual se deberá desplegar el servicio de emisión de documentos de identidad será la agencia matriz de la DIGERCIC en Quito. La DIGERCIC podrá cambiar esta definición según convenga y notifique con 7 días de anticipación al proveedor.  El proveedor deberá retirar los kits de producción de la bodega de la DIGERCIC ubicada en el edificio matriz en Quito, en coordinación con la DIGERCIC. Posteriormente, procederá a preparar cada kit, previo al envío, por su cuenta, a la(s) agencia(s) correspondiente(s) según el cronograma de trabajo.  Una vez en sitio y conforme el cronograma y horario acordados, el personal del proveedor con apoyo de personal designado por la DIGERCIC deberán proceder a instalar, configurar y probar cada kit de producción con el SEDIP.  Personal del proveedor y de la DIGERCIC deberán facilitar apoyo desde la matriz en Quito para las actividades de configuración y pruebas de cada kit de producción con el SEDIP y los sistemas propios de la DIGERCIC. El proveedor deberá considerar que, los kits de producción del sistema anterior continuarán en operación atendiendo la producción de documentos de identidad (con el formato actual), hasta la finalización del despliegue del sistema e emisión o hasta que la DIGERCIC notifique otra directriz al proveedor.  El proveedor deberá facilitar soporte in-situ para el comienzo de operaciones de producción de documentos de identidad en cada centro de producción según el cronograma de trabajo y hasta por 2 días laborables o hasta que se solucionen incidentes o errores imputables al inicio de operaciones. El personal operativo y técnico de la DIGERCIC prestará también el apoyo y soporte necesarios.  La DIGERCIC en coordinación con el proveedor activará el procedimiento de gestión de incidentes en caso que se presentaren errores o dificultades que interrumpan o paralicen el servicio de producción de documentos de identidad en la(s) agencia(s) en las cuales se haya iniciado operaciones.  El proveedor deberá suscribir con un funcionario designado por la DIGERCIC un acta de entrega-recepción con los datos de cada kit de producción implementado. Además, deberá elaborar un informe por agencia que detalle los trabajos realizados, la cantidad de kits implementados, la evidencia de la operatividad de los kits con el SEDIP, los usuarios, roles y permisos creados para uso de los kits, registro fotográfico de cada kit instalado, anexos y cualquier información adicional que se considere necesario. |  |  |

# KITS MÓVILES DE CAPTURA DE DATOS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| Los kits móviles de captura de datos estarán conformados por equipos y programas de software iguales o similares a los que de un kit fijo de captura. Los kits móviles serán utilizados para la captura de datos fuera de las agencias de la DIGERCIC o los consulados del MREMH para la emisión de documentos de identidad y/o pasaportes.  El proveedor deberá considerar que el funcionamiento de los kits móviles podrá ser: en-línea o fuera de-línea.  Para el modo de funcionamiento en-línea, un kit móvil deberá poder conectarse al sistema central a través de la Internet. En este caso, el proceso de captura será en-línea tal como ocurre desde una estación fija de captura de datos en una agencia o consulado. La conexión de la móvil al sistema central será por medio de una VPN que deberá configurarse en el computador portátil del kit móvil.  Para el modo de funcionamiento fuera de línea, la captura de datos biométrica se deberá realizar mediante una versión “stand-alone” del SEDIP, que el proveedor deberá implementar, conforme la sección de requerimientos funcionales.  La tabla a continuación especifica la cantidad de kits de captura móvil que deberán ser provistos.   |  |  | | --- | --- | | **ENTIDAD** | **CANTIDAD DE KITS MOVILES DE CAPTURA** | | DIGERCIC | 60 | | MREMH | 10 | | **Total** | **70** |   La siguiente tabla indica los tipos de equipos y rol que deben cumplir en la estación móvil. El proveedor puede proponer variantes equipos y accesorios o añadir otros mientras sirvan para el propósito de la captura de datos de forma fácil, rápida y segura.     |  |  |  |  | | --- | --- | --- | --- | | **Nro**. | **EQUIPO** | **CANTIDAD** | **ROL** | | 1 | COMPUTADOR PORTATIL “LAPTOP” | 1 | Acceso al SURI, SEDIP, software utilitario (email, ofimática) y conexión/control de equipos del kit | | 2 | ESCANER DE HUELLAS UNIDACTILAR | 1 | Captura de huella dactilar para autenticación del operador en el SEDIP. | | 2 | ESCANER DE HUELLAS DECADACTILAR | 1 | Captura de hasta 10 huellas dactilares del solicitante para validación biométrica de la identidad | | 4 | CAMARA FOTOGRAFICA DIGITAL, TRIPODE Y TELON DE FONDO | 1 | Captura de foto del rostro del solicitante (conforme OACI) para validación biométrica de la identidad | | 5 | TABLETA DIGITALIZADORA DE FIRMAS MANUSCRITAS | 1 | Captura de firma manuscrita del solicitante con lápiz digital para posterior impresión en los documentos | | 7 | ESCANER PORTÁTIL DE DOCUMENTOS | 1 | Captura de documentos de soporte de la solicitud de documentos; y captura de firmas manuscritas desde papel para posterior impresión en los documentos. | | 8 | IMPRESORA PORTÁTIL | 1 | Para imprimir comprobante de solicitudes, de pagos, otros | | 9 | MALETA PARA TRANSPORTE Y ACCESORIOS | 1 | Para almacenamiento, traslado y operación segura de los equipos. | | 10 | CONTENEDOR DE TELÓN Y TRÍPODE DE TELÓN | 1 | Para almacenamiento y traslado del telón y su respectivo trípode. | | 11 | KIT DE LIMPIEZA | 1 | Para limpieza de los equipos, accesorios y maleta. |   Las especificaciones técnicas mínimas de los equipos de los kits móviles de captura se encuentran en el Anexo E. Los equipos deberán ser nuevos de fábrica, no re-manufacturados y fabricados el año que sean entregados a la DIGERCIC. La maleta de transporte deberá ser liviana pero resistente a diversas variables (por ejemplo: agua, polvo, fuego, humedad, caída, golpes, etc.), es decir, condiciones extremas de uso. Adicionalmente, deberá permitir el embalaje seguro de los equipos para transporte por diversos medios. El montaje y desmontaje de la estación móvil deberá ser fácil y el uso ergonómico para evitar molestias al operador y a los ciudadanos. Inclusive el peso de los equipos incluidos deberá ser apropiado para el transporte manual, cuando las condiciones de trabajo así lo requieran.  Debido a la normativa legal ecuatoriana, el sistema operativo de la laptop del kit podrá ser preferencia libre open source (ej., Linux); o privativo (ej., de Microsoft) en sus versiones recientes. Los controladores (drivers) y kits de desarrollo de software de los equipos periféricos deberán ser compatibles con el sistema operativo que se proporcione. El proveedor deberá proveer las licencias o suscripciones de software respectivas para el sistema operativo y los programas de software que se solicitan. Todas las licencias o suscripciones deberán estar a nombre de la DIGERCIC.  El oferente deberá proveer e instalar software antivirus en las laptops de los kits móviles de captura, así como las suscripciones o licencias respectivas para cada laptop del kit; y para la consola centralizada de administración del software antivirus.  El proveedor deberá implementar una herramienta o funcionalidad para controlar y garantizar que solo equipos inventariados y autorizados puedan acceder y utilizar el SEDIP para la funcionalidad de captura de datos.  El oferente deberá proveer e instalar en cada PC del kit una herramienta de seguridad de punto final (endpoint security tool) que tenga la característica para prevenir la fuga de datos (data loss prevention) así como protección contra spam/virus, bloqueo de actividad maliciosa, control de navegación Web  Ese software particularmente deberá permitir controlar los puertos de entrada-salida (ej., USB), dispositivo de lectura/escritura de CD/DVD, puertos infrarrojos, bluetooth, Wifi, RJ45, para evitar la copia/transmisión de información no autorizada. El oferente deberá facilitará las suscripciones o licencias respectivas para cada laptop del kit de captura; así como para la consola centralizada de administración del software de seguridad de punto final.  El oferente deberá proveer e instalar software monitoreo y administración remota de laptop, cuando el kit esté conectado en-línea al SEDIP. El oferente deberá facilitar las suscripciones o licencias respectivas para cada laptop de los kits de captura; así como para la consola centralizada de administración del software de monitoreo y administración.  La DIGERCIC podrá instalar o facilitar el acceso a herramientas de software y/o sistemas/aplicaciones informáticas en las laptops de los kits, siempre que sea compatible con el hardware y software base de las mismas. El software a instalar por parte de la DIGERCIC consistirá al menos de: cliente de email, herramienta de ofimática, lector de archivos PDF, cliente de control remoto de la PC, navegadores Web (browsers): Mozilla Firefox, Google Chrome y Microsoft Internet Explorer, manejador de impresora de red.  La garantía técnica de los equipos y la vigencia de las licencias o suscripciones de software con mantenimiento/actualización incluidos deberá ser de al menos 3 años. La vigencia del soporte y mantenimiento/actualización de licencias suscripciones regirá partir de la fecha de la entrada en producción del SEDIP y así aceptado por la DIGERCIC mediante acta de entrega-recepción.  Durante la vigencia del soporte y mantenimiento/actualización se deberá realizar mantenimientos preventivos con frecuencia semestral para garantizar la operatividad de los kits móviles de captura. Para mantenimientos correctivos se deberá aplicar la garantía técnica solicitada. El cambio de equipos, piezas y accesorios de los kits móviles deberá estar contemplado como parte de los mantenimientos preventivos y correctivos sin costo adicional para la DIGERCIC.   * **Pruebas los de kits móviles de captura**   El proveedor deberá entregar todos los kits móviles de captura en la bodega de la DIGERCIC. El proveedor deberá proponer un plan y cronograma de pruebas de funcionamiento de todos los kits móviles de captura para aprobación de la DIGERCIC. El plan deberá considerar la capacitación al personal operativo que designe la DIGERCIC para operación de los kits; la preparación de cada móvil, y el entrenamiento al personal técnico que la DIGERIC delegue para la instalación, configuración, pruebas, puesta en operación, seguridad y soporte de primer nivel de los equipos y software de los kits de captura. Se deberá entregar la documentación técnica y de usuario respectiva, así como manuales, drivers, y cualquier ítem necesario para el entrenamiento del personal designado.  El proveedor deberá retirar los kits móviles de la bodega en coordinación con la DIGERCIC conforme el plan aprobado. A continuación, deberá preparar, configurar y probar los kits móviles para que puedan ser utilizados para captura de datos en línea en línea y fuera de línea. El proveedor deberá elaborar un informe de las pruebas de funcionamiento de cada móvil; y anexará una ficha técnica de cada móvil especificando los datos de los equipos (ejemplos: números de serie, marcas, modelos, otros), y el registro fotográfico de cada móvil. Posteriormente, deberá devolver los kits móviles a la bodega central de la DIGERCIC.   * **Pruebas de emisión de documentos con datos capturados con kits móviles**   El proveedor deberá implementar un piloto de captura de datos con kits móviles para para emisión de documentos de identidad y de pasaportes electrónicos de prueba. El piloto deberá implementarse en la ciudad de Quito para capturar y emitir al menos 30 solicitudes de documentos de identidad y 20 de pasaportes –de prueba- respectivamente. Esta cantidad podrá ser cambiada por la DIGERCIC previo aviso al proveedor.  Las pruebas de captura deberán ser realizadas en modalidad en-línea y en modalidad fuera de-línea. En el primer caso, las pruebas de captura y emisión se realizarán con kits móviles conectados al SEDIP mediante la Internet y estableciendo un canal cifrado con un cliente de VPN instalado y configurado en la laptop del kit. Los documentos a imprimir deberán ser enviados a los centros de producción de documentos de identidad y pasaportes implementados en la agencia matriz de la DIGERCIC en la ciudad de Quito. Se deberá utilizar hasta 10 móviles en línea para captura los datos para emisión de los documentos de identidad y pasaportes.  En el segundo caso, las pruebas de captura se realizarán fuera de línea, registrando los datos demográficos y biométricos utilizando la aplicación “stand-alone”, que deberá implementada por el proveedor e instalada previamente en la laptop del kit de captura. Posteriormente, las solicitudes de documentos de identidad y pasaportes deberán ser exportadas de forma segura al SEDIP para las validaciones y procesamiento respectivo.  El proveedor deberá asegurar que para la emisión de documentos de identidad y pasaportes -de prueba- el operador siga el procedimiento definido en los requerimientos funcionales. Esto comprende desde la generación de una solicitud de documentos en el SURI (modalidad en-línea) o aplicación (“stand-alone”) modulo fuera de línea hasta la producción y aseguramiento de la calidad del documento en el centro de producción, previo a la entrega.  El proveedor deberá elaborar un informe de la ejecución de la emisión de documentos de identidad y pasaportes -de prueba- al finalizar el mismo. Deberá anexar los documentos de identidad y pasaportes –de prueba- emitidos. |  |  |

# TRANSFERENCIA DE CONOCIMIENTOS Y ENTRENAMIENTO

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| Para asegurar la transferencia de conocimientos y entrenamiento al personal de la DIGERCIC y del MREMH respecto de la administración y uso del SEDIP, el Proveedor deberá presentar, dentro de los 15 días laborables a partir de la firma del contrato, un plan de transferencia de conocimientos y entrenamiento en el que conste la metodología, el temario, los tiempos, hojas de vida de los instructores, equipos, material didáctico, lugares, fechas y horas en la que se realizará. El plan de transferencia de conocimientos y entrenamiento será aprobado por la DIGERCIC. Los lugares y la logística de los eventos de entrenamiento deberán ser proporcionados por el Proveedor y aprobados por la DIGERCIC. Si amerita, el Administrador del contrato podrá solicitar que la transferencia de conocimientos y entrenamiento se ejecuten en las instalaciones de la DIGERCIC.  El Proveedor deberá realizar eventos de transferencia de conocimientos y entrenamiento en los siguientes ámbitos:   * **TÉCNICO INFORMÁTICO**   El Proveedor deberá realizar transferencia de conocimientos y entrenamiento al personal técnico de TIC que la DIGERCIC designe. Los eventos deberán asegurar que el personal adquiera todos los conocimientos necesarios y suficientes para administrar y monitorear el funcionamiento de los sistemas y los componentes de hardware suministrados. De igual forma, la transferencia de conocimientos deberá asegurar que el personal de la DIGERCIC y/o del MREMH esté en capacidad de analizar y resolver incidentes, problemas o errores de nivel 1 y 2 de los componentes de hardware o software de los sistemas suministrados; o en su defecto escalar al proveedor con la información que este requiera para solucionar los mismos. Adicionalmente, la transferencia de conocimientos, deberá reducir la dependencia del proveedor en cuanto a la administración, monitoreo, operación y gestión de soporte de los componentes de hardware y software suministrados.  El proveedor deberá preparar y entregar los contenidos y el material didáctico y de capacitación para los asistentes. El material didáctico, deberá tener un enfoque práctico, para que los asistentes prueben los conocimientos adquiridos.  Se deberá facilitar eventos de transferencia de conocimientos técnicos en al menos los siguientes temas:   * Arquitectura física y lógica detallada del sistema y los componentes de hardware y software, con una duración de 30 horas. * Administración y monitoreo del SEDIP y sus componentes de hardware y software, con una duración de 30 horas. * Administración y monitoreo del ABIS y sus componentes de hardware y software, con una duración de 30 horas. * Administración y monitoreo de la PKI y sus componentes de hardware y software, con una duración de 30 horas. * Gestión de respaldos y restauración a/desde disco; y a/desde cintas LTO, con una duración de 15 horas. * Gestión de switch-over y fail-over del sistema y sus componentes al centro de datos de contingencia, con una duración de 15 horas. * Administración y monitoreo del sistema de servicios Web 1 a 1 y 1 a n, con una duración de al menos 18 horas. * Desarrollo de clientes o interfaces para invocación de los servicios Web 1 a 1 desde otros sistemas, con una duración de al menos 18 horas. * Administración y monitoreo del sistema de monitoreo, con una duración de al menos 18 horas. * Administración y monitoreo del sistema de gestión de eventos de seguridad de la información (SIEM), con una duración de al menos 18 horas. * Administración y monitoreo del software antivirus, con una duración de al menos 15 horas. * Administración y monitoreo del sistema de protección de punto final * Instalación, configuración, administración y monitoreo del ambiente de pruebas, con una duración de al menos 18 horas. * Gestión y escalamiento de incidentes, problemas o errores del SEDIP, con una duración de al menos 12 horas. * Gestión de seguridad informática del sistema, con una duración de al menos 18 horas. * Revisión del código fuente que se entregue a la DIGERCIC, con una duración de al menos 18 horas. * Instalación, configuración, puesta en operación y mantenimiento básico a los componentes de los kits de captura de datos, producción y entrega de documentos de identidad y pasaportes, con una duración de al menos 48 horas que podrán distribuirse en uno o más eventos. * Mantenimiento básico de impresoras de documentos de identidad, con una duración de al menos 24 horas que podrán distribuirse en uno o más eventos. * Mantenimiento básico de impresoras de pasaportes, con una duración de al menos 24 horas que podrán distribuirse en uno o más eventos. * **OPERATIVO**   El Proveedor deberá realizar transferencia de conocimientos y entrenamiento orientados al ámbito operativo (operadores de captura, operadores centros de producción y operadores de entrega). El entrenamiento operativo deberá asegurar la prestación de los servicios de emisión de documentos de identidad y de pasaportes a los ciudadanos, a través del SEDIP y garantizar el uso correcto del sistema y los equipos suministrados. La capacitación operativa se proporcionará a personal clave designado por la DIGERCIC para que a su vez capaciten a todo el personal operativo (modalidad entrenamiento para entrenadores).  El proveedor deberá preparar y entregar los contenidos y el material didáctico y de capacitación para los asistentes. El material didáctico, deberá tener un enfoque práctico, para que los asistentes prueben los conocimientos adquiridos. Para la capacitación operativa deberá prepararse manuales para los entrenadores y para el operador.  Se deberá facilitar eventos de transferencia de conocimientos operativos en al menos los siguientes temas:   * Funcionalidades y uso del sistema SEDIP (captura, producción y entrega), con una duración de al menos 40 horas. * Funcionalidades y uso del sistema de análisis biométricos para posibles casos de suplantación o duplicidad de identidad detectados por el ABIS, con una duración de al menos 24 horas. * Operación de las impresoras de documentos de identidad, con una duración de al menos12 horas, que podrán distribuirse en uno o más eventos. * Operación de las impresoras de pasaportes, con una duración de al menos12 horas, que podrán distribuirse en uno o más eventos.   La transferencia de conocimientos y entrenamiento en el ámbito operativo se la realizará a servidores públicos de la DIGERCIC y el MREMH, líderes o usuarios claves en la prestación de los servicios de emisión de documentos de identidad y pasaportes, quienes deberán replicar los conocimientos adquiridos al personal pertinente de la DIGERCIC y del MREMH en modalidad de cascada. La DIGERCIC entregará al Proveedor el listado de las personas a capacitar (representantes de las diferentes Zonas de la DIGERCIC y representantes del MREMH).  El proveedor deberá incluir en su propuesta, el calendario sugerido de los eventos de capacitación en los ámbitos técnico y operativo. Para esto deberá considerar los hitos de implementación del sistema de forma que el personal este entrenado previamente, a la puesta en operación del sistema para la emisión de pasaportes y posteriormente de documentos de identidad. La DIGERCIC deberá revisar, ajustar y aprobar el calendario de capacitación con al menos 1 mes de anticipación del inicio del cronograma. Esto con el objeto de coordinar el personal y la logística necesaria.  El proveedor podrá incluir en su propuesta, temas adicionales o combinar los temas antes mencionados siempre que garantice la plena transferencia de conocimiento al personal designado.  La DIGERCIC podrá facilitar al proveedor un espacio físico para implementar una sala de capacitación con estaciones de captura, producción y entrega de documentos para las prácticas del caso. En ese, caso las estaciones deberán integradas al sistema de pruebas solicitado. De igual forma, la DIGERCIC podrá entregar un set limitado de tarjetas y libretas en blanco de muestras para las prácticas del entrenamiento operativo.  El Proveedor, una vez finalizada cada evento de transferencia de conocimientos y entrenamiento, deberá entregar, hasta los 15 días calendarios posteriores:   * Un certificado de asistencia y aprobación a cada participante. * Un informe de la transferencia de conocimientos y entrenamiento proporcionado (deberá incluir una copia: material didáctico, certificados entregados a los participantes, lista de participantes con la constancia de asistencia inicio-fin, registro fotográfico de cada evento). |  |  |

