**Anexo Técnico**

Unidad de Ingeniería Tecnológica Institucional

Coordinación de Atención a la Continuidad Operativa de Plataformas Aplicativas

**“Derecho de Uso del Componente de Enrolamiento y**

**Verificación Biométrica Facial para el Instituto Mexicano del**

**Seguro Social”**

**Control de versiones del documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Descripción** | **Responsable** |
| 0.1 | 08/11/2024 | Elaboración del documento | José Antonio Martínez Sánchez |
| 0.2 | 14/11/2024 | Revisión del documento | Fausto Mario Díaz Cabrera |
| 1.0 | 21/11/2024 | Aprobación del documento | Arturo Ortiz Peña |

1. **Objetivo del documento**

Documento que contiene requerimientos técnicos que la Coordinación de Atención a la Continuidad Operativa de Plataformas Aplicativas, estima conveniente para la prestación del servicio de “Derecho de Uso del Componente de Enrolamiento y Verificación Biométrica Facial para el Instituto Mexicano del Seguro Social”, con la calidad y oportunidad requeridos por las citadas unidades administrativas del Instituto.

1. **Clave CUCoP.**

|  |  |  |
| --- | --- | --- |
| **Clave CUCoP** | **Partida Específica** | **Descripción** |
| 32700003 | 32701 | Licencias de uso de programas de cómputo y su actualización |

1. **Objetivo**

El objetivo del servicio de “Derecho de Uso del Componente de Enrolamiento y Verificación Biométrica Facial para el Instituto Mexicano del Seguro Social”, será la de verificar la identidad de los derechohabientes y/o usuarios del Instituto Mexicano del Seguro Social por medio de la testificación biométrica y biográfica ante la base de datos del Instituto Nacional Electoral (INE) por medio de la captura de la biometría facial y los datos de la credencial para votar así como disponer de un mecanismo de validación biométrico para el acceso y uso del servicio de Cédula Digital en Salud, en la aplicación Móvil IMSS Digital (AMID).

1. **Antecedentes**

A través de la aplicación Móvil IMSS Digital (AMID), el Instituto Mexicano del Seguro Social (IMSS) otorga a sus derechohabientes 16 servicios a distancia, sin ser necesario asistir de forma presencial, lo cual permite otorgar un servicio eficiente y eficaz de manera digital, siendo una de las aplicaciones de gobierno federal más utilizadas.

Actualmente la AMID requiere fortalecer mediante mecanismos de seguridad biométrica que permitan garantizar el acceso a los servicios que lo requieran como lo es el servicio de cédula digital en salud, bajo un esquema de autenticación y control de accesos de identificación personal de características físicas (biométricos).

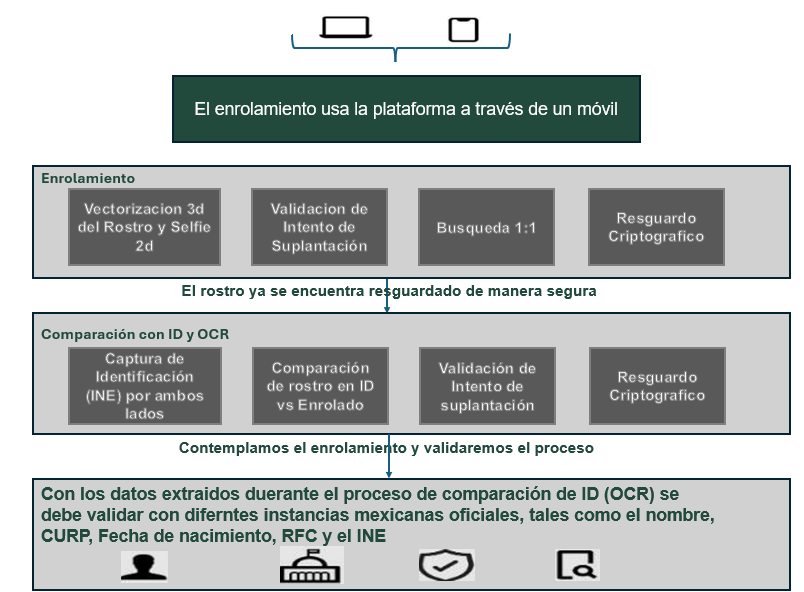
El Instituto Mexicano del Seguro Social como prestador de servicios de seguridad social, requiere garantizar con certeza que los derechohabientes y/o usuarios se identifiquen y autentiquen con base en un conjunto de datos reconocibles y verificables, que sean únicos en cada persona, por lo que se hace necesario la contratación de un servicio integral de enrolamiento y validación de identidad de sus derechohabientes y/o usuarios con la finalidad de hacer validaciones de identidades confiables, de forma segura y prevenir cualquier tipo de fraude con lo cual se le permita el acceso al servicio de cédula digital en salud desde el Aplicativo Móvil IMSS Digital.

1. **Descripción de los servicios solicitados**
   1. **Solución Conceptual**

Se requiere de una solución integrable por medio de API’s y/o SDK’s que permitan realizar la captura biométrica facial de los derechohabientes y/o usuarios del Instituto Mexicano del Seguro Social a través de la Aplicativo Móvil IMSS Digital el cual se encarga de realizar las peticiones de consulta de datos biográficos y biométrico facial ante el Instituto Nacional Electoral (INE), además que permita el enrolamiento facial una vez validada la identidad para autenticar posteriormente a los derechohabientes y/o usuarios por medio del servicio de cédula digital a través de la Aplicativo Móvil IMSS Digital,

.

* 1. **Arquitectura Conceptual**



Un dibujo en blanco y negro

Descripción generada automáticamente con confianza bajaImagen en blanco y negro

Descripción generada automáticamente con confianza media

**Enrolamiento**

**Comparación con ID y OCR**

**Con los datos extraídos durante el proceso de comparación de ID (OCR) se debe validar con diferentes instancias mexicanas oficiales, tales como el nombre, CURP, Fecha de nacimiento, RFC y el INE**

**Vectorización 3d del rostro y Selfie 2d**

**Validación de Intento de suplantación**

**Búsqueda 1:1**

**Resguardo Criptográfico**

**Captura de Identificación (INE) por ambos lados**

**Comparación de rostro en ID vs Enrolado**

**Validación de Intento de suplantación**

**Resguardo Criptográfico**

**El rostro ya se encuentra resguardado de manera segura**

**Contemplamos el enrolamiento y validaremos el proceso**

El proveedor, deberá de entregar un software de biometría facial que permita proteger la información sensible de los derechohabientes y/o usuarios, así como sus biométricos faciales, que pueda consultar los datos contenidos en la credencial para votar y de los biométricos (facial) que ofrece el INE, cumpliendo así con los estándares de seguridad y privacidad, en apego a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Datos Personales en Posesión de Sujetos Obligados.

La Coordinación de Atención a la Continuidad Operativa de Plataformas Aplicativas, será la encargada de proporcionar técnicamente todos los accesos necesarios al proveedor a fin de que éste, configure y entregue funcionando el software de biometría facial en los servidores del Instituto que este le indique.

El alcance de este requerimiento no contempla que el proveedor realice la implementación del software de biometría facial en servicio cédula digital en salud dentro de la aplicación Móvil IMSS Digital (AMID).

La funcionalidad de la solución será implementada por el Instituto en la aplicación Móvil IMSS Digital y en el servicio antes mencionado para fortalecer los mecanismos de identificación de los derechohabientes y/o usuarios, así como poder consumir los servicios de verificación de datos contenidos en la credencial para votar y de datos biométricos (facial) que ofrece el INE. Misma que tendrá interacción con la plataforma web para la administración y el registro del proceso de enrolamiento de los derechohabientes y/o usuarios por parte del Instituto. Ambas interfaces deberán proporcionar una experiencia de usuario intuitiva y fácil de usar.

Se requiere que el proveedor proporcione el Derecho de Uso del Componente de Enrolamiento y Verificación Biométrica Facial para el Instituto Mexicano del Seguro Social, con la consulta de los servicios de verificación de datos contenidos en la credencial para votar y los biométricos faciales que ofrece el INE, para el fortalecimiento del mecanismo de registro seguro al servicio de cédula digital en salud en la aplicación Móvil IMSS Digital, que se pondrá a disposición por parte del Instituto Mexicano del Seguro Social a sus derechohabientes y/o usuarios.

* 1. **Descripción del servicio de Derecho de Uso del Componente de Enrolamiento y Verificación Biométrica Facial para el Instituto Mexicano del Seguro Social**
* Servicio de enrolamiento biométrico
* Servicio de verificación biométrica facial con consulta al INE
* Servicio de soporte técnico.

* + 1. **Servicio de enrolamiento biométrico**

1. Enrolamiento biométrico**.**
   * Para la prestación del enrolamiento e identificación biométrica, el proveedor deberá otorgar el servicio requerido para el del enrolamiento biométrico en tiempo y forma, la cual deberá quedar concluida al 100% dentro de los primeros 60 días naturales, a partir del día siguiente a la notificación del fallo.
   * El enrolamiento facial deberá permitir al IMSS generar un mapa en el servicio de autenticación biométrica, 3D del rostro de cada uno de sus derechohabientes y/o usuarios en un formato que le permita ejecutar posteriores validaciones de identidad.
   * El IMSS tendrá que visualizar en una plataforma web el procedimiento de cada uno de los derechohabientes y/o usuarios enrolados.
   * Se requiere que la información generada durante la vigencia del contrato permita la compatibilidad y el uso de la base de datos de los rostros validados con otros proveedores de software de biometría facial, sin necesidad de un re-enrolamiento de derechohabientes y/o usuarios, por lo que el proveedor deberá realizar la entrega de las bases de datos en comento, en el formato estandar interoperable que le indique el Instituto a fin de que no sea exclusivo para un solo proveedor.

* + Para efectos de claridad a los licitantes, el proceso de enrolamiento se considerará tal, cuando se ejecute al menos uno de los procesos que se detallan en la tabla del numeral 5.2 denominada “Arquitectura conceptual” que se detalle en el recuadro “Enrolamiento”, y es independiente si el proceso concluyó en un enrolamiento o si dicho proceso es desechado por la identificación de algún intento de fraude/suplantación en alguna de las etapas previas. El proveedor deberá de considerar en su costo de enrolamiento biométrico facial con uso de verificaciones ilimitadas por el año de servicio que tenga vigencia este contrato.