# SERVICIOS POST-IMPLEMENTACION

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El proveedor deberá proporcionar los siguientes servicios a partir de la puesta en operación del SEDIP. Los servicios se aplicarán a los equipos y programas implementados en los puntos de atención en el país y el extranjero, y en los centros de cómputo de la DIGERCIC. Los servicios requeridos son:   * Mantenimiento preventivo de hardware y software * Mantenimiento correctivo de hardware y software * Soporte técnico especializado * Gestión de incidentes y problemas * Actualización tecnológica del sistema * Gestión del cambio del sistema   La descripción de cada servicio, así como las condiciones de prestación de los mismos constan en el Anexo F. |  |  |

# PRODUCTOS MINIMOS ESPERADOS

La tabla a continuación resume los productos o entregables mínimos del contrato conforme el alcance y especificaciones técnicas antes expuestas. La recepción se plantea por lotes y no existe un orden establecido. Dependerá del proveedor el orden de entrega de acuerdo al cronograma, plan de trabajo y metodología que proponga. Todos los servicios y bienes que facilite el proveedor deberán generar un producto que deje constancia del suministro (ej., informe y anexos).

|  |  |  |
| --- | --- | --- |
| **LOTE** | **CANTIDAD** | **DESCRIPCION** |
| 1 | 1 | **SISTEMA DE EMISION DE DOCUMENTOS DE IDENTIDAD Y PASAPORTES (SEDIP) EN OPERACIÓN EN LA DIGERCIC** |
| HARDWARE EN ALTA DISPONIBLIDAD EN CENTRO DE DATOS PRINCIPAL Y DE CONTINGENCIA EN CENTRO DE DATOS SECUDARIO EN OPERACIÓN |
| SUSCRIPCIONES Y/0 LICENCIAS DEL SOFTWARE BASE, DEL SEDIP, FIREWALL DE BASE DE DATOS Y ENCRIPTACION DE LA BASE DE DATOS |
| DOCUMENTACION OPERATIVA/USUARIOS Y TECNICA RECIBIDA |
| CODIGO FUENTE Y DOCUMENTACION DEL SOFTWARE O DE COMPONENTES IMPLEMENTADOS PARA LA DIGERCIC |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| INFORMES Y MANUALES TECNICOS DE LAS INTERFACES DE INTEGRACION IMPLEMENTADAS |
| AMBIENTE DE PRUEBAS DEL SEDIP EN OPERACIÓN |
| CODIGO FUENTE Y DOCUMENTACION DEL SOFTWARE PARA ENROLAMIENTO FUERA DE LINEA CON EQUIPOS MOVILES |
| 2 | 1 | **SISTEMA DE IDENTIFICACION BIOMETRICA AUTOMATIZADO (ABIS) EN OPERACIÓN EN LA DIGERCIC** |
| HARDWARE EN ALTA DISPONIBLIDAD EN CENTRO DE DATOS PRINCIPAL Y DE CONTINGENCIA EN CENTRO DE DATOS SECUDARIO EN OPERACIÓN |
| SUSCRIPCIONES Y/0 LICENCIAS DEL SOFTWARE BASE RECIBIDAS |
| LICENCIAS PARA 16’000.000 MILLONES DE REGISTRO BIOMETRICOS DE HUELLAS DECADACTILARES Y ROSTROS |
| BASE DE DATOS DE HUELLAS Y ROSTROS CARGADAS AL ABIS |
| SISTEMA DE SW PARA CONSULTAS 1 A 1 Y 1 A N EN OPERACIÓN |
| ABIS Y AFIS (ACTUALMENTE EN OPERACIÓN) SINCRONIZADOS |
| DOCUMENTACION OPERATIVA/USUARIOS Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| CODIGO FUENTE Y DOCUMENTACION DE LOS SERVICIOS WEB PARA CONSULTAS 1 A 1 Y 1 A N IMPLEMENTADOS Y DE LA APLICACIÓN WEB DE CONSUMO |
| AMBIENTE DE PRUEBAS DEL ABIS EN OPERACIÓN |
| 3 | 1 | **INFRESTRUCTURA DE CLAVE PUBLICA OACI BAC/SAC EN OPERACIÓN EN LA DIGERCIC** |
| HARDWARE DE LA PKI Y PKD NACIONAL EN ALTA DISPONIBLIDAD EN CENTRO DE DATOS PRINCIPAL Y DE CONTINGENCIA EN CENTRO DE DATOS SECUDARIO EN OPERACIÓN |
| SET DE HSMs PARA DESBLOQUEO DE CHIPS DE TARJETAS Y LIBRETAS EN BLANCO PARA CENTROS DE COMPUTO PRINCIPAL EN ALTA DISPONIBLIDAD Y DE CONTINGENCIA EN OPERACIÓN |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE BASE Y DE LA PKI RECIBIDAS |
| CEREMONIA DE CLAVES Y PROCEDIMIENTOS DE CEREMONIAS DE CLAVES Y PARA LA ADMINISTRACION DE LA PKI, PKD NACIONAL E INTEGRACION CON LA PKI DE LA OACI. |
| PKD NACIONAL EN OPERACIO E INTEGRADA A LA PKD DE LA OACI |
| FIRMANTES DE DOCUMENTOS DE IDENTIDAD Y DE PASAPORTES EN OPERACIÓN |
| DOCUMENTACION OPERATIVA/USUARIOS Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| AMBIENTE DE PRUEBAS DE LA PKI EN OPERACIÓN |
| 4 | 1 | **SISTEMA DE MONITOREO Y SEGURIDAD DEL SISTEMA DE EMISION EN OPERACIÓN EN LA DIGERCIC** |
| 4 MONITORES WALL-PANEL MINIMO; 3 ESTACIONES DE MONITOREO MINIMO RECIBIDOS Y EN OPERACIÓN |
| SUSCRIPCIONES Y/0 LICENCIAS DEL SOFTWARE BASE RECIBIDAS |
| SUSCRIPCIONES Y/0 LICENCIAS DEL SOFTWARE DE MONITOREO, DE GESTION DE EVENTOS DE SEGURIDAD DE INFORMACION (SIEM), ANTIVIRUS, DE SEGURIDAD DE PUNTO FINAL RECIBIDAS. |
| DOCUMENTACION OPERATIVA Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION RECIBIDA |
| 5 | 635 | **KITS FIJOS DE CAPTURA DE DATOS** |
| EQUIPOS Y ACCESORIOS EN OPERACIÓN EN AGENCIAS DE LA DIGERCIC Y OFICINAS DE QUITO, NUEVA YORK Y MADRID DEL MREMH. |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE BASE |
| DOCUMENTACION OPERATIVA/USUARIOS Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| 6 | 88 | **KITS COMPLETOS DE ENTREGA DE DOCUMENTOS** |
| EQUIPOS Y ACCESORIOS EN OPERACIÓN EN AGENCIAS DE LA DIGERCIC Y OFICINAS DE QUITO, NUEVA YORK Y MADRID DEL MREMH. |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE BASE Y UTILITARIO RECIBIDAS |
| DOCUMENTACION OPERATIVA Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| 7 | 290 | **KITS PARCIALES DE ENTREGA DE DOCUMENTOS** |
| EQUIPOS Y ACCESORIOS EN OPERACIÓN EN AGENCIAS DE LA DIGERCIC Y OFICINAS DE QUITO, NUEVA YORK Y MADRID DEL MREMH. |
| DOCUMENTACION OPERATIVA Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| 8 | 70 | **KITS MOVILES DE CAPTURA DE DATOS** |
| EQUIPOS Y ACCESORIOS RECIBIDOS |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE BASE Y UTILITARIO RECIBIDAS |
| DOCUMENTACION OPERATIVA Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| 9 | 13 | **KITS DE PRODUCCION DE PASAPORTES** |
| EQUIPOS Y ACCESORIOS EN OPERACIÓN EN AGENCIAS DE LA DIGERCIC Y OFICINAS DE QUITO, NUEVA YORK Y MADRID DEL MREMH. |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE BASE RECIBIDAS |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE DE MONITOREO DE LAS IMPRESORAS RECIBIDAS |
| INSUMOS PARA IMPRESIÓN DE MINIMO 1’000.000 DE PASAPORTES |
| DOCUMENTACION OPERATIVA Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| 10 | 4 | **EQUIPOS PARA CONEXIÓN DE AGENCIAS REMOTAS EN OPERACIÓN** |
| EQUIPOS Y ACCESORIOS EN OPERACIÓN EN OFICINAS DE NUEVA YORK Y MADRID DEL MREMH. |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE BASE RECIBIDAS |
| DOCUMENTACION OPERATIVA Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| 11 | 67 | **KITS DE PRODUCCION DE DOCUMENTOS DE IDENTIDAD** |
| EQUIPOS Y ACCESORIOS EN OPERACIÓN EN AGENCIAS DE LA DIGERCIC. |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE BASE RECIBIDAS |
| SUSCRIPCIONES Y/0 LICENCIAS DE SOFTWARE DE MONITOREO DE LAS IMPRESORAS RECIBIDAS |
| DOCUMENTACION OPERATIVA Y TECNICA RECIBIDA |
| INFORMES Y MANUALES DE ENTRENAMIENTO/CAPACITACION FACILITADA |
| 12 | 1 | **DOCUMENTACION DE GESTION DEL PROYECTO RECIBIDA** |
| PLAN, CRONOGRAMA Y METODOLOGIA DE TRABAJO |
| DOCUMENTACION DEL DISEÑO / ARQUITECTURA LOGICO Y FISICO DETALLADO DEL SEDIP Y SUS COMPONENTES |
| DOCUMENTACION DEL DISEÑO / ARQUITECTURA LOGICO Y FISICO DE LA INTEGRACION DEL SEDIP A LOS SISTEMAS INTERNOS DE LA DIGERCIC |
| DOCUMENTACION DE IMPLEMENTACION / PRUEBAS / AJUSTES / PASO A PRODUCCION DEL SISTEMA Y SUS COMPONENTES |
| LISTA DE MATERIALES (BOM) DE HARDWARE Y SOFTWARE DETALLADOS RECIBIDOS |
| PLANES DE PRUEBAS, CAPACITACION, DESPLIEGUE RECIBIDOS |
| INFORMES DE AVANCE Y FIN RECIBIDOS |
| GARANTIAS TECNICAS POR 3 AÑOS DEL HARDWARE Y SOFTWARE RECIBIDOS |
| PROCEDIMIENTOS PARA MANTENIMIENTO, SOPORTE Y GESTION DE INCIDENTES RECIBIDOS |
|  | PLAN DE MANTENIMIENTOS PREVENTIVOS PARA EQUIPAMIENTO DE AGENCIAS Y CONSULADOS |
| PROCEDIMIENTOS PARA RESPALDO/RESTAURACION DE INFORMACION; DE SWITCH-OVER Y DE FAIL-OVER DE LOS SISTEMAS |
| PLAN DE MANTENIMIENTOS PREVENTIVOS PARA EQUIPAMIENTO DE CENTROS DE COMPUTO |
|  |  | DOCUMENTACION OPERATIVA Y TECNICA DEL SISTEMA DE PRUEBAS IMPLEMENTADO (SEDIP, ABIS, PKI) |
|  |  | INFORMES DE LOS PILOTOS DE PRUEBA DE EMISION DE DOCUMENTOS DE IDENTIDAD Y PASAPORTES |
|  |  | INFORMES DE DESPLIEGUE DEL EQUIPAMIENTO Y SOFTWARE EN LOS CENTROS DE COMPUTO |
|  |  | INFORMES DE DESPLIEGUE DEL EQUIPAMIENTO Y SOFTWARE EN LAS AGENCIAS DE LA DIGERCIC Y CONSULADOS DE NUEVA YORK Y MADRID PARA EMISION DE PASAPORTES Y DOCUMENTOS DE IDENTIDAD |
|  |  | INFORMES DE LOS EVENTOS DE ENTRENAMIENTO OPERATIVO Y TECNICO |
|  |  | DOCUMENTACION ADICIONAL REFERIDA EN LOS TDR O ADICIONAL QUE SEA ASI CONSIDERADA POR LA DIGERCIC |

# ENTREGA DE LOS BIENES

Los bienes a ser suministrados deberán ser entregados por el proveedor en la Bodega de la DIGERCIC de la ciudad de Quito ubicada en las calles Jorge Drom y Unión Nacional de Periodistas.

# PLAZO

El plazo total que se otorga para la ejecución del contrato será de 48 meses calendario. Este plazo se contará a partir del día siguiente laborable de la firma del contrato.

El plazo intermedio fijado para la recepción del SEDIP completo y a plena satisfacción de la DIGERCIC es de 12 meses. A partir de la recepción completa del sistema correrá el plazo de 36 de mantenimiento, soporte, gestión de incidentes y problemas, actualización tecnológica y gestión del cambio del sistema.

# EXPERIENCIA GENERAL Y ESPECÍFICA DEL OFERENTE

Considerando la importancia del proyecto para el estado ecuatoriano, la necesidad de que se cumpla el objeto contractual a cabalidad, con conocimiento y experticia; y con el objeto de asegurar la prestación de los servicios de emisión de documentos de identidad y pasaportes electrónicos a los ciudadanos, la DIGERCIC establece los requerimientos de experiencia general y específica para los oferentes en los niveles más altos permitidos por la normativa vigente (Resoluciones emitidas por el Servicio de Compras Públicas No. RE.-SERCOP-2017-0000078 y No. RE.-SERCOP-2017-0000081 de 23 de mayo de 2017 y 06 de octubre de 2017 respectivamente):

|  |  |  |
| --- | --- | --- |
| **EXPERIENCIA GENERAL DEL OFERENTE** | | |
| **NO.** | **DESCRIPCIÓN** | **VALOR DEL MONTO MÍNIMO** |
| 1 | Copias de certificados o actas de entrega-recepción de contratos suscritos por la contratista y debidamente legalizados, ejecutados en los últimos quince (15) años (Tomando como referencia la fecha de publicación del proceso), que contemplen el diseño e implementación de sistemas automatizados de identificación biométrica (ABIS), sistemas de infraestructura de claves públicas (PKI), sistemas de emisión de documentos en general (ej., identidad, pasaportes, licencias de conducir, tarjetas de crédito, carnets de salud, otros); así como la implementación de sistemas informáticos de misión crítica tales como ERPs, CRMs, IVRs, otros.  Si el proveedor forma parte de una asociación o consorcio, se tomará el 100% del valor de la experiencia de la asociación o consorcio, independientemente de su grado de participación accionaria en el mismo. | El monto deberá ser igual o mayor a: **US$24’860.000,00**  **(VEINTE Y CUATRO MILLONES OCHOCIENTOS SESENTA MIL DOLARES DE ESTADOS UNIDOS DE AMÉRICA CON 00/100** |
| 2 | El monto de cada contrato para certificar la experiencia general no podrá ser inferior a: | **US$2’486.000,00**  **(DOS MILLONES CUATROCIENTOS OCHENTA Y SEIS MIL DOLARES DE ESTADOS UNIDOS DE AMÉRICA CON 00/100)** |

|  |  |  |
| --- | --- | --- |
| **EXPERIENCIA ESPECÍFICA DEL OFERENTE** | | |
| **No.** | **DESCRIPCIÓN** | **VALOR DEL MONTO MÍNIMO** |
| 1 | Copias de certificados o actas de entrega-recepción de contratos suscritos por la contratista y debidamente legalizados, durante los últimos 10 años (Tomando como referencia la fecha de publicación del proceso), en los cuales haya implementado un sistema informático para emisión de documentos de identidad electrónicos y/o un sistema informático para emisión de pasaportes electrónicos, en los que se especifique que el sistema incluyó un Sistema Automatizado de Identificación Biométrica (ABIS, por sus siglas en inglés) y un Sistema de Infraestructura de Clave pública (PKI, por sus siglas en inglés), además de equipamiento y software para captura de información demográfica y biométrica, codificación electrónica e impresión de documentos de identidad y pasaportes electrónicos (conforme recomendaciones del Doc. 9303 de la OACI).  Si el proveedor forma parte de una asociación o consorcio, se tomará el 100% del valor de la experiencia de la asociación o consorcio, independientemente de su grado de participación accionaria en el mismo. | El monto deberá ser igual o mayor a: **US$19’890.000,00 (DIECINUEVE MILLONES OCHOCIENTOS NOVENTA MIL DOLARES DE ESTADOS UNIDOS DE AMÉRICA CON 00/100)** |
| 2 | El monto de cada contrato para certificar la experiencia específica no podrá ser inferior a: | **US$1’989.000,00 (UN MILLÓN NOVECIENTOS OCHENTA Y NUEVE MIL DOLARES DE ESTADOS UNIDOS DE AMÉRICA CON 00/100)** |