1. Matcheo/coincidencia de los rostros de los derechohabientes y/o usuarios con su credencial para votar, expedida por el Instituto Nacional Electoral (INE).
   * La solución biométrica de reconocimiento facial deberá verificar el rostro obtenido durante el enrolamiento y comparar las características faciales de su cara, contra la presentada en la fotografía de la credencial para votar.
   * La respuesta esperada de este cotejo deberá presentar un porcentaje o nivel de coincidencia, el cual deberá establecerse entre un rango de 0 a 100%
   * El tiempo óptimo de respuesta deberá estar en promedio de 10 segundos, para tal efecto, el proveedor deberá manifestar bajo cuáles condiciones o restricciones dará cumplimiento.
   * Servicio asíncrono, esto se refiere a la capacidad de procesar la información de manera no secuencial.
2. Prueba de vida en tiempo real.
   * El mundo virtual es escenario de constantes ataques, fraudes y suplantaciones de identidad, en consecuencia, para que un proceso de verificación de identidad sea seguro y fiable, tiene que completarse con una prueba de vida en tiempo real, que asegure que la persona que realiza el proceso no está cometiendo algún tipo de fraude de identidad.

Es decir, verifica que se trate de una persona real y no un intento de fraude como fotos, máscaras 3D, videos o técnicas de deep fake (es un video, una imagen o un audio generado que imita la apariencia y el sonido de una persona), la solución deberá ejecutar al momento de la realización del enrolamiento facial, una prueba de vida en tiempo real, para garantizar que el derechohabiente y/o usuario esté en tiempo real frente a la cámara.

La solución deberá proveer detección de cualquier tipo de falsificación facial ya sea física (máscaras) o digital (rostros en videos).

* + El tiempo óptimo de respuesta deberá estar en promedio 4 segundos, para tal efecto el proveedor deberá manifestar bajo cuáles condiciones o restricciones dará cumplimiento.
  + Servicio síncrono, esto quiere decir que el procesamiento se ejecuta en tiempo real.

1. Validación de la credencial para votar en lista nominal del Instituto Nacional Electoral (INE).
   * Se requiere que la funcionalidad de la solución permita al Instituto validar que la identificación oficial del usuario esté registrada en el padrón electoral del Instituto Nacional Electoral, y que coincida con los datos de la identificación.
2. [[1]](#footnote-1)OCR de la credencial para votar.
   * Se requiere que el INE sea capturada a través de la cámara trasera del teléfono móvil con una interfaz intuitiva y que auxilie al usuario durante el proceso de captura por medio de guías visuales y textos con instrucciones claras.
   * Se requiere que todos los datos mostrados en la identificación como lo son: el nombre, apellido paterno y materno, CURP, sexo, fecha de nacimiento, vigencia, número OCR y CIC sean extraidos en un formato JSON.
   * El OCR deberá funcionar con todos los tipos de identificaciones emitidas por el Instituto Nacional Electoral, válidos actualmente (tipo D, E, F, G y H).El tiempo óptimo de respuesta deberá estar en promedio 7 segundos, para tal efecto el proveedor deberá manifestar bajo cuáles condiciones o restricciones dará cumplimiento.
   * Servicio síncrono, esto quiere decir que el procesamiento se ejecuta en tiempo real.
3. Anti spoofing de credencial para votar.
   * La solución deberá proveer tecnología anti spoof (técnica de detección de suplantación de identidad) de la credencial de elector, que permita detectar alteraciones en la misma, así como el cambio de letras o de la fotografía de la persona, mediante las respuestas que sean obtenidas a través del Servicio de Verificación Facial del INE y las alertas que deberá configurar el Proveedor con base a esas repuestas.
4. Plataforma web de visualización de datos de enrolamiento.
   * Se deberá proporcionar una plataforma web, la cual deberá ser instalada en los servidores que el IMSS le indique, y en la cual únicamente el Instituto podrá visualizar todos los rostros de los derechohabientes y/o usuarios enrolados, así como la verificación de los datos de la credencial para votar y los contenidos multimedia generados por el proceso de la toma de una selfi y la fotografía de la credencial para votar por la parte frontal y trasera de la misma. Los usuarios y roles deberán ser determinados por el IMSS de acuerdo con el uso. Esta plataforma deberá permitir la generación de reportes de acuerdo con la información que se vaya generando y se encuentre registrada en la plataforma web.
5. Autenticación facial de derechohabientes y/o usuarios.

* El IMSS requiere que el software de biometría facial permita a los derechohabientes y/o usuarios autenticarse cada vez que estos lo requieran, desde el dispositivo móvil, después de registrar sus características faciales (enrolamiento). Para ello, se deberá implementar un esquema de identificación por derechohabiente y/o usuario el cual iniciará a partir de la fecha de su enrolamiento y hasta la conclusión de la vigencia del respectivo contrato.

El enrolamiento facial deberá permitir al IMSS generar un mapa en 3D del rostro de cada uno de sus derechohabientes y/o usuarios en un formato que le permita ejecutar posteriores validaciones de identidad.

El software permitirá a los derechohabientes y/o usuarios enrolados validar su rostro con ayuda de la cámara frontal de su celular en lugar de escanear reiteradamente su credencial para votar. La autenticación facial de los derechohabientes y/o usuarios deberá ser por medio de una validación biométrica local.