# PERSONAL TÉCNICO MÍNIMO

El oferente para garantizar el cumplimiento del objeto contractual dentro del plazo estipulado deberá contar con el siguiente equipo técnico mínimo para la ejecución de los trabajos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PERSONAL TÉCNICO MÍNIMO** | | | | |
| **ÍTEM.** | **FUNCIÓN** | **NIVEL DE ESTUDIO** | **TITULACIÓN ACADÉMICA** | **CANTIDAD** |
| 1 | Gerente de proyecto | Tercer nivel o superior con título | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes, Mgs. Dirección de Proyectos o Carreras Afines InProyectoCarreras Afines. | 1 |
| 2 | Gerente técnico | Tercer nivel o superior con título | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |
| 3 | Arquitecto de sistemas | Tercer nivel o superior con título | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |
| 4 | Desarrollador de software | Tercer nivel o superior con título | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |
| 5 | Especialista de implementación de ABIS | Tercer nivel o superior con título. | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |
| 6 | Especialista de implementación de PKI | Tercer nivel o superior con título. | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |
| 7 | Especialista de infraestructura informática  (hardware / networking / centros de datos) | Tercer nivel o superior con título. | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |
| 8 | Especialista de base de datos | Tercer nivel o superior con título. | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |
| 9 | Especialista de seguridad informática | Tercer nivel o superior con título. | Ing. Telecomunicaciones, Ing. Sistemas, Ing. Redes o Carreras Afines. | 1 |

Para la prestación del servicio, el personal técnico del Oferente deberá contar con al menos la siguiente experiencia:

|  |  |  |
| --- | --- | --- |
| **Nro.** | **CARGO** | **EXPERIENCIA MÍNIMA** |
| 1 | Gerente de proyecto | Al menos una (1) certificación vigente que acredite internacionalmente la preparación en temas relacionados a la Dirección o Gestión de Proyectos como PMP o su equivalente.  La experiencia requerida para el Gerente del proyecto es de haber participado como Gerente de Proyectos o Administrador de Proyectos de tecnología por un monto de al menos USD 5’000.000,00 (CINCO MILLONES DE DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos el USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA)  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 2 | Gerente técnico | Al menos una (1) certificación vigente que acredite internacionalmente la preparación en temas relacionados a la Dirección o Gestión de Proyectos como PMP o su equivalente.  La experiencia requerida para el Gerente Técnico del Proyecto es de haber participado como Gerente Técnico en la implementación de sistemas de emisión de documentos de identidad y/o pasaportes electrónicos en el sistema ofertado por un monto de al menos USD 5’000.000,00 (CINCO MILLONES DE DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos el USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA)  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 3 | Arquitecto de sistemas | La experiencia requerida para el Arquitecto de Sistemas del Proyecto es haber participado como arquitecto de sistemas en la implementación de sistemas informáticos por un monto de al menos USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos USD 50.000,00 (CINCUENTA MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA)  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 4 | Desarrollador de software | La experiencia requerida para el Desarrollador de software, es haber participado como desarrollador de software en la implementación de sistemas informáticos por un monto de al menos USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos USD 50.000,00 (CINCUENTA MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA)  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 5 | Especialista de implementación de ABIS | Al menos una (1) certificación vigente del fabricante del ABIS de la marca ofertada (Emitido en los últimos 5 años).  La experiencia requerida para el Especialista de Implementación de ABIS, es haber participado en la implementación de un sistema automatizado de identificación biométrica por un monto de al menos USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos USD 50.000,00 (CINCUENTA MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA)  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 6 | Especialista de implementación de PKI | Al menos una (1) certificación vigente del fabricante de la PKI de la marca ofertada (Emitida en los últimos 5 años).  La experiencia requerida para el Especialista de Implementación de PKI, es haber participado en la implementación de un sistema que incluya infraestructura de clave pública (PKI) por un monto de al menos USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos USD 50.000,00 (CINCUENTA MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA)  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 7 | Especialista de infraestructura informática  (hardware / networking / centros de datos) | Al menos una (1) certificación vigente que acredite la preparación en la infraestructura informática ofertada.  La experiencia requerida para el Especialista de infraestructura informática (hardware / networking / centros de datos) es haber participado en la implementación de hardware de la marca ofertada por un monto de al menos USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos USD 50.000,00 (CINCUENTA MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA).  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 8 | Especialista de base de datos | La experiencia requerida para el Especialista de base de datos) es haber participado como administrador de base de datos del sistema de emisión de documentos de identidad y/o pasaportes electrónicos ofertado por un monto de al menos USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos USD 50.000,00 (CINCUENTA MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA).  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |
| 9 | Especialista de seguridad informática | Al menos una (1) certificación vigente que acredite la preparación en la seguridad informática.  La experiencia requerida para el Especialista de seguridad informática es haber participado en la implementación de un proyecto que incluya seguridad informática por un monto de al menos USD 500.000,00 (QUINIENTOS MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). Se aceptaran certificados o documentos por un valor de al menos USD 50.000,00 (CINCUENTA MIL DOLARES DE LOS ESTADOS UNIDOS DE AMÉRICA).  En los certificados debe constar al menos la siguiente información: nombre de cliente, nombre del proyecto, fecha de ejecución, monto y país. |

Las cantidades de personal de trabajo son las mínimas. El proveedor estará obligado a incorporar el personal que sea necesario para desempeñar otros roles o para aumentar la cantidad de personal en los roles solicitados. Esto con el objeto de cumplir con los hitos y plazos especificados en el TdR.

Los títulos de tercer nivel o superior requeridos para cada uno de los profesionales constituyen el requisito mínimo a cumplir por parte del personal técnico en lo que corresponde a formación académica.

Los títulos de tercer nivel o superior obtenidos en el país deberán estar registrados en la Secretaría de Nacional de Educación Superior Ciencia y Tecnología. Se deberá presentar copia.

Los títulos de tercer nivel o superior obtenidos en el extranjero deberán estar registrados o reconocidos por las instancias correspondientes en el país de origen. Se deberá presentar copia.

# FORMA DE PAGO

La DIGERCIC pagará el contrato con fondos propios asignados en el presupuesto de la institución. El contrato se pagará de la siguiente forma:

* **Pago del anticipo**

Hasta los 15 días de la firma del contrato del contrato. El porcentaje del anticipo corresponderá al 15% (QUINCE POR CIENTO) del valor total del contrato a suscribir.

* **Pago 1**

A efectuarse previa presentación del acta de entrega-recepción del SEDIP completo y a satisfacción de la DIGERCIC, el informe favorable del administrador del contrato y la factura emitida por el proveedor. El pago corresponderá a los bienes (hardware y software) y los servicios suministrados.

* **Pagos 2 al 7**

A efectuarse semestralmente a partir de la fecha de la firma del acta de entrega-recepción del SEDIP completo y a satisfacción de la DIGERCIC; y previa presentación del acta de entrega-recepción, el informe favorable del administrador del contrato y la factura emitida por el proveedor. Esos pagos corresponderán a los servicios que efectivamente sean prestados o suministrados, conforme especifica la normativa legal ecuatoriana vigente.

# MULTAS

La DIGERCIC aplicará multas en 2 ámbitos: incumplimiento de plazos, e incumplimiento niveles de servicio en la gestión de incidentes del sistema atribuibles al proveedor. Para el primer caso los montos de las multas estarán en proporción de los pagos a realizar al proveedor; mientras que, para el segundo caso, los valores de las multas estarán en función del impacto económico del incidente en los servicios de emisión de documentos de identidad y pasaportes.

* **Multas por incumplimiento de plazos**
* Se aplicarán por cada día de incumplimiento de los plazos establecidos por la DIGERCIC para los hitos obligatorios de la sección “6 Metodología de Trabajo”.
* Se aplicarán por cada día incumplimiento de los plazos intermedios de las actividades del cronograma de trabajo presentado por el proveedor y aprobado por la DIGERCIC.
* Se aplicarán por cada día de atraso en la entrega de informes o documentos solicitados en los términos de referencia, que consten como entregables en el cronograma de trabajo presentado por el proveedor y aprobado por la DIGERCIC o como entregable de los servicios de post-implementación. Si un informe o documento no resultare aprobado por la DIGERCIC, se aplicará una multa hasta que el proveedor presente un informe que sea aprobado por la DIGERCIC.
* **Multas por incumplimiento de niveles de servicio**

Se contabilizarán por cada hora adicional o fracción que el proveedor emplee para resolver un incidente de los componentes de hardware y software del sistema que ocasionen indisponibilidad o degradación de los servicios de emisión de cédulas y/o pasaportes en las agencias de la DIGERCIC y en los consulados del MREMH. En el Anexo F constan los “Niveles de Servicio” que el proveedor deberá cumplir para evitar multas. El proveedor deberá gestionar los incidentes que afecten la capacidad, disponibilidad y rendimiento del SEDIP de forma minuciosa y rigurosa integrándose a la mesa de soporte de TIC de la DIGERCIC

# 13. ANEXOS

# A) AGENCIAS DE EMISION DE DOCUMENTOS DE IDENTIDAD DE LA DIGERCIC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **ZONA** | **PROVINCIA** | **CIUDAD** | **AGENCIA** |
| 1 | 9 | PICHINCHA | QUITO | MATRIZ - IÑAQUITO |
| 2 | 9 | PICHINCHA | QUITO | SAN BLAS (QUITO) |
| 3 | 9 | PICHINCHA | QUITO | QUITUMBE |
| 4 | 9 | PICHINCHA | RUMIÑAHUI | RUMIÑAHUI |
| 5 | 9 | PICHINCHA | CAYAMBE | CAYAMBE |
| 6 | 9 | PICHINCHA | MEJÍA | MEJÍA |
| 7 | 9 | PICHINCHA | QUITO | CALDERÓN |
| 8 | 9 | PICHINCHA | QUITO | EL QUINCHE |
| 9 | 9 | PICHINCHA | QUITO | POMASQUI |
| 10 | 9 | PICHINCHA | QUITO | TUMBACO |
| 11 | 9 | PICHINCHA | PEDRO MONCAYO | PEDRO MONCAYO |
| 12 | 9 | PICHINCHA | PUERTO QUITO | PUERTO QUITO |
| 13 | 9 | PICHINCHA | QUITO | LA ROLDOS |
| 14 | 9 | PICHINCHA | SAN MIGUEL DE LOS BANCOS | SAN MIGUEL DE LOS BANCOS |
| 15 | 9 | PICHINCHA | QUITO | PUELLARO |
| 16 | 8 | GUAYAS | GUAYAQUIL | CENTRO GYE / ROCAFUERTE |
| 17 | 8 | GUAYAS | GUAYAQUIL | NORTE GYE / TARQUI |
| 18 | 8 | GUAYAS | GUAYAQUIL | SUR GYE / XIMENA |
| 19 | 8 | GUAYAS | DURAN | DURÁN |
| 20 | 8 | GUAYAS | DAULE | DAULE |
| 21 | 8 | GUAYAS | GUAYAQUIL | GOBIERNO ZONAL |
| 22 | 8 | GUAYAS | BALZAR | BALZAR |
| 23 | 8 | GUAYAS | EMPALME | EMPALME |
| 24 | 8 | GUAYAS | EL TRIUNFO | EL TRIUNFO |
| 25 | 8 | GUAYAS | NARANJAL | NARANJAL |
| 26 | 8 | GUAYAS | PLAYAS | GENERAL VILLAMIL PLAYAS |
| 27 | 8 | GUAYAS | COLIMES | COLIMES |
| 28 | 8 | GUAYAS | NARANJITO | NARANJITO |
| 29 | 8 | GUAYAS | PEDRO CARBO | PEDRO CARBO |
| 30 | 8 | GUAYAS | SALITRE | SALITRE |
| 31 | 8 | GUAYAS | SAMBORONDON | SAMBORONDON |
| 32 | 8 | GUAYAS | ALFREDO MORENO | JUJAN |
| 33 | 8 | GUAYAS | YAGUACHI | YAGUACHI |
| 34 | 8 | GUAYAS | GUAYAQUIL | UVC CUARTEL MODELO |
| 35 | 7 | EL ORO | MACHALA | MACHALA |
| 36 | 7 | EL ORO | ARENILLAS | ARENILLAS |
| 37 | 7 | EL ORO | HUAQUILLAS | HUAQUILLAS |
| 38 | 7 | EL ORO | PASAJE | PASAJE |
| 39 | 7 | EL ORO | SANTA ROSA | SANTA ROSA |
| 40 | 7 | EL ORO | EL GUABO | EL GUABO |
| 41 | 7 | EL ORO | MARCABELI | MARCABELI |
| 42 | 7 | EL ORO | PIÑAS | PIÑAS |
| 43 | 7 | EL ORO | ZARUMA | ZARUMA |
| 44 | 7 | LOJA | LOJA | LOJA |
| 45 | 7 | LOJA | SARAGURO | SARAGURO |
| 46 | 7 | LOJA | CALVAS | CALVAS |
| 47 | 7 | LOJA | CATAMAYO | CATAMAYO |
| 48 | 7 | LOJA | CELICA | CELICA |
| 49 | 7 | LOJA | PALTAS | PALTAS |
| 50 | 7 | LOJA | ESPÍNDOLA | ESPÍNDOLA |
| 51 | 7 | LOJA | MACARA | MACARA |
| 52 | 7 | LOJA | ZAPOTILLO | ZAPOTILLO |
| 53 | 7 | ZAMORA CHINCHIPE | ZAMORA | ZAMORA |
| 54 | 7 | ZAMORA CHINCHIPE | YANTZAZA | YANTZAZA |
| 55 | 7 | ZAMORA CHINCHIPE | CHINCHIPE | CHINCHIPE |
| 56 | 7 | ZAMORA CHINCHIPE | EL PANGUI | EL PANGUI |
| 57 | 7 | ZAMORA CHINCHIPE | NANGARITZA | NANGARITZA |
| 58 | 7 | ZAMORA CHINCHIPE | YACUAMBI | YACUAMBI |
| 59 | 6 | AZUAY | CUENCA | SAN BLAS (CUENCA) |
| 60 | 6 | AZUAY | CUENCA | EL BATAN |
| 61 | 6 | AZUAY | GUALACEO | GUALACEO |
| 62 | 6 | AZUAY | GIRÓN | GIRÓN |
| 63 | 6 | AZUAY | PAUTE | PAUTE |
| 64 | 6 | AZUAY | CAMILO PONCE ENRÍQUEZ | CAMILO PONCE ENRÍQUEZ |
| 65 | 6 | AZUAY | NABON | NABON |
| 66 | 6 | AZUAY | OÑA | OÑA |
| 67 | 6 | AZUAY | PUCARA | PUCARA |
| 68 | 6 | AZUAY | SANTA ISABEL | SANTA ISABEL |
| 69 | 6 | AZUAY | SIGSIG | SIGSIG |
| 70 | 6 | CAÑAR | AZOGUES | AZOGUES |
| 71 | 6 | CAÑAR | CAÑAR | CAÑAR |
| 72 | 6 | CAÑAR | LA TRONCAL | LA TRONCAL |
| 73 | 6 | CAÑAR | SUSCAL | SUSCAL |
| 74 | 6 | MORONA SANTIAGO | MORONA | MACAS |
| 75 | 6 | MORONA SANTIAGO | SUCUA | SUCUA |
| 76 | 6 | MORONA SANTIAGO | GUALAQUIZA | GUALAQUIZA |
| 77 | 6 | MORONA SANTIAGO | PALORA | PALORA |
| 78 | 6 | MORONA SANTIAGO | LIMÓN INDANZA | LIMÓN INDANZA |
| 79 | 6 | MORONA SANTIAGO | SANTIAGO | SANTIAGO |
| 80 | 6 | MORONA SANTIAGO | TAISHA | TAISHA |
| 81 | 6 | MORONA SANTIAGO | TIWINTZA | TIWINTZA |
| 82 | 5 | GALÁPAGOS | ISABELA | ISABELA |
| 83 | 5 | GALÁPAGOS | SAN CRISTÓBAL | SAN CRISTÓBAL |
| 84 | 5 | GALÁPAGOS | SANTA CRUZ | SANTA CRUZ |
| 85 | 5 | GUAYAS | MILAGRO | MILAGRO |
| 86 | 5 | GUAYAS | PALENQUE | PALENQUE |
| 87 | 5 | LOS RÍOS | BABAHOYO | BABAHOYO |
| 88 | 5 | LOS RÍOS | QUEVEDO | QUEVEDO |
| 89 | 5 | LOS RÍOS | BUENA FE | SAN JACINTO DE BUENA FE |
| 90 | 5 | LOS RÍOS | PUEBLO VIEJO | PUEBLO VIEJO |
| 91 | 5 | LOS RÍOS | URDANETA | URDANETA |
| 92 | 5 | LOS RÍOS | VENTANAS | VENTANAS |
| 93 | 5 | LOS RÍOS | BABA | BABA |
| 94 | 5 | LOS RÍOS | MOCACHE | MOCACHE |
| 95 | 5 | LOS RÍOS | QUINSALOMA | QUINSALOMA |
| 96 | 5 | LOS RÍOS | VALENCIA | VALENCIA |
| 97 | 5 | LOS RÍOS | VINCES | VINCES |
| 98 | 5 | LOS RÍOS | MONTALVO | MONTALVO |
| 99 | 5 | SANTA ELENA | SALINAS | SALINAS |
| 100 | 5 | SANTA ELENA | SANTA ELENA | SANTA ELENA |
| 101 | 5 | SANTA ELENA | SANTA ELENA | COLONCHE |
| 102 | 5 | SANTA ELENA | SANTA ELENA | MANGLARALTO |
| 103 | 5 | SANTA ELENA | SANTA ELENA | CHANDUY |
| 104 | 4 | MANABÍ | CHONE | CHONE |
| 105 | 4 | MANABÍ | MANTA | MANTA |
| 106 | 4 | MANABÍ | PORTOVIEJO | PORTOVIEJO |
| 107 | 4 | MANABÍ | MONTECRISTI | MONTECRISTI |
| 108 | 4 | MANABÍ | PICHINCHA | PICHINCHA |
| 109 | 4 | MANABÍ | ROCAFUERTE | ROCAFUERTE |
| 110 | 4 | MANABÍ | SANTA ANA | SANTA ANA |
| 111 | 4 | MANABÍ | BOLÍVAR | BOLÍVAR |
| 112 | 4 | MANABÍ | EL CARMEN | EL CARMEN |
| 113 | 4 | MANABÍ | JIPIJAPA | JIPIJAPA |
| 114 | 4 | MANABÍ | PORTOVIEJO | CAC PORTOVIEJO |
| 115 | 4 | MANABÍ | PUERTO LÓPEZ | PUERTO LOPEZ |
| 116 | 4 | MANABÍ | PAJAN | PAJAN |
| 117 | 4 | MANABÍ | PEDERNALES | PEDERNALES |
| 118 | 4 | MANABÍ | SUCRE | SUCRE |
| 119 | 4 | MANABÍ | FLAVIO ALFARO | FLAVIO ALFARO |
| 120 | 4 | MANABÍ | JAMA | JAMA |
| 121 | 4 | MANABÍ | OLMEDO | OLMEDO |
| 122 | 4 | STO DOM. TSÁCHILAS | SANTO DOMINGO | SANTO DOMINGO |
| 123 | 4 | STO DOM. TSÁCHILAS | LA CONCORDIA | LA CONCORDIA |
| 124 | 3 | BOLIVAR | CHILLANES | SAN JOSE DEL TAMBO |
| 125 | 3 | BOLIVAR | LAS NAVES | LAS NAVES |
| 126 | 3 | BOLÍVAR | GUARANDA | GUARANDA |
| 127 | 3 | BOLÍVAR | CALUMA | CALUMA |
| 128 | 3 | BOLÍVAR | CHILLANES | CHILLANES |
| 129 | 3 | BOLÍVAR | ECHEANDÍA | ECHEANDÍA |
| 130 | 3 | BOLÍVAR | CHIMBO | CHIMBO |
| 131 | 3 | BOLÍVAR | SAN MIGUEL | SAN MIGUEL |
| 132 | 3 | BOLÍVAR | GUARANDA | SIMIATUG |
| 133 | 3 | CHIMBORAZO | RIOBAMBA | RIOBAMBA |
| 134 | 3 | CHIMBORAZO | CHUNCHI | CHUNCHI |
| 135 | 3 | CHIMBORAZO | ALAUSI | ALAUSI |
| 136 | 3 | CHIMBORAZO | COLTA | COLTA |
| 137 | 3 | CHIMBORAZO | CUMANDA | CUMANDA |
| 138 | 3 | CHIMBORAZO | GUAMOTE | GUAMOTE |
| 139 | 3 | CHIMBORAZO | GUANO | GUANO |
| 140 | 3 | CHIMBORAZO | PALLATANGA | PALLATANGA |
| 141 | 3 | CHIMBORAZO | PENIPE | PENIPE |
| 142 | 3 | COTOPAXI | LATACUNGA | LATACUNGA |
| 143 | 3 | COTOPAXI | SALCEDO | SALCEDO |
| 144 | 3 | COTOPAXI | LA MANA | LA MANA |
| 145 | 3 | COTOPAXI | PUJILÍ | PUJILÍ |
| 146 | 3 | COTOPAXI | SAQUISILI | SAQUISILI |
| 147 | 3 | COTOPAXI | PANGUA | PANGUA |
| 148 | 3 | COTOPAXI | SIGCHOS | SIGCHOS |
| 149 | 3 | COTOPAXI | PUJILÍ | ZUMBAHUA |
| 150 | 3 | TUNGURAHUA | AMBATO | AMBATO |
| 151 | 3 | TUNGURAHUA | AMBATO | IZAMBA |
| 152 | 3 | TUNGURAHUA | PELILEO | PELILEO |
| 153 | 3 | TUNGURAHUA | PILLARO | PILLARO |
| 154 | 3 | TUNGURAHUA | BAÑOS | BAÑOS |
| 155 | 3 | TUNGURAHUA | QUERO | QUERO |
| 156 | 3 | TUNGURAHUA | PATATE | PATATE |
| 157 | 2 | NAPO | TENA | TENA |
| 158 | 2 | NAPO | EL CHACO | EL CHACO |
| 159 | 2 | ORELLANA | ORELLANA | ORELLANA (COCA) |
| 160 | 2 | ORELLANA | LA JOYA DE LOS SACHAS | JOYA DE LOS SACHAS |
| 161 | 2 | ORELLANA | AGUARICO | AGUARICO |
| 162 | 2 | ORELLANA | LORETO | LORETO |
| 163 | 2 | PASTAZA | PUYO | PUYO |
| 164 | 2 | PASTAZA | ARAJUNO | ARAJUNO |
| 165 | 2 | SUCUMBÍOS | LAGO AGRIO | LAGO AGRIO |
| 166 | 2 | SUCUMBÍOS | SHUSHUFINDI | SHUSHUFINDI |
| 167 | 2 | SUCUMBÍOS | CASCALES | CASCALES |
| 168 | 2 | SUCUMBÍOS | CUYABENO | CUYABENO |
| 169 | 2 | SUCUMBÍOS | GONZALO PIZARRO | GONZALO PIZARRO |
| 170 | 1 | CARCHI | TULCÁN | TULCÁN |
| 171 | 1 | CARCHI | MONTUFAR | MONTUFAR |
| 172 | 1 | CARCHI | ESPEJO | ESPEJO |
| 173 | 1 | ESMERALDAS | ESMERALDAS | ESMERALDAS |
| 174 | 1 | ESMERALDAS | ATACAMES | ATACAMES |
| 175 | 1 | ESMERALDAS | ELOY ALFARO | ELOY ALFARO |
| 176 | 1 | ESMERALDAS | MUISNE | MUISNE |
| 177 | 1 | ESMERALDAS | QUININDE | QUININDE |
| 178 | 1 | ESMERALDAS | RIOVERDE | RIOVERDE |
| 179 | 1 | ESMERALDAS | SAN LORENZO | SAN LORENZO |
| 180 | 1 | IMBABURA | IBARRA | IBARRA |
| 181 | 1 | IMBABURA | ANTONIO ANTE | ANTONIO ANTE |
| 182 | 1 | IMBABURA | OTAVALO | OTAVALO |
| 183 | 1 | IMBABURA | COTACACHI | COTACACHI |

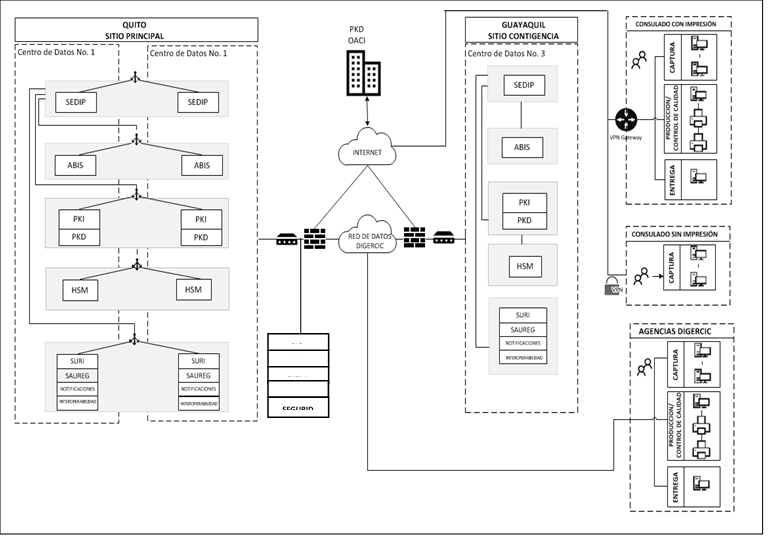
# AGENCIAS DE EMISION DE PASAPORTES DE LA DIGERCIC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **ZONA** | **PROVINCIA** | **CIUDAD** | **AGENCIA** |
| 1 | 9 | PICHINCHA | QUITO | MATRIZ NNUU |
| 2 | 8 | GUAYAS | GUAYAQUIL | GOBERNACIÓN ZONAL |
| 3 | 7 | EL ORO | MACHALA | MACHALA |
| 4 | 7 | LOJA | LOJA | LOJA |
| 5 | 7 | ZAMORA CHINCHIPE | ZAMORA | ZAMORA |
| 6 | 6 | AZUAY | CUENCA | SAN BLAS |
| 7 | 6 | CAÑAR | AZOGUES | AZOGUES |
| 8 | 6 | MORONA SANTIAGO | MORONA | MORONA |
| 9 | 5 | GALAPAGOS | SAN CRISTOBAL | SAN CRISTOBAL |
| 10 | 5 | LOS RIOS | BABAHOYO | BABAHOYO |
| 11 | 5 | SANTA ELENA | SALINAS | SALINAS |
| 12 | 4 | MANABI | MANTA | MANTA |
| 13 | 4 | MANABI | PORTOVIEJO | PORTOVIEJO |
| 14 | 4 | STO DOM TSACHILAS | SANTO DOMINGO | SANTO DOMINGO |
| 15 | 3 | BOLIVAR | GUARANDA | GUARANDA |
| 16 | 3 | CHIMBORAZO | RIOBAMBA | RIOBAMBA |
| 17 | 3 | COTOPAXI | LATACUNGA | LATACUNGA |
| 18 | 3 | TUNGURAHUA | AMBATO | AMBATO |
| 19 | 2 | NAPO | TENA | TENA |
| 20 | 2 | ORELLANA | ORELLANA | ORELLANA |
| 21 | 2 | PASTAZA | PASTAZA | PASTAZA |
| 22 | 2 | SUCUMBIOS | LAGO AGRIO | LAGO AGRIO |
| 23 | 1 | CARCHI | TULCAN | TULCAN |
| 24 | 1 | ESMERALDAS | ESMERALDAS | ESMERALDAS |
| 25 | 1 | IMBABURA | IBARRA | IBARRA |

# PUNTOS DE CAPTURA DE DATOS PARA EMISIÓN DE PASAPORTES DEL MREMH

|  |  |  |
| --- | --- | --- |
| **Nro** | **PAÍS** | **CIUDAD** |
| 1 | VENEZUELA | CARACAS |
| 2 | VENEZUELA | VALENCIA-VENEZUELA |
| 3 | COLOMBIA | BOGOTÁ |
| 4 | COLOMBIA | IPIALES |
| 5 | CHILE | SANTIAGO DE CHILE |
| 6 | PERÚ | LIMA |
| 7 | PERÚ | TUMBES |
| 8 | BOLIVIA | LA PAZ |
| 9 | PARAGUAY | ASUNCIÓN |
| 10 | URUGUAY | MONTEVIDEO |
| 11 | ARGENTINA | BUENOS AIRES |
| 12 | BRASIL | SAO PAULO |
| 13 | BRASIL | BRASILIA |
| 14 | BRASIL | RIO DE JANEIRO |
| 15 | ECUADOR | QUITO |
| 16 | ECUADOR | GUAYAQUIL |
| 17 | PANAMÁ | PANAMÁ |
| 18 | REP. DOMINICANA | SANTO DOMINGO - REP. DOMINICANA |
| 19 | NICARAGUA | MANAGUA |
| 20 | HONDURAS | TEGUCIGALPA |
| 21 | GUATEMALA | CIUDAD DE GUATEMALA |
| 22 | EL SALVADOR | SAN SALVADOR |
| 23 | COSTA RICA | SAN JOSÉ DE COSTA RICA |
| 24 | CUBA | LA HABANA |
| 25 | MÉXICO | CIUDAD DE MÉXICO |
| 26 | MÉXICO | MONTERREY |
| 27 | MÉXICO | TAPACHULA |
| 28 | ESTADOS UNIDOS | NUEVA YORK |
| 29 | ESTADOS UNIDOS | MIAMI |
| 30 | ESTADOS UNIDOS | HOUSTON |
| 31 | ESTADOS UNIDOS | LOS ÁNGELES |
| 32 | ESTADOS UNIDOS | WASHINGTON |
| 33 | ESTADOS UNIDOS | ATLANTA |
| 34 | ESTADOS UNIDOS | PHOENIX |
| 35 | ESTADOS UNIDOS | CHICAGO |
| 36 | ESTADOS UNIDOS | NEW JERSEY |
| 37 | ESTADOS UNIDOS | QUEENS |
| 38 | ESTADOS UNIDOS | MINNEAPOLIS |
| 39 | ESTADOS UNIDOS | NEW HAVEN - CONNECTICUT |
| 40 | CANADÁ | TORONTO |
| 41 | CANADÁ | OTTAWA |
| 42 | CANADÁ | MONTREAL |
| 43 | ESPAÑA | MADRID |
| 44 | ESPAÑA | BARCELONA |
| 45 | ESPAÑA | VALENCIA-ESPAÑA |
| 46 | ESPAÑA | MURCIA |
| 47 | ESPAÑA | MÁLAGA |
| 48 | ESPAÑA | PALMA DE MALLORCA |
| 49 | ITALIA | MILÁN |
| 50 | ITALIA | ROMA |
| 51 | ITALIA | GÉNOVA |
| 52 | SUECIA | ESTOCOLMO |
| 53 | HOLANDA | LA HAYA |
| 54 | ALEMANIA | BERLÍN |
| 55 | ALEMANIA | HAMBURGO |
| 56 | HUNGRÍA | BUDAPEST |
| 57 | RUSIA | MOSCÚ |
| 58 | AUSTRIA | VIENA |
| 59 | REINO UNIDO | LONDRES |
| 60 | SUIZA | BERNA |
| 61 | FRANCIA | PARIS |
| 62 | BÉLGICA | BRUSELAS |
| 63 | EGIPTO | EL CAIRO |
| 64 | SUDÁFRICA | PRETORIA |
| 65 | ETIOPIA | ADDI ABEBA |
| 66 | NIGERIA | ABUJA |
| 67 | IRAN | TEHERAN |
| 68 | TURQUÍA | ANKARA |
| 69 | CHINA | BEIJING |
| 70 | CHINA | GUANZHOU |
| 71 | CHINA | SHANGHÁI |
| 72 | MALASIA | KUALA LUMPUR |
| 73 | COREA DEL SUR | SEÚL |
| 74 | INDIA | NUEVA DELHI |
| 75 | INDIA | MUMBAI |
| 76 | ISRAEL | TEL AVIV |
| 77 | JAPÓN | TOKIO |
| 78 | QATAR | DOHA-QATAR |
| 79 | INDONESIA | YAKARTA |
| 80 | AUSTRALIA | CANBERRA |

# DISEÑO FISICO DE ALTO NIVEL DEL SEDIP



# ESPECIFICACIONES TECNICAS DE EQUIPOS

|  |  |  |
| --- | --- | --- |
| ESPECIFICACIÓN TÉCNICA | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * **Condición de los equipos y componentes**   Todos los equipos y sus componentes deberán ser nuevos, de fábrica y no re-manufacturados   * **Año de fabricación**   El año de fabricación no deberá ser menor al año que se suministren los mismos o inferior al año de suscripción del contrato   * **Licencias de software**   Las licencias y/o suscripciones deberán ser contratadas a nombre de la DIGERCIC.   * **Integración de los equipos periféricos y componentes al SEDIP**   Los equipos, periféricos y componentes deberán integrarse y operar con el nuevo Sistema de Emisión de Documentos de Identidad y Pasaportes (SEDIP), a ser provisto por el proveedor   * **Garantía Técnica de los equipos**   Servirá(n) para asegurar la calidad y buen funcionamiento de los equipos de computación, periféricos e Impresoras. Tendrá(n) vigencia de 3 años contados a partir de la finalización de la implementación del nuevo sistema (SEDIP). Esta garantía tiene como finalidad la reposición de los bienes en caso de que estos tuvieren o presentaren fallas. El proveedor deberá reparar el equipo; o, reemplazarlo sin costo para la DIGERCIC.   * **Garantía de Vigencia Tecnológica**   Esta garantía establece de manera obligatoria el cumplimiento del principio de vigencia tecnológica respecto de:   1. Certificado del fabricante que garantice que los equipos no serán declarados descontinuados por el fabricante por un periodo mínimo de 5 años contados desde la fecha de entrega - recepción. 2. El fabricante deberá certificar que al menos durante los 5 años contará con vigencia de repuestos, partes y piezas, parches y software de actualización para los equipos ofertados. |  |  |

* **ESPECIFICACIONES TÉCNICAS**
* **COMPUTADORA DE ESCRITORIO “ULTRA-SLIM”**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Procesador | Mínimo Intel Core i7 de 8va. generación |  |  |
| N° de Núcleos | Mínimo 4 núcleos |  |  |
| Frecuencia base del procesador | Mínimo 3.20 GHz. |  |  |
| Cache | Mínimo 8 MB |  |  |
| Capacidad Disco Duro | Mínimo 240 GB |  |  |
| Tipo de Disco | De estado sólido |  |  |
| Memoria RAM | Mínimo 8 GB DDR4 2666 MHZ |  |  |
| Puertos USB | Mínimo 8 puertos USB 2.0 o superior integrados, independientes de los puertos de mouse y teclado |  |  |
| Otros puertos | 1 puerto HDMI integrado  Opcional 1 puerto VGA integrado |  |  |
| Interfaz de audio | Integrada |  |  |
| Unidad óptica | No requerida, no debe venir con el equipo |  |  |
| Interfaz de red cableada | Puerto Ethernet: mínimo 100/1000 BASE-T integrada (compatible IPV4 - IPV6) |  |  |
| Interfaz de red inalámbrica | Opcional Wireless integrada estándar 802.11 a/b/g/n |  |  |
| Alimentación eléctrica | Debe soportar:  Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |
| Monitor | Tecnología Retroiluminación LED  Entre 18’’ y 19’’ con resolución nativa HD (1366 x 768 a 60 Hz)  Interfaces de entrada HDMI o VGA (Debe poseer mínimo la interfaz de conexión del CPU)  Alimentación eléctrica AC 100V – 240 V, ±10%, frecuencia de AC 50Hz – 60Hz (dependiendo de la región) |  |  |
| Teclado | USB 2.0 o Superior o PS/2, idioma español |  |  |
| Mouse | USB 2.0 o Superior o PS/2 |  |  |
| Sistema operativo | Preinstalado con su respectivo licenciamiento o suscripción (Microsoft última versión o Linux en sus distribuciones estables), en español.  El sistema operativo deberá garantizar la operación del SEDIP. |  |  |
| Software requerido | Antivirus, aplicación de seguridad o bloqueo de puertos USB a través de BIOS, con el licenciamiento o suscripciones correspondiente para al menos 3 años.  El software deberá garantizar la operación del SEDIP. |  |  |