* + 1. **Servicio de verificación biométrica facial con consulta al INE**

El proveedor deberá ofrecer el servicio de verificación de datos contenidos en la credencial para votar y de datos biométricos (faciales) a través del INE para lo cual debe incluir un algoritmo de comparación que reconozca los datos biométricos conforme a los estándares y políticas del INE.

Este algoritmo debe contar con las siguientes funcionalidades:

1. Se requiere utilizar modelos de inteligencia artificial para realizar la verificación de identidad. No se aceptarán proveedores que usen revisiones manuales en ningún caso. Los umbrales de aceptación y rechazo automático deberán definirse entre las partes en el plan detallado para la implementación del servicio.
2. Se deberá de cumplir con los parámetros solicitados ante el NIST (Instituto Nacional de Estándares y Tecnología NIST por sus siglas en inglés, National Institute of Standards and Technology) .
3. Se deberá de contar con la modalidad MUGSHOT, con una evaluación FALSA TASA DE NO COINCIDENCIA (FALSE NON-MATCH RATE – FNMR) menor o igual a 0.0025, en la Prueba de proveedor de reconocimiento facial uno a uno (Face Recognition Vendor Test 1:1 Verification), como indicado en la página web https://pages.nist.gov/frvt/html/frvt11.html .
4. Se deberá de contar con la configuración del canal punto a punto para él envió de sobres digitales encriptados los cuales contienen la información del usuario consumidor; este canal será suministrado por el proveedor.
5. Se requiere proporcionar un mecanismo que impida que el IMSS sobrepase el nivel de servicio (verificaciones máximas por minuto) contratado.
6. Se requiere que la solución contemple el uso de un Servicio Web encargado de recibir las solicitudes enviadas por las terminales de consulta del IMSS, el cual devolverá como respuesta la coincidencia de la verificación de los datos recibidos respecto de los datos de la base de datos de “EL INE” y el porcentaje de similitud de los datos biométricos (facial) enviados, según sea el caso.
7. Se deberá comprobar que el proveedor se apega a las especificaciones técnicas que solicita el INE respecto de los equipos de seguridad perimetral, enlace de comunicaciones, así como la infraestructura de cómputo y software necesario para la operación y administración de las aplicaciones para realizar las consultas y control de las verificaciones de datos, mediante carta bajo protesta de decir verdad suscrita por el representante legal del proveedor y descripción en la arquitectura técnica que pueda validar el cumplimiento de lo antes mencionado.
8. El proveedor será responsable de proporcionar la infraestructura tecnológica necesaria para el adecuado funcionamiento del servicio, con base en lo establecido en las especificaciones técnicas, considerando que el IMSS operará el servicio en el nivel 7, de acuerdo con las políticas del INE para este servicio.
9. Se requiere contar con la capacidad tecnológica para un nivel de disponibilidad de este servicio cuyo mínimo sea del 98% de disponibilidad mensual para este servicio.
10. Se requiere otorgar al IMSS documentación referente al consumo del servicio de la verificación de los datos biográficos y biométricos de la credencial para votar del INE.
11. Se deberá de contar con la entrega de la infraestructura de los servidores, suscripciones para licencias red hat, suscripción de Base de datos y licencia de bus criptográfico que solicita el INE para la operación a nivel 7.
12. Se requiere presentar dentro de su propuesta técnica, en forma impresa un escrito en hoja membretada y firmado por el representante legal, en el que manifieste contar con la autorización de realizar, la estructuración y control del servicio de infraestructura e implementación de licencias y garantías para el correcto funcionamiento de los servicios de Suscripción para el uso del sistema de consultas ante el INE.
13. Se requiere presentar dentro de su propuesta técnica, en forma impresa un escrito en hoja membretada y firmado por el representante legal, en el que manifieste contar con la autorización de realizar, la estructuración, control y envío de solicitudes de validación de datos ante el INE.
14. Se deberá entregar dentro **30 días hábiles**, contados a partir de la notificación de la adjudicación, la infraestructura, suscripciones y software necesario para la operación a nivel 7 en las Instalaciones del INE (aplicable para la subpartida 1. “Servicio de soporte técnico de la base existente de biometría facial para las autenticaciones”) y administración de las aplicaciones para las consultas de verificación y validación de identidad ante el INE, mismos que tendrán una vigencia hasta la conclusión del contrato.
15. Se deberá iniciar al día natural posterior a la fecha de conclusiónde los servicios de aprovisionamiento de infraestructura e implementación, los servicios de validación de identidad ante el INE, mismos que tendrán una vigencia hasta la conclusión del contrato.
16. Se deberá proveer el servicio de conectividad en todos los ambientes que sean acordados entre IMSS e INE.
17. Se requiere que las peticiones de validación sean cifradas y firmadas, conforme a los requerimientos del INE e IMSS.