* **ESCANER UNIDACTILAR**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Funcionalidad | Deberá soportar:  Solo captura de huella plana viva |  |  |
| Estándares y Certificaciones | El equipo deberá cumplir con las certificaciones y estándares ampliamente aceptados a nivel internacional para este tipo de equipo (ANSI/NIST, Restriction of Hazardous Substances, Federal Bureau of Investigation o equivalentes) |  |  |
| Resolución | Mínimo 500 dpi |  |  |
| Mecanismo de captura | Automático |  |  |
| Área de escaneo (Platen Size) | Mínimo: Largo=2.5 cm x ancho=1.8 cm |  |  |
| Formato de captura | Una huella plana viva |  |  |
| Software estándar | Software de procesamiento  Módulo de compresión WSQ  Módulo de interface |  |  |
| Tipo de Conexión | Poseer la capacidad de comunicación por puerto USB 2.0 o superior |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **ESCANER DE HUELLAS DECADACTILAR**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Funcionalidad | Deberá soportar:  Solo captura de huellas planas vivas  Calibración automática y actualizaciones de tablas.  Campos de datos pre formateados basados en listas predefinidas.  Características configurables de entrada de datos. |  |  |
| Estándares y Certificaciones | El equipo deberá cumplir con las certificaciones y estándares ampliamente aceptados a nivel internacional para este tipo de equipo (ANSI/NIST, Restriction of Hazardous Substances, Federal Bureau of Investigation o equivalentes) |  |  |
| Resolución | Mínimo 500 dpi |  |  |
| Mecanismo de captura | Automático o vía botón de captura |  |  |
| Área de escaneo (Platen Size) | Mínimo (Ancho= 9.5 cm x Largo= 7.5 cm) |  |  |
| Indicadores LED | Alimentación, estado y calidad de imagen |  |  |
| Formato de captura | Huellas planas vivas (tipo de captura 4, 4, 2) |  |  |
| Software estándar | Software de procesamiento  Captura de imágenes de huellas NIST  Módulo de compresión WSQ  Módulo de interface  Módulo de comprobación de calidad y secuencia  Segmentación de huellas posadas a imágenes de huellas posadas singulares |  |  |
| Tipo de Conexión | Poseer la capacidad de comunicación por puerto USB 2.0 o superior. |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **CÁMARA FOTOGRÁFICA DIGITAL**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Tipo de Cámara | WEB con estabilizador óptico de imagen. |  |  |
| Captura de Imágenes | Capacidad de capturar imágenes en vivo, en tiempo real. |  |  |
| Zoom óptico | Soportar la capacidad de zoom óptico controlado desde software |  |  |
| Funcionalidad | Poseer controladores de funciones y captura de imágenes desde el computador. |  |  |
| Resolución Fotográfica | Mínimo 8 Megapíxeles, que permita la captura de imágenes de acuerdo a lo que establece las normas OACI documento 9303 vigente. |  |  |
| Autofoco | Automático |  |  |
| Sistema de encuadre y recorte de imagen | Obligatorio |  |  |
| Reducción de ojos rojos | Obligatorio durante disparo y reproducción |  |  |
| Sistema de Iluminación | Obligatorio, especificar (no debe afectar la calidad requerida para la imagen) |  |  |
| Comprensión | Debe cumplir con la norma H.264 o MPEG-4 parte 10 |  |  |
| Tipo de Conexión | Poseer la capacidad de comunicación por puerto USB 2.0 o superior |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **TRIPODE DE CÁMARA FOTOGRÁFICA**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Longitud | Tamaño Plegado:  Entre 30,0 cm y 36,0 cm, incluyendo rótula o cabeza.  Altura Máxima:  Entre 50,0 cm y 110,0 cm, incluyendo rótula o cabeza.  Altura Mínima (Apertura de soportes o patas):  Entre 28,0 cm y 35,0 cm, incluyendo rótula o cabeza.  Estas dimensiones son adecuadas para la operación eficiente de la cámara fotográfica y su ubicación sin afectar la organización y el diseño de las estaciones de trabajo ubicadas en los módulos de atención que la DIGERCIC tiene instalados a nivel nacional. |  |  |
| Funcionalidad | Deberá soportar y asegurar la cámara web que se utilizará para la captura de datos |  |  |
| Rótula o cabeza | 3D que permita el movimiento de la cámara web en los tres ejes |  |  |
| Características adicionales | * Patas selladas de 3 secciones con columna central elevadora * Bloqueo rápido de palancas * Soportes radiales para escritorio * Número de niveles de burbuja 1 |  |  |
| Material principal | Aluminio |  |  |

* **TELÓN PARA CAPTURA DE FOTOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Dimensiones | Ancho: Entre 73 y 75 cm  Alto: 100 y 105 cm.  Este tamaño es el adecuado para no obstaculizar ni afectar la organización ni el diseño de las áreas físicas correspondientes a los módulos de atención que la DIGERCIC tiene instalados a nivel nacional. |  |  |
| Materiales | Lona impermeable + Aluminio |  |  |
| Color de la lona | Blanco no reflectivo. |  |  |

* **TRÍPODE DE TELON**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Dimensiones | Tamaño Plegado:  Entre 63,0 cm y 110,0 cm, incluyendo soporte de telón.  Altura Máxima:  Entre 180,0 cm y 250,0 cm, incluyendo soporte de  Telón.  Altura Mínima (Apertura de soportes o patas):  Entre 80,0 cm y 120,0 cm, incluyendo soporte de  Telón.  Estas dimensiones son adecuadas para el mejor uso del telón y su ubicación sin afectar la organización y el diseño de las estaciones de trabajo ubicadas en los módulos de atención que la DIGERCIC tiene instalados a nivel nacional |  |  |
| Funcionalidad | Deberá soportar y asegurar de forma vertical el telón que se utilizará para la captura de datos |  |  |
| Características adicionales | * Piernas selladas de 3 secciones con columna central elevadora * Bloqueo rápido de palancas * Soportes radiales para piso. * Rosca de tornillo de diámetro: ¼” |  |  |
| Material principal | Aluminio |  |  |

* **TABLETA/PAD DE CAPTURA DE FIRMAS MANUSCRITAS**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Diseño | Ergonómico |  |  |
| Tipo de sensor | Activo electromagnético |  |  |
| Lápiz/bolígrafo | * Activo energizado, sin batería * Ultrasensible con al menos 1024 niveles de sensibilidad a la presión en la captura de la firma * Integrado al pad o con mecanismo de seguridad contra robos |  |  |
| Pantalla | Retro iluminada |  |  |
| Resolución nativa | Mínimo 800 x 480 píxeles |  |  |
| Tamaño de pantalla | Mínimo (Ancho=11.0 cm x Largo=6.0 cm) |  |  |
| Velocidad de Captura | Mínimo 200 puntos por segundo o superior |  |  |
| Visualización | Soportar la capacidad de visualizar la firma en tiempo real. |  |  |
| Tipo de conexión | Poseer la capacidad de comunicación por puerto USB 2.0 o superior |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **ESCANER DE DOCUMENTOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Fuente de alimentación | Debe soportar:  Voltajes de AC entre 110V – 240V, ±10% (dependiendo de la región)  Frecuencia de AC entre 50Hz – 60Hz (dependiendo de la región) |  |  |
| Tipo de escaneo | Simplex, Dúplex, blanco y negro, color |  |  |
| Tipo de alimentación de documentos | Alimentación frontal, ADF |  |  |
| Resolución óptica | Mínimo 300 dpi |  |  |
| Resolución de producción | 100dpi / 150dpi / 200dpi / 240dpi / 300dpi / 600dpi o superior |  |  |
| Tamaño de documentos | Máximo A4/Carta/Oficio (21.0 x 29.7 cm)  Mínimo A8 (5.2 x 7.4 cm) |  |  |
| Velocidad de escaneo blanco y negro | Simplex: mínimo 40 ppm  Dúplex: mínimo 80 ipm |  |  |
| Velocidad de escaneo color | Simplex: mínimo 30 ppm  Dúplex: mínimo 60 ipm |  |  |
| Controladores | Al menos deberá poseer controladores TWAIN, WIA que permita la captura desde otras aplicaciones. |  |  |
| Tipo de conexión | Poseer la capacidad de comunicación por puerto USB 2.0 o superior |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **ESCÁNER PORTÁTIL DE KIT MÓVIL DE CAPTURA DE DATOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Fuente de alimentación | A través de bus USB y batería interna |  |  |
| Tiempo de carga de la batería | Mínimo 4 horas |  |  |
| Alimentación eléctrica | Debe soportar:   * Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |
| Tipo de escaneo | Simplex, Dúplex, blanco y negro, color |  |  |
| Tipo de alimentación de documentos | Automática |  |  |
| Resolución óptica | 300 dpi o superior |  |  |
| Resolución de producción | 100dpi / 150dpi / 200dpi / 240dpi / 300dpi / 600dpi o superior |  |  |
| Tamaño de documentos | Máximo A4/Carta/Oficio (21,6 cm x 27,9 cm)  Mínimo A8 (5,2 cm x 7,4 cm) |  |  |
| Velocidad de escaneo blanco y negro | Simplex: mínimo 7 ppm  Dúplex: mínimo 14 ipm |  |  |
| Velocidad de escaneo color | Simplex: mínimo 5 ppm  Dúplex: mínimo 10 ipm |  |  |
| Controladores | Al menos deberá poseer controladores TWAIN, WIA que permita la captura desde otras aplicaciones. |  |  |
| Tipo de conexión | Poseer la capacidad de comunicación por puerto USB 2.0 o superior y WiFi integrado 802.11 |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **COMPUTADORA PORTÁTIL DE KIT MÓVIL DE CAPTURA DE DATOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Procesador | Mínimo Intel Core i7 de 8va generación |  |  |
| N° de Núcleos | Mínimo 4 núcleos |  |  |
| Frecuencia base del procesador | Mínimo 1.8Ghz. hasta 4.0 GHz. Con frecuencia turbo |  |  |
| Cache | Mínimo 8 MB |  |  |
| Capacidad Disco Duro | Mínimo 240 GB |  |  |
| Tipo de Disco | De estado sólido |  |  |
| Memoria RAM | Mínimo 8 GB DDR4 2666 MHZ |  |  |
| Puertos USB | Mínimo 4 puertos USB 2.0 o superior integrados. Adicional un concentrador de al menos 4 puertos USB 2.0 o superior que garantice la operación simultánea de periféricos.(8 puertos USB 2.0 o superior en TOTAL) |  |  |
| Otros puertos | 1 puerto HDMI, opcional 1 puerto VGA (integrado) |  |  |
| Interfaz de audio | Integrada |  |  |
| Unidad óptica | No requerida, no debe venir con el equipo |  |  |
| Interfaz de red cableada | Puerto Ethernet: mínimo 100/1000 BASE-T integrada (compatible IPV4 - IPV6). |  |  |
| Interfaz de red inalámbrica | Wireless integrada estándar 802.11 a/b/g/n o superior |  |  |
| Pantalla | Mínimo 14” HD |  |  |
| Teclado | En español |  |  |
| Duración de la batería | Mínimo 4 horas |  |  |
| Alimentación eléctrica | Debe soportar:   * Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |
| Sistema operativo | Preinstalado con su respectivo licenciamiento o suscripción (Microsoft última versión o Linux en sus distribuciones estables), en español.  El sistema operativo deberá garantizar la operación del SEDIP |  |  |
| Software requerido | Antivirus, aplicación de seguridad o bloqueo de puertos USB a través de BIOS, con el licenciamiento o suscripciones correspondiente para al menos 3 años.  El software deberá garantizar la operación del SEDIP. |  |  |

* **LECTOR DE DOCUMENTOS OACI DOC 9303**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Diseño | Compacto |  |  |
| Funcionalidad | Deberá soportar:   * Lectura de pasaportes y tarjetas inteligentes con chip RFID sin contacto (cumplen con la norma OACI doc. 9303 y el estándar ISO 14443 vigentes) * Exploración automática mediante lectura OCR (MRZ) * Integración automática de lectura OCR (MRZ) y RFID (Lectura del chip) |  |  |
| Estándares y certificaciones | El equipo deberá cumplir con las certificaciones y estándares ampliamente aceptados a nivel internacional para este tipo de equipo ( Restriction of Hazardous Substances o equivalentes) |  |  |
| Procesamiento de documentos | * OCR con mínimo 400 dpi * RFID * NFC * Código de barras * Lectura de imágenes a color con una profundidad de al menos 24 bits * Lectura infrarrojo, lectura de laminado de seguridad ultra violeta * Tecnología anti deslumbrante * Lectura en ambiente con luz natural, luz ultravioleta, luz infrarroja |  |  |
| Área de escaneo | Mínimo 12,5 cm x 8,5 cm |  |  |
| Formatos de captura | ID – 1 (tarjeta de identidad)  ID – 2 (tarjeta de pasaporte, visa)  ID – 3 (pasaporte) |  |  |
| Tipo de conexión | Poseer la capacidad de comunicación por puerto USB 2.0 o superior |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **IMPRESORA DE CÉDULAS DE GRABADO POR LASER**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Tipo | Desktop |  |  |
| Tecnología de impresión | Sistema de grabado láser CLI / MLI |  |  |
| Modo de impresión | Dúplex |  |  |
| Módulo de codificación electrónica | * Integrado * Con capacidad de codificación de tarjetas electrónicas sin contacto |  |  |
| Unidad láser | Láser de fibra de al menos 20 W con cámara de protección |  |  |
| Color de impresión | Escala de grises |  |  |
| Resolución | Mínimo 600 dpi |  |  |
| Material de la tarjeta del documento de identidad | Policarbonato (PC) |  |  |
| Características de la tarjeta del documento de identidad | Formato ID – 1  Cumple con:   * Norma OACI doc. 9303 vigente * Estándar ISO 7816 vigente * Estándar ISO 7810 vigente |  |  |
| Rendimiento | Mínimo 150 tarjetas por hora terminadas incluyendo los siguientes procesos para cada tarjeta inteligente:   * Grabado láser a doble lado. * Codificación electrónica (grabación de información en el chip conforme normas ICAO) * Verificación de la codificación electrónica (Control de calidad - QC) |  |  |
| Pantalla de impresora (display) | Incluido para alertas y estado de la impresora |  |  |
| Alimentador de entrada | Al menos de 125 tarjetas |  |  |
| Bandeja de rechazo | Incluida |  |  |
| Bandeja de salida | Incluida |  |  |
| Alimentación eléctrica | Debe soportar:  Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |
| Tipo de conexión | Ethernet 10/100 BASE-T integrada (compatible IPV4 - IPV6) y/o USB 2.0 o superior |  |  |
| Sistema operativo soportado | Basados en distribuciones estables de Linux o Microsoft últimas versiones |  |  |
| Monitoreo | Por software, requerido. Se deberá incluir licencia o suscripción respectiva, de ser el caso |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **IMPRESORA DE PASAPORTES POR TECNOLOGIA DE TINTA**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Tipo | Modular |  |  |
| Tecnología de impresión | Inyección a tinta de cuatro (4) colores |  |  |
| Modo de impresión | Simplex |  |  |
| Funcionalidades de impresión | Imprimir fotos a todo color, en tonos o en blanco y negro, imágenes y texto directamente en páginas de datos para pasaportes de papel conforme normas ICAO doc. 9303 vigente. |  |  |
| Resolución impresión | Mínimo 720 dpi |  |  |
| Depósitos de tinta | De alta capacidad  Mínimo de 400 ml (100 ml para cada color) |  |  |
| Sistema de alineación óptico para impresión | Requerido   * Auto posicionamiento * OCR * Detección de color |  |  |
| Sistemas de inspección óptica para la verificación de entrada / salida | Requeridos |  |  |
| Características del pasaporte | Formato ID – 3  Estándares:   * Norma OACI doc. 9303 vigente |  |  |
| Grosor del pasaporte | Mínimo 32 páginas |  |  |
| Alimentador automático de pasaportes | Requerido, con bandeja de entrada mínimo para 30 pasaportes |  |  |
| Alimentador manual de pasaportes | Incluido |  |  |
| Bandeja de rechazo | Incluida |  |  |
| Bandeja de salida | Incluida |  |  |
| Módulo de laminación | Requerido, en línea para superposición de seguridad en la página de datos del pasaporte. La laminadora debe permitir el uso de láminas de cualquier fabricante de láminas de seguridad holográficas. |  |  |
| Módulo de codificación electrónica | Integrado y en línea  Con capacidad de codificación de pasaportes electrónicos con chip sin contacto, ISO / IEC 14443 |  |  |
| Correspondencia de datos entre personalización óptica y electrónica | Requerida |  |  |
| Rendimiento | Mínimo 120 pasaportes por hora incluyendo los siguientes procesos para cada pasaporte electrónico: impresión gráfica, codificación electrónica (grabación en el chip conforme normas ICAO doc. 9303 vigentes) y verificación de la codificación electrónica |  |  |
| Alimentación eléctrica | Debe soportar:   * Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |
| Tipo de conexión | Ethernet 10/100 BASE-T integrada (compatible IPV4 - IPV6) y/o USB 2.0 o superior |  |  |
| Sistema operativo soportado | Basados en distribuciones estables de Linux o Microsoft últimas versiones |  |  |
| Monitoreo | Por software, requerido. Se deberá incluir licencia o suscripción respectiva, de ser el caso. |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **IMPRESORA PORTÁTIL DE KIT MÓVIL DE CAPTURA DE DATOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Velocidad de impresión con alimentación AC | Mínimo 7 ppm en negro y 4 ppm en color |  |  |
| Velocidad de impresión con Batería | Mínimo 3,5 ppm en negro y 2 ppm en color |  |  |
| Resolución de impresión | Mínimo 760 x 1440 dpi |  |  |
| Tamaño de papel | A4/Carta/Oficio (21,6 cm x 27,9 cm) |  |  |
| Capacidad de la bandeja de entrada | Mínimo 20 hojas de papel común |  |  |
| Rendimiento de los cartuchos de tinta | Mínimo 600 páginas en negro y 450 páginas a color |  |  |
| Rendimiento de la batería a carga completa | Mínimo 100 páginas en blanco y negro o 50 páginas en colores |  |  |
| Peso de la impresora | Inferior a 1.6 KG |  |  |
| Alimentación eléctrica | Debe soportar:   * Voltajes de AC 110V – 120V, ±10% * Frecuencia de AC 60Hz |  |  |
| Tipo de conexión | USB de alta velocidad y Wi-Fi integrado 802.11 b/g/n |  |  |
| SDK (software development kit) | Requerido, de preferencia Java |  |  |

* **MALETA DEL KIT MÓVIL DE CAPTURA DE DATOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Funcionalidad | Deberá contener todos los ítems excepto el telón y trípode de telón correspondientes al Kit de Captura Móvil y permitir su traslado de forma segura y protegida, considerando que la mayoría de componentes son electrónicos y de precisión. |  |  |
| Material | Carcasa de polipropileno |  |  |
| Resistente a | * Golpes * Agua * Polvo * Calor * Humedad |  |  |
| Características adicionales | Diseño ergonómico, cierres de fácil apertura, válvula de compensación de presión automática permitiendo que el aire se escape bajo presión e impidiendo la entrada de agua. Facilidad para transportar.  Temperatura del contenido de la maleta estable con temperaturas exteriores de entre -40 ° C y + 80 ° C |  |  |
| Acolchados en el interior | Deberá ser con espuma y separadores acolchados |  |  |
| Fuente de alimentación | Especificar |  |  |
| Dimensiones externas deseables mínimas | Largo: entre 56 cm y 60 cm.  Ancho: entre 45 cm y 50 cm.  Profundidad: entre 20 cm y 25 cm. |  |  |
| Portabilidad | Debe disponer de un mango ergonómico con acolchado interior, ruedas de goma y asa ergonómica telescópica. |  |  |
| Aseguramiento | Bisagras con llave de seguridad |  |  |

* **CONTENEDOR DE TELÓN Y TRÍPODE DE TELÓN**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Funcionalidad | Deberá contener el telón y el trípode de telón correspondientes al Kit de Captura Móvil y permitir su traslado de forma segura y protegida |  |  |
| Material | Carcasa de polipropileno |  |  |
| Resistente a | Golpes  Agua  Polvo |  |  |
| Características adicionales | Diseño ergonómico, cierres de fácil apertura |  |  |
| Acolchados en el interior | Separadores acolchados |  |  |
| Dimensiones externas deseables  Mínimas | Largo total externo:  Hasta 110 cm. que es el largo máximo plegado del trípode de telón.  Diámetro externo:  Hasta 14 cm. |  |  |
| Portabilidad | Correas ergonómicas |  |  |
| Aseguramiento | Mecanismo de fácil aseguramiento |  |  |

* **GATEWAY DE SEGURIDAD**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Frecuencia CPU | Mínimo 880 MHz |  |  |
| Memoria | Mínimo 256 MB |  |  |
| Puertos físicos | Mínimo 2 puertos Layer 3 Gigabit Ethernet 1000BASE-T |  |  |
| Características IP | Debe soportar:   * IPv4 e IPv6 * Enrutamiento estático. * Capacidad para crear al menos 20 802.1Q VLANs. * Capacidad para realizar enrutamiento inter-VLAN. * Network Address Translation. * Virtual Router Redundancy Protocol (VRRP) (RFC 2338). * Servidor DHCP. * Cliente/Servidor FTP para transferencia de archivos de configuración. |  |  |
| Internet Protocol Security (IPsec) | Debe soportar:   * Capacidad para crear al menos 5 túneles IPsec. * Métodos de encriptación IKEv1 e IKEv2. * Algoritmos de encriptación: DES, 3DES, AES 128, AES 192 y AES 256. * Al menos SHA-256 para integridad de datos. * Diffie-Hellman Group 1, 2, 5, 14. * Autenticación PSK. * Compatibilidad total con Checkpoint GAiA R77.30, R80.10 y R80.20 para la negociación y establecimiento de los túneles IPsec. |  |  |
| Seguridad del Dispositivo | Debe tener la capacidad de:   * Creación de usuarios de administración. * Capacidad de encriptación de contraseñas de usuarios de administración. * Administración vía SSHv2. * Mecanismos de control de acceso o firewall para bloqueo de tráfico IP y aseguramiento del dispositivo. |  |  |
| Administración | Debe permitir:   * Administración vía SSHv2 * SNMP v1, v2 y v3 * Interfaz de línea de comandos. * Administración web vía http o https (opcional) |  |  |
| Alimentación eléctrica | Debe soportar:  Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |

* **MODULOS DE SEGURIDAD POR HARDWARE (HSM)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| APIS criptográficos | * PKCS#11, * CAPI/CNG, (MS) * JCA/JCE, (Java) * Otros opcional (Jcprov, Openssl) |  |  |
| Algoritmos  criptográficos  asimétricos  soportados | * RSA (hastaq 4096 bits) * DSA * ECDSA, * Diffie Hellman (DH) * ECC * Brainpool curves (nombrados y definidos por el usuario) |  |  |
| Algoritmos  criptográficos  simétricos  soportados | * AES * DES * 3DES * Otros opcionales (CAST-128, RC2, RC4, SEED, ARIA, etc.) |  |  |
| Algoritmos de  HASING | * MD5, * SHA-1, SHA-2(SHA-224, SHA-256, SHA-384, SHA-512) * RIPEMD (RIPEMD128, RIPEMD160) * Otros opcionales (ND2, DES MDC-2, PADI.) |  |  |
| Códigos para  autentificación de  mensajes | * SHA-1, SHA-2(SHA-224, SHA-256, SHA-384, SHA-512) * RIPEMD (RIPEMD128, RIPEMD160) * MAC / CMAC / HMAC * Otros opcionales (ND2, DES MDC-2 PADI, SSL3, DES3 RETAIL, VISA CVV.) |  |  |
| Condiciones de  Operación | * Voltajes de operación: 110/220 V. * Temperatura de operación: 10°C- 40°C. * Humedad relativa no condensada: 20% a 90% * MTBF mínimo 150,000 horas a 25°C / 77°F |  |  |
| Certificaciones de  seguridad y  ambientales | * Niveles de seguridad: FIPS 140-2 Level 3 * UL, CSA, CE, * FCC, KC Mark, VCCI, * ROHS, WEEE |  |  |
| Características  Generales | * Generación de números aleatorios reales (TNRG) * Copia de seguridad de la tarjeta inteligente del material clave * Doble conector de red * Administración remota (vía red) * Administración local * Soportar interface gráfica del HSM * Opciones múltiples para autentificación y control de acceso. * Múltiple integración para aplicaciones de PKI, servicios de encriptación * Separación de tareas * Sistemas operativos soportados: Windows y Linux * Rendimiento nominal mínimo (firmas RSA /segundo, 2048 bit, modo Bulk): 25 * Habilitado para operación en cluster (alta disponibilidad). * Debe permitir la importación / exportación de llaves internas a través de un método seguro y NO propietario, desde y hacia otro HSM * Protección física contra manipulación |  |  |

* **MONITOR WALL PANEL (PARA MONITOREO)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Tipo de pantalla | EDGE LED o superior |  |  |
| Tamaño de la pantalla (pulgada) | Mínimo 60’’ |  |  |
| Resolución | Mínimo 1920 x 1080p |  |  |
| Interfaz | Deberá contar con al menos:  3 puertos HDMI  2 puertos USB 2.0 o superior  1 canal de retorno de audio (CRA)  1 entrada RF IN |  |  |
| Comunicación | Mínimo WiFi (802.11ac) y LAN (puerto Ethernet) |  |  |
| Soporte de pared | Requerido |  |  |
| Alimentación eléctrica | Debe soportar:  Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |

* **COMPUTADOR PERSONAL “ALL IN ONE” CON DOBLE MONITOR (PARA MONITOREO)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **REQUERIMIENTO** | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| Marca | Especificar, debe ser de marca reconocida a nivel mundial. |  |  |
| Modelo | Especificar |  |  |
| Procesador | Mínimo Core i7 de 8va generación |  |  |
| N° de Núcleos | Mínimo 4 núcleos |  |  |
| Frecuencia base del procesador | Mínimo 3.20 Ghz |  |  |
| Cache | Mínimo 8 MB |  |  |
| Capacidad Disco Duro | Mínimo 240 GB |  |  |
| Tipo de Disco | De estado sólido |  |  |
| Memoria RAM | Mínimo 8 GB DDR4 2666 MHZ |  |  |
| Puertos USB | Mínimo 6 puertos USB 2.0 o superior integrados |  |  |
| Otros puertos | 1 puerto HDMI integrado  1 puerto VGA integrado (Opcional) |  |  |
| Interfaz de audio | Integrada |  |  |
| Unidad óptica | No requerida, no debe venir con el equipo |  |  |
| Interfaz de red cableada | Puerto Ethernet: mínimo 100/1000 BASE-T integrada (compatible IPV4 - IPV6) |  |  |
| Interfaz de red inalámbrica | Opcional Wireless integrada estándar 802.11 a/b/g/n |  |  |
| Alimentación eléctrica | Debe soportar:  Voltajes de AC entre 110V – 240V ±10% con frecuencias entre 50Hz y 60Hz con capacidad de integrarse a las redes eléctricas a nivel mundial. |  |  |
| Monitores | Con retroiluminación LED o WLED  Display integrado: Mínimo 20” con resolución nativa HD mínima de 1366 x 768, interfaces de entrada HDMI y VGA (Opcional).  Monitor adicional: Mínimo 20” con resolución nativa HD mínima de 1366 x 768, Interfaces de entrada HDMI y VGA (Opcional), de la misma marca del equipo All in One ofertado con su respectivo cable de conexión.  Alimentación eléctrica AC 100V ±10%, frecuencia de AC 60Hz. |  |  |
| Teclado | USB |  |  |
| Mouse | USB |  |  |
| Sistema operativo | Preinstalado con su respectivo licenciamiento o suscripción (Microsoft última versión o Linux en sus distribuciones estables), en español. |  |  |

# REQUERIMIENTOS DE LOS SERVICIOS POST-IMPLEMENTACION

**E.1) MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE**

| **CARACTERÍSTICAS Y CONDICIONES REQUERIDAS POR LA DIGERCIC** | | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| --- | --- | --- | --- |
| **Actividades del mantenimiento preventivo** | El Proveedor deberá aplicar mantenimiento preventivo a los componentes del sistema: hardware y software de los centros de datos, kits de captura, kits de producción y kits de entrega de documentos de identidad y pasaportes instalados en los puntos de atención del país y del extranjero.  El Proveedor deberá ejecutar al menos las siguientes actividades:   * Revisar visualmente los equipos, accesorios, conexiones y realizar un diagnóstico relacionado con el estado de su funcionamiento. Revisar alertas, logs y posibles fallas. * Aplicar a los kits y sus componentes limpieza externa e interna, conforme los estándares de los fabricantes y las buenas prácticas. * Aplicar actualizaciones de firmware, drivers y software de administración o control recomendado y liberado por el fabricante de los equipos, previa autorización y aprobación de la CGTIC de la DIGERCIC. * Reemplazar equipos, partes y/o piezas defectuosas o dañadas por cuenta del Proveedor, de ser necesario y sin costo adicional para la DIGERCIC. Los equipos, partes y piezas deberán ser nuevas de fábrica y no usadas o re- manufacturadas (Refurbished). Los reemplazos se deberán ejecutar en coordinación con los técnicos de la CGTIC y el MREMH. * Levantar/actualizar el inventario de los equipos: marca, modelo, número de serie, componentes básicos y sus características, dispositivos y otros según lineamientos de la CGTIC. * Realizar pruebas de hardware y software para verificar el funcionamiento normal de los equipos, previo a la finalización del mantenimiento. |  |  |
| **Periodicidad del mantenimiento preventivo** | El mantenimiento preventivo deberá ejecutarse:   * Semestralmente. Es decir, durante los tres años deberán ejecutarse 6 mantenimientos preventivos. El primer mantenimiento deberá ejecutarse 6 meses después de que haya finalizado el despliegue del SEDIP. * Previa la ejecución de cada visita de mantenimiento, el Proveedor deberá presentar un cronograma que deberá ser aprobado por la CGTIC de la DIGERCIC, con al menos 15 días de anticipación al inicio de la visita. Con este cronograma el Proveedor presentará el listado de actualizaciones de hardware (drivers, firmware, otros) y software(parches de seguridad, actualizaciones, nuevas versiones, herramientas liberadas por el fabricante), que si la DIGERCIC lo considera pertinentes autorizará para que se apliquen como parte del mantenimiento preventivo. * La DIGERCIC podrá cambiar las fechas de los mantenimientos previa notificación al Proveedor con al menos 3 días laborables de anticipación. |  |  |
| **Plazo de ejecución de cada visita de mantenimiento preventivo** | Cada visita semestral de mantenimiento preventivo de hardware y software tendrá como plazo máximo de duración 30 días calendario para aplicar el mantenimiento a todos los equipos de los centros de datos y los kits de captura, producción y entrega de documentos de identidad y pasaportes. |  |  |
| **Horarios para los mantenimientos preventivos** | El Proveedor deberá considerar que los horarios para ejecución de los mantenimientos preventivos en los centros de datos y centros de producción de documentos de identidad y pasaportes serán fuera de la jornada laboral (pasadas las 18H00 y cuando amerite fines de semana o feriados), tanto en el Ecuador como en el extranjero.  El mantenimiento de las estaciones de captura de datos y entrega de cédulas y pasaportes deberá ejecutarse preferentemente fuera del horario laboral o durante la jornada laboral previa autorización expresa de los responsables de agencia o puntos de atención sin afectar la prestación de los servicios a los ciudadanos.  La DIGERCIC podrá modificar el horario de los mantenimientos preventivos, previa notificación al Proveedor con al menos 24 horas de anticipación. |  |  |
| **Modalidad del mantenimiento preventivo** | El Proveedor deberá aplicar los mantenimientos preventivos de forma presencial y/o remota, así como también físicos o lógicos, tomando en cuenta las siguientes definiciones:   | **ITEM** | **LUGAR** | **TIPO DE**  **MANTENIMIENTO** | **MODALIDAD** | **RESPONSABLE** | | --- | --- | --- | --- | --- | | Hardware y Software instalados en los Centros de Datos. | Ecuador  (Quito y Guayaquil) | Físico de hardware y lógico de software | En sitio | Proveedor | | Equipos y software de captura, producción y entrega de documentos de identidad o pasaportes | Ecuador  (agencias DIGERCIC, Oficina del MREMH en -Quito) | Físico de hardware y lógico de software | En sitio | Proveedor | | Equipos y software de captura, producción y entrega de documentos de identidad o pasaportes | Extranjero (MREMH consulados de Madrid y New York) | Físico de hardware y lógico de software | En sitio | Proveedor | | Equipos y software de captura y entrega | Extranjero (MREMH: consulados, no incluye Madrid y New York) | Lógico de software | Remoto | Proveedor | | Equipos y software de captura y entrega | Extranjero (MREMH: consulados, no incluye Madrid y New York)) | Físico de hardware | En sitio | Personal técnico de soporte del MREMH con apoyo remoto del Proveedor |   La DIGERCIC y/o el MREMH facilitarán al Proveedor el acceso remoto a los equipos involucrados, para que se realice el respectivo mantenimiento lógico. |  |  |
| **Informe técnico del mantenimiento preventivo** | El Proveedor emitirá un Informe Técnico por cada agencia, consulado o punto de atención, que contendrá:   * Punto de atención de la DIGERCIC o el MREMH en el cual se realizó el mantenimiento. * Componentes de hardware y software a los cuales se realizó el mantenimiento preventivo tanto físico como lógico. * Fecha y hora de inicio del mantenimiento. * Fecha y hora de fin del mantenimiento. * Datos de contacto del técnico(s) del Proveedor que ejecutaron el mantenimiento preventivo. * Datos de contacto del técnico(s) de la DIGERCIC o el MREMH que supervisaron el mantenimiento preventivo. * Detalle de las tareas realizadas. * Archivo fotográfico por cada equipo o periférico al que se le aplicó mantenimiento. * Estado en el que quedan los componentes de hardware y software luego del mantenimiento preventivo (operando normalmente, operando con observaciones, otro). * El original del Acta de Entrega-Recepción de equipos, cuando corresponda por reemplazo. * Conclusiones * Recomendaciones * Anexos * Firmas de responsabilidad del informe técnico. |  |  |
| **Mano de obra, insumos, transporte, otros para la prestación del mantenimiento preventivo** | La mano de obra, los insumos, materiales, partes, piezas o equipos, transporte y cualquier otro rubro requerido para la prestación del servicio de mantenimiento preventivo, correrán por cuenta del Proveedor, sin costo adicional para la DIGERCIC. |  |  |