1. Se deberá incluir el servicio de HSM (Hardware Security Module) conforme a las especificaciones técnicas del INE mismo que deberá instalarse donde el IMSS lo indique.
2. Se requiere que el proveedor gestione, administre e implemente los enlaces de telecomunicaciones punto a punto entre el INE y donde el IMSS especifique, conforme a las especificaciones técnicas del INE a los 15 días hábiles después de firmado el contrato.
3. Se requiere que el proveedor cuente con el servicio FUNCIONALIDAD WEB SERVICE (UNO A UNO) para las validaciones de datos individuales del INE, por lo que deberá presentar en su propuesta técnica un escrito preferentemente en hoja membretada y firmado por el representante legal, en donde manifieste que cuenta con el servicio y funciones conforme a lo establecido con en el Servicio de Verificación facial del INE.
4. Se deberá permitir al IMSS el acceso y disposición sin restricciones a la información y datos comprendidos en la solución objeto del contrato.
   * 1. **Servicio de soporte técnico.**

El Instituto requiere que el proveedor proporcione el soporte técnico a la solución implementada en la Cédula Digital en Salud, de la Aplicación Móvil IMSS Digital, en la Coordinación de Atención a la Continuidad Operativa de Plataformas Aplicativas.

El soporte técnico del servicio de Derecho de Uso del Componente de Enrolamiento y Verificación Biométrica Facial para el Instituto Mexicano del Seguro Social considera lo siguiente:

1. Soporte de gravedad las veinticuatro horas del día, los siete días de la semana 24x7 durante toda la vigencia del contrato.
2. El soporte deberá ser provisto con base en lo señalado en el numeral 5 “Descripción de los servicios solicitados” descrito en el presente Anexo Técnico.
3. Parches de actualización (Parches) para los componentes del servicio solicitado.
4. Registro de tickets de servicio (Service Request, SR) con gravedad 1 (7x24), para lo cual el proveedor deberá indicar cuál es la liga de conexión y el debido procedimiento, para que el Instituto levante los requerimientos de servicio que este requiera y de seguimiento hasta su conclusión.
5. Asistencia para asuntos no técnicos durante un horario de las 09:00 am a las 18:00 pm. (por ejemplo, asistencia para clarificar procesos de tipo administrativo o de gestión de los servicios proporcionados por el proveedor).
6. Asistencia telefónica, en un horario de atención para el IMSS las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato.
7. Asistencia técnica vía remota o web según lo determine el IMSS. La asistencia remota se efectuará cuando el IMSS requiera consultar o solicitar un mejor diagnóstico.
8. Los niveles de gravedad de las solicitudes de servicio conforme a la asistencia técnica (Service Request) deberá ser clasificado, dependiendo la forma en la que impacta al negocio del IMSS.
9. Derecho de Asistencia Técnica en sitio, en caso de ser necesario y a petición del IMSS.
10. Identificación y solución de fallas a manera de mantenimiento correctivo, deberán cumplir con 98% de disponibilidad del servicio, debiendo presentar el siguiente reporte:

**j.1**. Reporte mensual de cumplimiento de disponibilidad de los niveles

de servicio.

El administrador del contrato deberá identificar el nivel de gravedad del incidente que en su caso se llegue a presentar como se indica en la siguiente tabla:

|  |  |  |  |
| --- | --- | --- | --- |
| **Niveles de gravedad** | **Gravedad 1**  El software de producción fundamental no funciona. | **Gravedad 2**  Fallo de función o característica principal grave. | **Gravedad 3**  Fallo de función o característica secundaria intermedio. |
| Descripción de los niveles de gravedad | 1. El software de producción está gravemente afectado o completamente inoperativo, o 2. Las operaciones del software o aplicaciones de misión crítica no funcionan. | 1. El software funciona con capacidades limitadas, o 2. Es inestable, con interrupciones periódicas, o 3. A pesar de no verse afectadas, las aplicaciones de misión crítica han sufrido importantes interrupciones del software. | El software es plenamente operativo, pero se han observado errores que no afectan a la posibilidad de uso del software. |
| Tiempo de respuesta | **1 hora** | **4 horas** | **8 horas** |

*Tabla 1. Niveles de gravedad.*

Los servicios de soporte técnico que en su caso requieran de acceso físico al Instituto (personal técnico especializado del proveedor), deberán estar habilitados durante la vigencia del servicio y del contrato.

Con base en los procesos tecnológicos institucionales, que en su caso sean aplicables al servicio de derecho de uso del componente de enrolamiento y verificación biométrica facial para el Instituto Mexicano del Seguro Social. El proveedor deberá documentar y gestionar sin costo para el Instituto, los entregables referidos en la tabla 2 de los términos y condiciones que soporten la prestación de sus servicios.

El administrador del contrato deberá dar a conocer al proveedor en un plazo no mayor a 10 días hábiles posteriores al día siguiente a la notificación del fallo, los procesos tecnológicos compartidos en el Instituto Mexicano del Seguro Social que en su caso le apliquen al servicio requerido.