**E.2) MANTENIMIENTO CORRECTIVO DE HARDWARE Y SOFTWARE**

| **CARACTERÍSTICAS Y CONDICIONES REQUERIDAS POR LA DIGERCIC** | | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| --- | --- | --- | --- |
| **Actividades del mantenimiento correctivo** | El mantenimiento correctivo es un conjunto de acciones técnicas que el Proveedor ejecutará para recuperar el funcionamiento normal de uno o varios componentes de hardware y/o software del SEDIP, cuando se presente un incidente, problema, error o fallo.  El mantenimiento correctivo puede implicar la ejecución de actividades detalladas en el mantenimiento preventivo y otras, hasta solventar la situación de excepción (incidente, problema, error o fallo) y dejar el componente completamente operativo en condiciones de funcionamiento normal. |  |  |
| **Modalidad para el mantenimiento correctivo** | El Proveedor deberá realizar el mantenimiento correctivo de forma presencial y/o remota, tomando en cuenta las siguientes consideraciones:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ÍTEM** | **LUGAR** | **TIPO DE**  **MANTENIMIENTO** | **MODALIDAD** | **RESPONSABLE** | | Hardware y Software instalados en los Centros de Datos. | Ecuador  (Quito y Guayaquil) | Físico de hardware y lógico de software | En sitio | Proveedor | | Equipos y software de captura, producción y entrega de documentos de identidad o pasaportes | Ecuador  (agencias DIGERCIC, Oficina del MREMH en Quito) | Físico de hardware y lógico de software | En sitio o remoto de hardware y/o software. Entrega en sitio de repuestos, partes, piezas o equipos. | Proveedor | | Equipos y software de captura, producción y entrega de documentos de identidad o pasaportes | Extranjero (MREMH consulados de Madrid y New York) | Físico de hardware y lógico de software | En sitio o remoto de hardware y/o software. Entrega en sitio de repuestos, partes, piezas o equipos. | Proveedor | | Equipos y software de captura y entrega de documentos de identidad o pasaportes | Extranjero (MREMH consulados, no incluye New York y Madrid) | Físico de hardware y lógico de software | Remoto de hardware y/o software.  Entrega de equipos a la DIGERCIC para envío al consulado por medio del MREMH. | Proveedor | |  |  |
| **Horario para la prestación del servicio de mantenimiento correctivo (atención de incidentes o problemas)** | El Proveedor deberá prestar el servicio de mantenimiento correctivo en horario 24x7x365 (24 horas, los 7 días de la semana, los 365 días del año). |  |  |
| **Reporte o notificación de un incidente, problema, error o fallo (situación de excepción)** | El personal técnico de la DIGERCIC o del MREMH responsable de notificar incidentes, problemas, errores o fallos, relacionados con el funcionamiento de los componentes de hardware y/o software del SEDIP, utilizará como medio oficial de comunicación con el Proveedor la Mesa de Soporte de TIC de la DIGERCIC ([soportic@registrocivil.gob.ec](mailto:soportic@registrocivil.gob.ec)). |  |  |
| **Mano de obra, herramientas, materiales, insumos, transporte, otros para la prestación del servicio de mantenimiento correctivo** | La mano de obra especializada, las herramientas, materiales, insumos y otros requeridos para la prestación del servicio de mantenimiento correctivo corren de cuenta del Proveedor, sin costo adicional para la DIGERCIC.  El traslado de equipos, suministros, partes yo/ piezas a nivel nacional, así como también a New York o Madrid estarán a cargo del Proveedor, sin costo adicional para la DIGERCIC. |  |  |
| **Equipos, partes y piezas para el mantenimiento correctivo** | El Proveedor para solventar el incidente, dando cumplimiento a los tiempos establecidos en los Niveles de Servicio, podrá reemplazar, de forma temporal, un equipo que presente fallas por uno de su propiedad, de similares o mejores características. En este caso, el equipo de la DIGERCIC o MREMH que presentó fallas deberá ser arreglado y restituido por el Proveedor en un plazo máximo de30 días calendario. Los costos de transporte y de logística de este equipo corren de cuenta del Proveedor.  Los equipos, repuestos, partes y piezas que se requieran para recuperar el funcionamiento normal de los equipos correrán de cuenta del Proveedor, sin costo adicional para la DIGERCIC. |  |  |
| **Reemplazo o restitución definitiva de equipos** | Los equipos que reemplazan de forma definitiva a los que presentan daños irreparables deberán ser nuevos, de fábrica (no re manufacturados), de la misma marca y de características técnicas iguales o superiores.  Si el Proveedor requiere reemplazar de forma definitiva un equipo en el Ecuador, este equipo deberá ser entregado en la DIGERCIC (Quito Matriz) para el trámite correspondiente de alta y codificación del bien. Una vez cumplido con este trámite, el Proveedor deberá trasladarlo a la Agencia o punto de atención asumiendo los costos de traslado y logística.  Si el Proveedor requiere reemplazar de forma definitiva un equipo en los consulados de Ecuador en New York o Madrid, este equipo deberá ser entregado en dichos consulados. El Proveedor debe entregar toda la documentación pertinente y el Acta de Entrega Recepción a la DIGERCIC (Quito Matriz) en el plazo máximo de 15 días después de la suscripción del Acta, para que la DIGERCIC realice el trámite correspondiente de alta y codificación del bien.  Si el Proveedor requiere reemplazar de forma definitiva un equipo en los otros consulados de Ecuador en el mundo, este equipo deberá ser entregado en la DIGERCIC (Quito Matriz) para el trámite correspondiente de alta y codificación del bien. Una vez cumplido con este trámite, la DIGERCIC lo entregará al MREMH (Quito) para que lo remita por valija diplomática al consulado correspondiente; los costos del traslado serán asumidos por el MREMH.  La DIGERCIC, a petición del Proveedor, podrá autorizar la restitución de un equipo con entrega directa por parte del Proveedor en un determinado consulado; en cuyo caso el Proveedor entregará toda la documentación y el Acta de Entrega Recepción a la DIGERCIC (Quito Matriz) en el plazo máximo de 15 días después de la suscripción del Acta para que la DIGERCIC pueda realizar el procedimiento de alta y codificación del bien. |  |  |
| **Equipos de respaldo** | Se considera conveniente que el Proveedor para cumplir con los Niveles de Servicio disponga de un stock de equipos que permitan reemplazar a los existentes de manera temporal, a fin de recuperar el servicio en el menor tiempo posible. |  |  |
| **Cierre de una situación de excepción (incidente, problema, error o fallo)** | La situación de excepción (incidente, problema, error, fallo) se considerará cerrada cuando el Proveedor cierre el ticket correspondiente en la Mesa de Soporte de TIC de la DIGERCIC adjuntando las evidencias del caso. |  |  |
| **Número de notificaciones o reportes de incidentes, problemas, errores o fallos** | Durante el periodo de vigencia del contrato, la DIGERCIC y el MREMH podrán generar los requerimientos tecnológicos que sean necesarios para reportar incidentes, problemas, errores o fallos en los componentes sujetos de este servicio; no existirá límite. |  |  |
| **Atención de incidentes, problemas, errores o fallos** | El Proveedor asignará uno o varios técnicos para evaluar, diagnosticar y solucionar un incidente, problema, error o fallo reportado o notificado por la DIGERCIC o el MREMH. Los técnicos asignados por el Proveedor deberán ejecutar acciones correctivas, observando y aplicando las recomendaciones y estándares del fabricante o de la industria |  |  |
| **Informe Técnico Individual de mantenimiento correctivo por incidente, problema, error o fallo** | El Proveedor deberá elaborar un Informe Técnico por cada incidente, problema, error o fallo reportado que se presente en un componente sujeto de este servicio. El informe deberá ser recibido y avalado mediante la firma del Técnico de la DIGERCIC o el MREMH que acompañe, supervise y verifique la ejecución.  El Informe Técnico contendrá al menos:   * Agencia/consulado o centro de datos en el cual se realizó el mantenimiento correctivo. * Fecha y hora de inicio en la que se ejecutó el mantenimiento. * Fecha y hora de fin del mantenimiento. * Número de requerimiento generado a través de la Mesa de Soporte de TIC de la DIGERCIC. * Hardware y/o software sujeto del mantenimiento: marca, modelo, número de serie, código institucional, versión, fabricantes, etc. * Descripción de la situación de excepción atendida. * Procedimiento aplicado para solucionar la situación de excepción. * Detalle de los repuestos (materiales, partes, piezas, componentes o equipos completos) utilizados efectivamente para solucionar el incidente (en caso de aplicar). * Conclusiones y recomendaciones para asegurar que la situación de excepción no se vuelva a presentar. * Apellidos, nombres y firmas de los servidores de la DIGERCIC y/o del MREMH que reciben el servicio y del técnico del Proveedor que ejecutó este servicio. * Tiempo en el cual el Proveedor respondió a la notificación inicial de la situación de excepción (historia del ticket)   El Proveedor deberá presentar el Informe Técnico máximo en 72 horas luego del cierre de requerimiento. |  |  |
| **Informe Ejecutivo periódico de mantenimiento correctivo** | El Proveedor deberá presentar a la DIGERCIC un Informe Ejecutivo relacionado con el mantenimiento correctivo, dentro de los 10 días calendarios posteriores a la finalización del mantenimiento preventivo. El informe contendrá como mínimo:   * Un cuadro consolidado de los incidentes, problemas, errores o fallos atendidos. * Un cuadro consolidado de equipos, partes y/o piezas reemplazadas. * Observaciones generales relacionadas con la ejecución del mantenimiento correctivo. * Conclusiones y recomendaciones generales relacionadas con la ejecución del mantenimiento correctivo. * Firmas de responsabilidad del informe ejecutivo.   A este Informe Ejecutivo se deben adjuntar las copias de los Informes Técnicos Individuales de mantenimiento correctivo. El informe deberá presentarse junto con el Informe Técnico del Mantenimiento Preventivo.  El Informe Ejecutivo periódico de mantenimiento correctivo también se presentará al finalizar el contrato, para la suscripción del Acta de Entrega-Recepción Final. |  |  |

**E.3) GESTIÓN DE INCIDENTES Y PROBLEMAS**

Los incidentes, problemas, errores, fallos o requerimientos de soporte técnico especializado relacionados al SEDIP serán gestionados a través de la Mesa de Soporte de TIC de la DIGERCIC, como medio de comunicación único y oficial con el equipo de soporte del Proveedor.

Se definen 3 niveles de gestión de soporte para atender incidentes y problemas:

* Nivel 1 (N1) 🡪 Técnicos de soporte informático de la DIGERCIC o del MREMH (dependiendo del caso). Los técnicos N1 del MREMH abrirán tickets a la Mesa de Soporte de TIC de la DIGERCIC desde la Mesa de Ayuda del MREMH.
* Nivel 2 (N2) 🡪 Técnicos informáticos especialistas de la DIGERCIC.
* Nivel 3 (N3) 🡪 Personal técnico del Proveedor.

|  |  |  |
| --- | --- | --- |
| **CARACTERÍSTICAS Y CONDICIONES REQUERIDAS POR LA DIGERCIC** | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| El Proveedor deberá delegar a los técnicos que accederán a la Mesa de Soporte de TIC de la DIGERCIC, para garantizar la atención de incidentes y problemas en modalidad 24x7x365 de forma global (en el Ecuador y en el extranjero).  Las atenciones de incidentes, problemas generados deberán ser solventados a través de mantenimientos correctivos de hardware y software.  Por cada incidente o problema que se presente en el SEDIP y que el Proveedor lo solvente o solucione en un tiempo superior al establecido en los niveles de servicio citados en el ámbito de mantenimiento correctivo, se aplicarán las multas correspondientes.  Los técnicos designados por el Proveedor deberán gestionar la atención de los incidentes, problemas, errores, fallos y solicitudes de soporte técnico especializado mediante la Mesa de Soporte de TIC de la DIGERCIC ([soportic@registrocivil.gob.ec](mailto:soportic@registrocivil.gob.ec)), que será el único punto de contacto para gestión del soporte y la contabilización de tiempos de atención.  Los técnicos que delegue el Proveedor serán creados como usuarios de la Mesa de Soporte de TIC de la DIGERCIC.   * **Procedimiento General para la Gestión de Incidentes o problemas**   A continuación, se describe los pasos a seguir para la solución de incidentes:   * Los técnicos de soporte informático del MREMH o de la DIGERCIC (N1) serán los encargados de realizar el diagnóstico inicial y reportar el incidente a través de [soportic@registrocivil.gob.ec](mailto:soportic@registrocivil.gob.ec) e informar a los técnicos N2 y/o N3. Es necesario que la información proporcionada en el requerimiento emitido, sea clara, describiendo el error, daño, problema o fallo lo más detallado posible. Se deberán anexar logs, reportes, datos de pruebas, capturas de pantalla resaltando errores, mensajes, datos, etc. * Si el incidente puede ser solucionado en N1, el técnico asignado facilitará el tratamiento correspondiente y el respectivo cierre al requerimiento; caso contrario lo escalará a N2 o N3, según sea el caso. * N2 una vez revisado el incidente, podrá escalar directamente a N3, cuando la solución a un incidente no esté a su alcance. * En caso de que el incidente haya llegado a N3, el Proveedor deberá diagnosticar y solucionar el incidente dentro de los tiempos establecidos en los niveles de servicio. En caso que, el Proveedor incumpla los niveles de servicio, se contabilizará el tiempo para aplicar las multas correspondientes. Durante un incidente notificado al Proveedor, este deberá mantener informados a los niveles N1 y N2 sobre los avances realizados. * Una vez solucionado el incidente, este será cerrado copiando a todos los involucrados. Posteriormente se procederá a la elaboración del informe respectivo, conforme a lo solicitado por la DIGERCIC. * **Consideraciones del procedimiento de gestión de incidentes y de los servicios post implementación:** * El Proveedor deberá entregar y hacer aprobar a la DIGERCIC (Administrador del contrato), hasta los primeros 15 días laborables de ejecución del contrato, el procedimiento para notificar o reportar y gestionar incidentes, problemas, errores o fallos tanto a nivel de hardware como de software, incluyendo listas de distribución y niveles de escalamiento. * El Proveedor deberá presentar y hacer aprobar a la DIGERCIC (Administrador del Contrato), hasta los primeros 15 días laborables de ejecución del contrato, los siguientes formatos:   + - Formatos de informes técnicos individuales y ejecutivos.     - Formatos de acta de entrega recepción de equipos.     - Formatos de documentación relacionada con la implementación del sistema (arquitectura física y lógica, informes de pruebas, manuales). * La DIGERCIC será la responsable de socializar estos procedimientos y formatos con los Técnicos de la DIGERCIC y el MREMH de ser el caso; así como también de verificar el cumplimiento de los mismos. * **Representantes del Proveedor a los cuales la DIGERCIC reporte un caso de no atención o incumplimiento.**   El Proveedor deberá especificar los datos de contacto de al menos tres representantes jerárquicos a los cuales se deberá escalar, en caso de la no atención de un incidente, problema, error, fallo o incumplimiento de requerimientos relacionados con la prestación del servicio.  Los datos mínimos que deberá especificar el Proveedor de esos contactos son: apellidos y nombres, cargo, número de teléfono celular, número de teléfono convencional, correo electrónico empresarial/trabajo, dirección de lugar de trabajo. |  |  |

* **Niveles de Servicio**

El Proveedor deberá observar los siguientes Niveles de Servicio para la solución de incidentes, problemas, errores o fallos en los componentes de hardware y/o software que afecten la disponibilidad o degraden el rendimiento de los servicios de emisión de documentos de identidad y/o pasaportes tanto a nivel de las agencias de la DIGERCIC como de los consulados del MREMH.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. ***COMPONENTES DE HARDWARE Y/O SOFTWARE IMPLEMENTADOS EN LOS CENTROS DE DATOS***  * **NIVELES DE CRITICIDAD**  | **CRITICIDAD** | **DESCRIPCIÓN** | | --- | --- | | Alta (A) | No se puede capturar datos, producir o entregar documentos de identidad o pasaportes en el Ecuador y en el exterior porque los equipos y/o el software de los centros de cómputo del sistema presentan fallos o errores. | | Media (M) | Existe lentitud o intermitencia en la captura de datos, producción o entrega de documentos de identidad o pasaportes en el Ecuador y en el exterior) porque los equipos y/o el software de los centros de cómputo del sistema presentan fallos o errores. | | Baja (B) | Se puede capturar datos, producir o entregar documentos de identidad o pasaportes en el Ecuador y en el exterior pero alguno de los equipos y/o software de los centros de cómputo del sistema presentan fallos o errores o alertas. |   ***Nota:*** Un incidente producido por afectaciones en el servicio de redes o comunicaciones o los centros de datos no será imputable al Proveedor.   * **NIVELES DE SERVICIO**  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Servicio** | **Lugar** | **Tipo** | **Componente afectado** | **Criticidad** | **NIVEL 3: PROVEEDOR** | | | | **Tiempo de respuesta a la notificación de incidente** | **Tiempo de solución desde la notificación del incidente** | | | **EMISION DE PASAPORTES Y/O DOCUMENTOS DE IDENTIDAD** | Centros de Datos | HW | SEDIP, ABIS, PKI, PKD, HSM | A | Hasta 1 hora | Hasta 4 horas | | M | Hasta 6 horas | | B | Hasta 24 horas | | SW | SEDIP, ABIS, PKI, PKD, HSM | A | Hasta 1 hora | Hasta 2 horas | | M | Hasta 4 horas | | B | Hasta 24 horas |   *Dónde:* HW: Hardware, SW: Software, A: Alta; M: Media; B: Baja.   1. ***COMPONENTES DE HARDWARE Y/O SOFTWARE IMPLEMENTADOS PARA LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD Y/ PASAPORTES***  * **NIVELES DE CRITICIDAD**  | **CRITICIDAD** | **DESCRIPCIÓN** | | --- | --- | | Alta (A) | No se puede producir documentos de identidad o pasaportes en el Ecuador y en el exterior porque los equipos y/o el software del sistema dejan de funcionar. | | Media (M) | Existe lentitud o intermitencia en la producción de documentos de identidad o pasaportes en el Ecuador y en el exterior porque los equipos y/o el software del sistema presentan degradación en su funcionamiento o rendimiento.  No se puede producir documentos de identidad o pasaportes en un centro de producción en el Ecuador o en el exterior porque los equipos y/o el software del sistema dejan de funcionar. | | Baja (B) | Se presentan alertas en los equipos y/o software del sistema sin afectar la producción de documentos de identidad y pasaportes. |   ***Nota:*** Un incidente producido por afectaciones en el servicio de redes o comunicaciones o de los centros de datos no será imputable al Proveedor.   * **NIVELES DE SERVICIO**  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Servicio** | **Sitio** | **Tipo** | **Componente afectado** | **Criticidad** | **NIVEL 3: PROVEEDOR** | | | | **Tiempo de respuesta a la notificación ante incidente** | **Tiempo de solución desde la notificación del incidente** | | | **PASAPORTES / DOCUMENTOS DE IDENTIDAD** | Centros de producción de la DIGERCIC y MREMH | HW | Equipos, Impresoras, componentes del kit de producción de pasaportes y de documentos de identidad | M | Hasta 1 hora | Hasta 6 horas en Quito y Guayaquil.  Hasta 24 horas en el resto de ciudades del Ecuador continental.  Hasta 48 horas en Galápagos.  Hasta 24 horas en los consulados de Madrid y New York | |  |  | | B | Hasta 24 horas en Quito y Guayaquil.  Hasta 48 horas en el resto de ciudades del Ecuador continental y Galápagos.  Hasta 48 horas en los consulados de Madrid y New York | | Centros de producción de la DIGERCIC y MREMH | SW | SEDIP, Software base (sistema operativo, antivirus, otros) | A | Hasta 1 hora | Hasta 3 horas | | M | Hasta 5 horas | | B | Hasta 24 horas |   *Dónde:* HW: Hardware; SW: Software; A: Alta; M: Media; B: Baja.   1. ***COMPONENTES DE HARDWARE Y/O SOFTWARE DE LOS KITS DEL SEDIP PARA LA CAPTURA DE DATOS Y ENTREGA DE DOCUMENTOS DE IDENTIDAD Y/ PASAPORTES***  * **NIVELES DE CRITICIDAD**  | **CRITICIDAD** | **DESCRIPCIÓN** | | --- | --- | | Alta (A) | No se puede capturar datos y/o entregar documentos de identidad o pasaportes por daños de hardware y/o software presentados en uno o varios kits de captura o entrega. | | Media (M) | Uno o varios kits tienen algún componente de hardware y/o software que presenta limitaciones, daños o fallas que afectan la operación, pero no impiden, en las agencias o puntos de atención, la captura de datos y/o entrega de documentos de identidad o pasaportes. | | Baja (B) | Los kits tienen algún componente de hardware y/o software que presenta alarmas o notificaciones de error. |  * **NIVELES DE SERVICIO**  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Servicio** | **Sitio** | **Tipo** | **Componente afectado** | **Criticidad** | **NIVEL 3: PROVEEDOR** | | | | **Tiempo de respuesta a la notificación ante incidente o fallo (en horas laborables)** | **Tiempo de Solución (en horas laborables)** | | | **PASAPORTES / DOCUMENTOS DE IDENTIDAD** | Agencias de la DIGERCIC y MREMH en Ecuador | HW | Kits de captura de datos y entrega de documentos de identidad y pasaportes | A | Hasta 1 hora | Hasta 8 horas, en Quito y Guayaquil Hasta 24 horas en el resto de ciudades del Ecuador continental Hasta 48 horas en Galápagos | | M | Hasta 24 horas, en Quito y Guayaquil Hasta 48 horas en el resto de ciudades del Ecuador continental Hasta 72 horas en Galápagos. | | B | Hasta 72 horas en Ecuador continental y Galápagos | | Agencias del MREMH en el extranjero (Consulados) | HW | Kits de captura de datos y entrega de documentos de identidad y pasaportes | A | Hasta 1 hora | Hasta 24 horas | | M | Hasta 48 horas | | B | Hasta 72 horas | | Agencias de la DIGERCIC y MREMH (Quito y Consulados) | SW | Software de las estaciones de captura de datos y entrega de documentos de identidad y pasaportes | A | Hasta 1 hora | Hasta 6 horas | | M | Hasta 8 horas | | B | Hasta 24 horas |     *Dónde:* HW: Hardware; SW: Software; A: Alta; M: Media; B: Baja.   * **CONSIDERACIONES** * La DIGERCIC y/o el MREMH facilitarán al Proveedor el acceso remoto a los equipos que presenten incidentes, problemas, errores o fallos. * Si para solucionar un incidente, el proveedor requiere reemplazar o restituir de forma definitiva un equipo; el incidente se cerrará con la entrega del equipo a la DIGERCIC. * El tiempo de respuesta a la notificación de incidente y tiempo de solución desde la notificación del incidente está expresado en horas continuas. * El Proveedor deberá actualizar e informar a la DIGERCIC el estado de avance de la solución a través de la Mesa de Soporte de TIC. * El incumplimiento de los niveles de servicio por parte del Proveedor ocasionará multas que serán descontadas en el pago correspondiente. | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |

**E.4) SOPORTE TÉCNICO ESPECIALIZADO**

| **CARACTERÍSTICAS Y CONDICIONES REQUERIDAS POR LA DIGERCIC** | | **CUMPLE**  **(SI / NO)** | **INDICAR**  **PÁGINAS(S)**  **OFERTA** |
| --- | --- | --- | --- |
| **Actividades del servicio de soporte técnico especializado** | El soporte técnico especializado consiste en un paquete de 80 horas anuales de soporte técnico especializado acumulables, mismas que iniciarán después de que haya finalizado el despliegue del SEDIP, a ser proporcionadas por el Proveedor en aspectos relacionados con la administración, gestión, afinamiento y productividad de cualquier componente de hardware y/o software del sistema. La DIGERCIC puede hacer uso de estas horas cuando así lo requiera. |  |  |
| **Modalidad para el soporte técnico** | El Proveedor proporcionará soporte técnico especializado de forma presencial en las oficinas o centros de datos de Quito o Guayaquil o de forma remota de acuerdo a las necesidades de la DIGERCIC. |  |  |
| **Horario para la prestación del servicio de soporte técnico especializado** | El Proveedor deberá prestar el servicio de soporte técnico especializado en horario 9x5x12 (Las 9 horas laborables de la DIGERCIC en Ecuador, los 5 días laborables de cada semana, los 12 meses del año). |  |  |
| **Reporte o notificación de requerimiento de soporte técnico especializado** | La DIGERC solicitará al Proveedor la atención a un requerimiento de soporte técnico especializado, por medio de la Mesa de Soporte de TIC. |  |  |
| **Tiempo de respuesta ante un requerimiento de soporte técnico especializado (Nivel de Servicio)** | El Proveedor deberá atender el requerimiento de soporte técnico especializado en máximo dos días laborables contados a partir de la notificación del requerimiento. |  |  |
| **Mano de obra, insumos, transporte, otros para la prestación del servicio de soporte técnico especializado** | La mano de obra especializada, equipos, herramientas, materiales, insumos, transporte y otros ítems requeridos para la prestación del servicio de soporte técnico especializado correrán por cuenta del Proveedor, sin costo adicional para la DIGERCIC. |  |  |
| **Cierre de requerimiento de soporte técnico especializado** | El soporte técnico especializado se considerará cerrado cuando el Proveedor cierre el ticket correspondiente en la Mesa de Soporte de TIC de la DIGERCIC adjuntando las evidencias del caso. |  |  |
| **Informe Técnico Individual de soporte técnico especializado** | El Proveedor emitirá un Informe Técnico por cada requerimiento de soporte técnico especializado. El informe deberá ser recibido y avalado mediante la firma del funcionario de la DIGERCIC que solicitó el soporte técnico especializado.  El Informe Técnico contendrá, como mínimo:   * Número de requerimiento generado a través de la Mesa de Soporte de TIC. * Fecha y hora de inicio en la que se ejecutó el soporte técnico. * Fecha y hora de fin del soporte técnico. * Número de horas empleadas. * Descripción del soporte proporcionado. * Conclusiones y recomendaciones generales. * Apellidos, nombres y firmas de los servidores de la DIGERCIC que reciben el servicio y del Técnico del Proveedor que ejecutó este servicio.   El Proveedor deberá presentar el Informe Técnico máximo en 72 horas luego del cierre de requerimiento de soporte técnico especializado.  Copias de estos informes deberán adjuntarse al Informe Ejecutivo de soporte técnico especializado. |  |  |
| **Informe Ejecutivo periódico de soporte técnico especializado** | El Proveedor deberá presentar a la DIGERCIC junto con los Informes Ejecutivos de Mantenimiento Preventivo y Correctivo, el Informe Ejecutivo periódico relacionado con la prestación del servicio de soporte técnico especializado que contendrá:   * Un cuadro consolidado de los requerimientos de soporte técnico atendidos. * El número total de horas de soporte consumidas en el periodo y el saldo de horas disponibles para el año en el cual se ejecute el soporte.   A este Informe Ejecutivo deberán adjuntarse las copias de los Informes Técnicos Individuales de Soporte Técnico Especializado.  Este Informe Ejecutivo periódico de soporte técnico especializado también se presentará al finalizar el contrato, para la suscripción del Acta de Entrega Recepción Final. |  |  |
| **Aprobación de procedimiento para el soporte técnico especializado** | El Proveedor deberá entregar y hacer aprobar a la DIGERCIC (Administrador del contrato), hasta los primeros 15 días laborables de ejecución del contrato, el procedimiento para la atención de soporte técnico especializado. |  |  |

**E.5) ACTUALIZACION TECNOLOGICA DEL SISTEMA**

|  |  |  |
| --- | --- | --- |
| **CARACTERÍSTICAS Y CONDICIONES REQUERIDAS POR LA DIGERCIC** | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| Para asegurar la actualización y vigencia tecnológica del SEDIP, el Proveedor deberá entregar con el cronograma de mantenimiento preventivo el listado de actualizaciones de hardware (drivers, firmware, otros) y software(parches de seguridad, actualizaciones, nuevas versiones, herramientas liberadas por el fabricante)de los componentes del SEDIP, ABIS, PKI, componentes de los kits de captura, producción y entrega de documentos de identidad y pasaportes.  La DIGERCIC autorizará la aplicación de las actualizaciones durante las visitas de mantenimiento preventivo sin costos adicionales para la DIGERCIC durante la vigencia del contrato  Para actualización de componentes de software base como pueden ser: sistemas operativos, bases de datos, software de virtualización, servidores de aplicaciones, etc.; o de gestión del ABIS o la PKI, el proveedor deberá coordinar dichas actualizaciones en el ambiente de pruebas previo a la implementación en el ambiente de producción.  La DIGERCIC tendrá el derecho de instalar actualizaciones de software en sus diferentes componentes debido a que las licencias y/o suscripciones deberán ser contratadas a nombre de la DIGERCIC, bajo regímenes de mantenimiento y actualización por 3 años. |  |  |

**E.6) GESTION DEL CAMBIO**

|  |  |  |
| --- | --- | --- |
| **CARACTERÍSTICAS Y CONDICIONES REQUERIDAS POR LA DIGERCIC** | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * Se deberá poder administrar y/o parametrizar diferentes funcionalidades del SEDIP para evitar cambios al código fuente del sistema y dependencia de marcas y modelos de componentes de hardware y/o software para la captura de datos, así como la producción y entrega de documentos. Por ejemplo, instalar otra marca y modelo de impresora, o personalizar un nuevo modelo de chip o añadir un campo al documento de identidad, entre otros, debe ser factible cambiar/parametrizar en el sistema, bajo límites razonables. * Los diseños (layouts) de la sección visual de los documentos deberán poder ser cambiados de acuerdo a nuevos requerimientos que la DIGERCIC y/o el MREMH deban aplicar. Si el SEDIP no incorpora funcionalidad para cumplir este requisito, el proveedor quedará obligado a realizar el cambio por su cuenta para incorporar o eliminar campos en la sección visual de los documentos por hasta 4 veces durante la vigencia del contrato.   La DIGERCIC deberá realizar el pedido formal del cambio anexando la documentación respectiva. La DIGERCIC no pagará costos adicionales por este tipo de requerimientos. El proveedor tendrá hasta 60 días calendario para implementar, probar y pasar a producción el cambio. Cualquier cambio a la personalización gráfica de los documentos deberá ser implementado y probado previamente en el ambiente de pruebas por parte del proveedor. El proveedor deberá actualizar la documentación operativa y técnica para documentar el cambio realizado.   * La codificación electrónica de los chips deberá ser flexible para adaptarse a nuevas marcas y modelos de chip, nuevas versiones de sistemas operativos de los chips, nuevos materiales de tarjetas para documentos de identidad y/o de páginas de datos de libretas de pasaportes, y para añadir/eliminar datos a codificar,   El SEDIP podrá tener un módulo específico para gestionar la personalización electrónica de los documentos; o interfaces que traduzcan el lenguaje de bajo nivel de la personalización electrónica a un lenguaje de alto nivel (ej., XML o Java).  Si el SEDIP no incorpora funcionalidad para cumplir este requisito, el proveedor quedará obligado por su cuenta a realizar los cambios al software de personalización hasta 4 veces durante la vigencia del contrato. La DIGERCIC deberá realizar el pedido formal del cambio anexando la documentación respectiva. La DIGERCIC no pagará costos adicionales por este tipo de requerimientos. El proveedor tendrá hasta 60 días calendario para implementar, probar y pasar a producción el cambio. Cualquier cambio a la personalización electrónica de los documentos deberá ser implementado y probado previamente en el ambiente de pruebas por parte del proveedor. El proveedor deberá actualizar la documentación operativa y técnica para registrar el cambio.   * La instalación, configuración y puesta en operación de equipos de captura, producción y entrega de diferentes marcas y modelos de manufactura reconocida en el mercado internacional.   Si el SEDIP no incorpora funcionalidad para cumplir este requisito, el proveedor quedará obligado a realizar la integración por su cuenta de equipos cuyos modelos o marcas no sean soportados directamente por el sistema hasta 4 veces durante la vigencia del contrato. La DIGERCIC no pagará costos adicionales por este tipo de requerimientos. La DIGERCIC deberá realizar el pedido formal del cambio anexando la documentación respectiva. El proveedor tendrá hasta 60 días calendario para implementar, probar y pasar a producción el cambio. Cualquier integración de equipos de marcas y/o modelos diferentes a los suministrados para los kits de captura, producción deberá ser implementada y probada previamente en el ambiente de pruebas solicitado por parte del proveedor. El proveedor deberá actualizar la documentación operativa y técnica para registrar el cambio. |  |  |

**INFORMES DE LOS SERVICIOS POST-IMPLEMENTACION**

|  |  |  |
| --- | --- | --- |
| **CARACTERÍSTICAS Y CONDICIONES REQUERIDAS POR LA DIGERCIC** | CUMPLE  (SI / NO) | INDICAR  PÁGINAS(S)  OFERTA |
| * **Entrega de Informes al Administrador del Contrato**   El Proveedor deberá entregar los informes de los servicios de post-implementación de la siguiente manera:   * Al menos dos ejemplares impresos por cada informe. * Dos medios magnéticos (DVD o CD) que contengan los informes en formato no editable (PDF) y en formato editable (DOC, DOCX, ODF, ODT, otro). * **Aprobación de informes**   Los informes que deberá presentar el proveedor como parte de la prestación de los servicios de post-implementación estarán sujetos a la aprobación por parte de la DIGERCIC. En caso de que éstos no estén a conformidad, el proveedor deberá re-elaborar los mismos hasta que estén a satisfacción de la DIGERCIC.  Dentro del tiempo máximo establecido para la entrega cada informe, estará incluido el tiempo necesario para que el proveedor coordine con la DIGERCIC su aprobación. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **ACCION** | **CARGO** | **FIRMA** | **FECHA** |
| **APROBADO POR** | ING. CLAUDIO PRIETO  SUBDIRECTOR DE REGISTRO CIVIL E IDENTIFICACIÓN |  |  |
| **ELABORADO Y REVISADO POR** | ING. JAIME SAENZ  DIRECTOR DE INFRAESTRUCTURA Y OPERACIONES  COORDINACIÓN GENERAL DE TIC |  |  |
| ING. MANUEL PLASENCIA  DIRECTOR DE SOPORTE E INTEROPERABILIDAD  COORDINACIÓN GENERAL DE TIC |  |  |
| ING. LENIN LIZANO  GERENTE DEL PROYECTO SEDIP  DIRECTOR DE PLANIFICACIÓN E INVERSIÓN  COORDINACIÓN GENERAL DE PLANIFICACION |  |  |
| ING. DANIEL BECERRA  DIRECTOR DE SERVICIO DE CEDULACION, ENCARGADO  COORDNINACIÓN GENERAL DE SERVICIOS |  |  |

1. En inglés ICAO: International Civil Aviation Organization [↑](#footnote-ref-1)
2. EMRTD: Electronic Machine Readable Travel Document [↑](#footnote-ref-2)
3. Véase: https://www.icao.int/publications/pages/publication.aspx?docnum=9303 [↑](#footnote-ref-3)
4. Véase: https://www.icao.int/Security/FAL/TRIP/Pages/default.aspx [↑](#footnote-ref-4)
5. AFIS: Automated Fingerprint Identification System [↑](#footnote-ref-5)
6. PKI: Public Key Infraestructure [↑](#footnote-ref-6)
7. ABIS: Automated Biometric Identification System [↑](#footnote-ref-7)
8. PKI: Public Key Infraestructure [↑](#footnote-ref-8)
9. BAC: Basic Access Control [↑](#footnote-ref-9)
10. SAC: Supplemental Access Control [↑](#footnote-ref-10)
11. CSCA: Country Signature Certifying Authority [↑](#footnote-ref-11)
12. DS: Document Signers [↑](#footnote-ref-12)
13. nPKD: Directorio de Claves Públicas Nacional [↑](#footnote-ref-13)
14. La “Agencia Virtual” de la DIGERCIC es una aplicación Web que ofrece servicios o trámites electrónicos en-línea a los ciudadanos. Está disponible en: https://apps.registrocivil.gob.ec/portalCiudadano/index.jsf [↑](#footnote-ref-14)
15. ISO: International Standard Organization [↑](#footnote-ref-15)
16. NIST: National Institute of Standards and Technology [↑](#footnote-ref-16)
17. Véase: https://www.nist.gov/itl/iad/image-group/fpvte-2012 [↑](#footnote-ref-17)
18. Véase: https://www.nist.gov/itl/iad/image-group/face-recognition-vendor-test-frvt-2013 [↑](#footnote-ref-18)
19. HSM: Hardware Security Module [↑](#footnote-ref-19)
20. SIEM: Security Information and Event Management [↑](#footnote-ref-20)