**Actividades enunciativas más no limitativas del servicio de soporte técnico en tecnología de biometría facial.**

1. El proveedor del servicio será identificado como tal en el Convenio de Colaboración que al efecto del Instituto Mexicano del Seguro Social celebre con el Instituto Nacional Electoral.
2. El proveedor debe describir en su propuesta los prerrequisitos de integración, instalación, configuración y/o puesta a punto del servicio a proporcionar en aplicaciones y/o sistemas del IMSS. Siendo el equipo técnico del IMSS quien será encargado de las integraciones y habilitaciones de las aplicaciones y/o sistemas del IMSS; debiendo considerar la participación del proveedor como apoyo técnico en caso de ser requerido.
3. Asistencia en la integración del SDK y API en el Aplicativo Móvil IMSS Digital, para el servicio de cédula digital en salud.
4. Análisis y aplicación de parches de actualización (Parches) para los componentes del servicio solicitado.
5. Asistencia y orientación en la instalación, configuración y soporte técnico proactivo especializado relativo al software biométrico facial.
6. A solicitud del Instituto las partes (el proveedor y el Instituto) deberán participar en reuniones de trabajo.
7. Comunicar los procedimientos y pautas apropiadas a seguir, para rastrear y documentar requerimientos del servicio.
8. Asistencia en la recuperación del repositorio de contenido en caso de corrupción de la información del IMSS utilizando procedimientos y herramientas que solamente están disponibles para el reconocimiento biométrico facial.
9. Escalamiento directo en caso de incidentes críticos por parte de personal autorizado del IMSS, a ejecutivos del proveedor para acelerar la solución de estos.
10. En caso de fallas, acceso directo a personal de soporte técnico global del fabricante, así como también a los grupos de atención de clientes críticos.
11. Análisis y afinación del desempeño del biométrico facial.
12. Planeación y actividades de recuperación del biométrico facial en caso de desastres.
13. Evaluación (Assessment) para la creación e implementación de procedimientos de respaldo y recuperación de los componentes del biométrico facial.
14. Análisis y Aplicación de Fixes y Bundles para el producto biométrico facial.
15. Asistencia y orientación para lograr un uso eficiente del producto de biométrico facial.
16. Evaluación y análisis (Assessment) de la arquitectura del biométrico facial del IMSS para proponer futuras mejoras y optimizaciones.
17. Acompañamiento y asistencia técnica para la administración del servicio de derecho de uso del componente de enrolamiento y verificación biométrica facial para el Instituto Mexicano del Seguro Social.

|  |  |  |  |
| --- | --- | --- | --- |
| **Servicio de derecho de uso del componente de enrolamiento y verificación biométrica facial para el instituto mexicano del seguro social.** | | | |
| Número | Componente | Enrolamientos mínimos | Enrolamientos máximos |
| **1** | **Servicio** | **2,800,000** | **7,000,000** |

*Tabla 2. Mínimos y máximos requeridos.*

**1.** **Servicio de soporte técnico de la base existente de biometría facial para las autenticaciones.**

El proveedor deberá dar soporte técnico integral para las bases de datos existentes tales como biométrica y biográfica, por lo que podrá solicitar al administrador del contrato la información general que de forma razonable requiera para su respectivo soporte, mismo que de forma enunciativa mas no limitativa describe su atención:

* Mantenimiento preventivo y correctivo.
* Actualización de software y firmware en caso de requerirse.
* Gestión de infraestructura asociada al servicio de soporte de la base de datos existente.
* Atención de incidencias relacionadas con el acceso y la operación del sistema.

**2. Mantenimiento de la Infraestructura**

**2.1** El proveedor gestionará y optimizará los recursos de infraestructura asociados a la base de datos, tales como:

* Servidores físicos o virtuales.
* Almacenamiento y backup de datos.
* Redes y conexiones para garantizar la accesibilidad y redundancia del servicio.

**2.2** El proveedor se encargará de monitorear de manera continua los componentes biométricos instalados en los servidores, a fin de identificar posibles fallos o caídas de rendimiento, implementando las acciones necesarias para evitar interrupciones en el servicio.

**2.3** En caso de que la infraestructura sea proporcionada por un tercero, el Proveedor colaborará estrechamente con el proveedor externo para garantizar el cumplimiento de los niveles de servicio acordados.

**3. Mantenimiento Preventivo y Correctivo**

**3.1** El proveedor llevará a cabo actividades de mantenimiento preventivo con una frecuencia semestral, para garantizar el correcto funcionamiento y optimización de la base de datos de plantillas biométricas.

**3.2** Cualquier intervención de mantenimiento correctivo será realizada tan pronto como se detecte una falla o anomalía que comprometa el rendimiento, seguridad o disponibilidad del sistema.

**3.3** Todas las actividades de mantenimiento deberán realizarse en una ventana de mantenimiento coordinada con el Instituto Mexicano del Seguro Social.

**4. Auditorías y Monitoreo**

**4.1** El proveedor implementará sistemas de monitoreo de la solución biométrica en sus propios servidores y deberá reportar comportamientos anómalos en la base de datos o accesos no autorizados. En caso de que se detecte una brecha de seguridad, el Proveedor notificará al Instituto Mexicano del Seguro Social a la brevedad posible para que coordine las acciones necesarias.

1. **Requerimientos Técnicos**

**No funcionales**

1. El licitante deberá manifestar en su propuesta técnica que la solución que ofrece al IMSS, en relación con la tecnología de biométrica, funciona en dispositivos móviles con recursos de hardware y software limitados, presentan la siguiente funcionalidad:
   * Funcionamiento con Android 9 en adelante.
   * Funcionamiento con iOS 15 en adelante.
   * Funcionamiento con dispositivos desde 1 GB de RAM.
   * Funcionamiento en navegadores modernos como Edge, Chrome, Mozilla, Opera y Safari, que entren en la categoría Evergreen.
   * Funcionamiento con cámaras desde 2 Megapíxeles.
   * Soporte de Openshift Container Platform para el funcionamiento del componente biométrico facial.
2. Integración mediante API y SDK en caso de ser requerido, compatible con el framework Xamarin.
3. La solución deberá ser en formato On Premise, por lo cual el proveedor deberá llevar a cabo la Instalación y configuración en infraestructura del centro de datos del Instituto Mexicano del Seguro Social.
4. Los precios deberán ser expresados en pesos mexicanos MXN, sin IVA.

**Funcionales**

El servicio de soporte técnico deberá mantener la operación del Servicio de derecho de uso del componente de enrolamiento y verificación biométrica facial para el Instituto Mexicano del Seguro Social bajo niveles de operación cubiertos las 24 horas del día, los siete días de la semana, (7x24) durante la vigencia del contrato que ampare el citado servicio incluyendo soporte en sitio tanto en oficina como en el centro de datos del IMSS, que se indique.

Se requiere que el Servicio de derecho de uso del componente de enrolamiento y verificación biométrica facial para el Instituto Mexicano del Seguro Social solicitado en el presente anexo permita el uso de la base de datos de rostros generados con otras tecnologías de biometría facial, sin necesidad de un re-enrolamiento de sus derechohabientes y/o usuarios.

1. **Pruebas**

La Coordinación de Atención a la Continuidad Operativa de Plataformas Aplicativas, no requiere de pruebas para el Servicio de derecho de uso del componente de enrolamiento y verificación biométrica facial para el Instituto Mexicano del Seguro Social, la garantía de la funcionalidad del software biométrico se encuentra estandarizada en el mercado considerado la normalización estandarizada de productos que se encuentran regulados bajo la International Organization for Standardization (ISO) - ISO 30107-3 en nivel 2 por sus siglas en inglés.

Una vez concluida la implementación de la infraestructura y garantías para la operación en nivel 7 del INE, “el proveedor” efectuará con el IMSS la ejecución de las pruebas necesarias para la debida operación de los servicios a través de la Infraestructura de Telecomunicaciones implementadas en este servicio, con el objeto de determinar si las condiciones de operación son adecuadas, dichas pruebas serán coordinadas al interior del IMSS por el área encargada del proyecto.

1. **Niveles de servicio acordados que deberán cumplirse**

El Instituto ingresará las solicitudes de servicio de soporte técnico de acuerdo con la gravedad del incidente en curso a través del portal web del proveedor.

Una vez implementada la solución descrita en el presente documento, este deberá realizar el proceso completo de enrolamiento y deberá cumplir con la verificación tal y como se describe en Anexo, no obstante, el proveedor deberá considerar los tiempos de respuesta mencionados en la Tabla 1. “Niveles de gravedad” y proporcionar la atención que en tiempo y forma se describen en la misma.

1. **Requerimientos de arquitectura tecnológica**

No aplica.

1. **Restricciones e Interfaces con otros elementos**

El proveedor deberá manifestar con un escrito firmado por el representante legal, que dará cumplimiento a los requisitos que derivan de las disposiciones emitidas por el Instituto Nacional Electoral para la verificación de datos faciales, son enunciativos más no limitativos, las acciones serán coordinadas por el IMSS.

1. **Transición del servicio**

Previo a la conclusión del contrato, el proveedor que resulte adjudicado deberá realizar la transferencia del servicio de regreso al “Instituto”, o a un tercero que este designe, para ello, deberá de haber proporcionado la documentación, entregables y servicios descritos en la Tabla 4. Entregables de la fase de transición de los términos y condiciones.

La documentación deberá incluir la información que se generó durante la vigencia del contrato, debidamente actualizada, en consideración los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar del “Instituto”. Adicionalmente en esta fase el “proveedor” entregará la base de conocimientos generada durante las fases de operación.

**En el caso de terminación anticipada o de finalización de la vigencia del contrato**, "el proveedor" que resulte adjudicado, será responsable de iniciar el proceso de respaldo de la información, del proceso de baja, y de realizar los movimientos de resguardo, traslado y empaquetado de los respaldos propiedad del “Instituto” al lugar donde indique la entidad.

En su caso el retiro podrá ser realizado en coordinación con la entrega de un nuevo contrato, prestador de servicios o solución que dará continuidad a la operación del “Instituto”, observando los acuerdos operativos de migración que de un contrato a otro sean necesarios, y que consideren aspectos como la configuración del servicio, contraseñas y documentación necesaria para la adecuada toma de control y administración de parte del nuevo grupo y asegurando la continuidad operativa de los servicios.

Una vez adjudicado el siguiente contrato o al mismo Instituto, el proveedor actual deberá revisar el plan de trabajo propuesto por el nuevo proveedor adjudicado o en su caso el Instituto contando con diez días hábiles a partir de la recepción de dicho plan para observar y/o aceptar las fechas en las que deberá entregar la información y retirar la infraestructura. Se deberá de firmar una minuta de acuerdos entre ambos proveedores, el saliente y el entrante.

1. **En caso de que se requieran pruebas, deberá indicar el método de evaluación.**

En lo referente al punto anterior, se aclara que por la naturaleza del servicio requerido dicho supuesto, no aplica.

1. **En aquellos casos en que el Área Requirente modifique la especificación técnica de algún bien que no se encuentre regulado por el Compendio Nacional de Insumos para la Salud.**

Por la naturaleza del servicio requerido, no aplica.

1. **En aquellos casos en que el Área Requirente, modifique las especificaciones técnicas de un bien respecto de las estipuladas en el ejercicio anterior, deberá presentar un dictamen en el que justifique que los requisitos contenidos en las especificaciones técnicas del bien no limitan de ninguna forma la libre participación, concurrencia y competencia económica.**

Por la naturaleza del servicio requerido, no aplica.

1. **Normas: Oficial Mexicana, Estándar (antes Mexicana), Internacional, de Referencia o Especificación Técnica, que resulte aplicable a los servicios requeridos**

No se requieren certificaciones de normas oficiales mexicanas o internacionales (NOMS).

No obstante, se verificará que el algoritmo de comparación esté evaluado por el NIST en el listado de pruebas de proveedores de reconocimiento facial. Aparecer en los últimos 2 años en el Reporte NIST FRVT, disponible en el siguiente enlace: https://pages.nist.gov/frvt/html/frvt11.html.

Asimismo, la prueba de vida deberá contar con la garantía de la funcionalidad del software biométrico se encuentra estandarizada en el mercado considerado la normalización estandarizada de productos que se encuentran regulados bajo la International Organization for Standardization (ISO) - ISO 30107-3 en nivel 2 por sus siglas en inglés

1. **Perfil del Prestador de Servicios.**

El proveedor deberá presentar en su propuesta técnica un escrito  firmado por el representante legal, donde manifieste que su objeto social, actividades comerciales, profesionales y experiencia para la implementación de los servicios que están relacionadas con la prestación de los servicios que se requieren en el presente Anexo Técnico, la cantidad de años que lleva prestando servicios relacionados con la propuesta solicitada (anexando documentos probatorios para ser evaluados), que cuenta con la capacidad técnica, administrativa, financiera y legal para realizar los citados servicios en la forma y tiempos establecidos en el presente anexo técnico.

El proveedor deberá presentar la siguiente información sobre su organización:

* Descripción general de la empresa.
* Nombre de la empresa y dirección de sus oficinas.
* Describir los antecedentes de la empresa.
* Premios y reconocimientos.
* Certificaciones.

El personal encargado del mantenimiento y soporte, vinculado a esta contratación, deberá estar avalado mediante una carta expedida por el proveedor donde manifieste el conocimiento de los servicios ofertados, así como de las aplicaciones que correspondan para el funcionamiento correcto del enlace de comunicación para pago de cuotas de recuperación por consultas al INE, la cual deberá formar parte de su propuesta Técnica.

El proveedor tecnológico deberá estar actualmente habilitado por el INE, dentro de su Directorio de proveedores aprobados para ofrecer este tipo de servicios

El proveedor deberá contar con experiencia para la implementación de los servicios citados en este Anexo Técnico”.

1. **Documentación que acredite el cumplimiento de los requerimientos del servicio.**

El proveedor deberá proporcionar la evaluación del NIST del motor biométrico para proveer el servicio de consulta de biometría facial con prueba de vida, a efecto de realizar verificaciones biométricas y biográficas ante la base de datos biométrica del Instituto Nacional Electoral (INE), indicando la versión del algoritmo implementado, mediante una carta bajo protesta de decir verdad firmada por el representante legal del proveedor.

El posible licitante deberá realizar una carta bajo protesta de decir verdad, en la que se relacionen y adjunten al menos tres contratos íntegros suscritos con clientes del sector gubernamental o privado, pero al menos acreditando uno en gobierno en el sector Salud. Estos contratos deben evidenciar la implementación de aplicaciones para la verificación de datos de la credencial para votar del INE y de biometría facial. Al menos uno de estos contratos debe tener un mínimo de 750,000 enrolamientos biométricos faciales. Se deben anexar documentos probatorios a efectos de ser evaluados.

El posible licitante deberá demostrar que al menos dos de los tres contratos que demuestren que ha implementado la solución, se encuentren operando en ambiente productivo.

**SUBPARTIDA 1.1: Servicio de instalación y garantías de infraestructura tipo 3 del INE para operar a nivel operativo 7 del INE.**

El proveedor entregará reportes físicos dirigido al área administradora del contrato, después de la instalación de la infraestructura e implementación, por lo que contará con 5 días naturales siguientes, para la entrega de la siguiente información:

1. Reporte de Instalación de la infraestructura de comunicación y enlace de validación de datos con el INE.
2. Reportes de pruebas productivas de comunicación y validación de datos con el INE.
3. **Firmas de Elaboración, Revisión y Aprobación.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaboró** | **Cargo** | **Firma** | **Fecha** |
| José Antonio Martínez Sánchez | Coordinador Técnico A 80 |  | 08/11/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Revisó** | **Cargo** | **Firma** | **Fecha** |
| Arturo Ortiz Peña | Titular de la Coordinación de Atención a la Continuidad Operativa de Plataformas Aplicativas |  | 14/11/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Aprobó** | **Cargo** | **Firma** | **Fecha** |
| Arturo Ortiz Peña | Titular de la Coordinación de Atención a la Continuidad Operativa de Plataformas Aplicativas |  | 21/11/2024 |

1. OCR. - Reconocimiento óptico de caracteres (*OCR*) es el proceso por el cual se convierte una imagen de texto en un formato de texto que pueden leer las máquinas [↑](#footnote-ref-1)