**Control de versiones del documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Descripción** | **Responsable** |
| 0.1 | 05/01/2026 | Elaboración del documento | José Antonio Martínez Sánchez |
| 1.0 | 06/01/2026 | Revisión y aprobación del documento | Fausto Mario Díaz Cabrera |

**Contenido**

[a) Descripción amplia y detallada de los bienes a adquirir o arrendar o servicios solicitados 3](#_Toc218609108)

[I. Características y especificaciones 3](#_Toc218609109)

[i. Objetivo 3](#_Toc218609110)

[ii. Alcance 3](#_Toc218609111)

[iii. Requerimientos técnicos 4](#_Toc218609112)

[1) Funcionales 4](#_Toc218609113)

[Los servicios comprenderán: 4](#_Toc218609114)

[Entregables 7](#_Toc218609115)

[Garantía de producción y/o distribución de software. 8](#_Toc218609116)

[iv. Acuerdo de Nivel de Servicios (ASL) 8](#_Toc218609117)

[v. Definiciones 9](#_Toc218609118)

[vi. Perfil del proveedor 10](#_Toc218609119)

[vii. Condiciones técnicas de aceptación de entregable 10](#_Toc218609120)

[viii. Niveles de servicio acordados que deberán cumplirse 11](#_Toc218609121)

[Tiempo de respuesta de acuerdo con la prioridad del incidente 12](#_Toc218609122)

[Horarios y medios de comunicación al área de soporte requeridos por el IMSS 12](#_Toc218609123)

[Soporte después del horario hábil en días hábiles 12](#_Toc218609124)

[Ciclo del proceso de Soporte Técnico de atención de incidentes 13](#_Toc218609125)

[ix. Requerimientos de arquitectura tecnológica 14](#_Toc218609126)

[x. Restricciones e interfaces con otros elementos 14](#_Toc218609127)

[b) Pruebas requeridas, método de evaluación y el resultado mínimo que debe obtenerse al ejecutar las pruebas 14](#_Toc218609128)

[c) Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud 14](#_Toc218609129)

[d) Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior. 14](#_Toc218609130)

[e) Normas: Oficial Mexicana, Estándar (antes Mexicana), Internacional, de Referencia o Especificación Técnica, que resulte aplicable a los bienes o servicios requeridos 14](#_Toc218609131)

[f) Firmas de elaboración, revisión y aprobación 15](#_Toc218609132)

**Objetivo del documento**

Precisar las características técnicas que se requieren de los bienes o servicios objeto de la contratación, así como la oportunidad con que son requeridos, y que forma parte integrante del contrato o pedido.

# Descripción amplia y detallada de los bienes a adquirir o arrendar o servicios solicitados

La clave del Clasificador Único de las Contrataciones Públicas (CUCOP) de los bienes a adquirir o arrendar o servicios solicitados se identifica en la siguiente tabla:

|  |  |
| --- | --- |
| **Clave CUCOP** | 32700003 |
| **Descripción** | Patentes, derechos de autor, regalías y otros. |
| **Unidad de medida** | Servicio. |
| **Partida específica (COG)** | 32701. |
| **Objetivo del contrato** | Renovación, Soporte Técnico y mantenimiento de la Plataforma **SeguriData** para el Instituto Mexicano del Seguro Social. |

# Características y especificaciones

# Objetivo

Presentar la necesidad tecnológica que debe ser atendida por medio de la contratación de la **“Renovación del Licenciamiento, Soporte Técnico y Modernización de la Plataforma SeguriData para el Instituto Mexicano del Seguro Social”, en adelante “EL SERVICIO”** para soportar la operación del sistema IMSS desde su empresa (IDSE) en cuanto a la generación, renovación y revocación de certificados de autenticación y generación y validación de firmas electrónicas y acceso al aplicativo de gestión de firmas y a los servicios de sellos de tiempo emitidos por la Notaría electrónica.

# Alcance

**“EL SERVICIO”** deberá presentar una vigencia a partir del día hábil siguiente a la notificación de la contratación y hasta el 31 de diciembre de 2026.

El alcance de “**EL SERVICIO”** se describe a continuación:

* **Soporte técnico** y continuidad a las versiones de infraestructura de llave pública con las que cuenta el IMSS y que opera actualmente, cubriendo 2 ambientes: producción y desarrollo.
* **Mantenimiento** a las versiones de infraestructura de llave pública con las que cuenta el IMSS es decir acceso a las versiones más recientes de los componentes y servicios cubriendo 2 ambientes, producción y desarrollo.
* **Servicios de asistencia técnica**. Acceso a las funcionalidades de la plataforma Seguridata. Acceso a plataforma de Soporte Técnico y Base de Datos de Conocimiento.
* **Servicios de soporte técnico y mantenimiento**. Atender incidencias que se presenten durante la operación de la plataforma Seguridata así como los servicios de criptografía con los módulos de seguridad HSM.

# Requerimientos técnicos

# Funcionales

# 

# Los servicios comprenderán:

**Soporte técnico** para la arquitectura de los siguientes componentes desplegados en el Instituto en un esquema 7x24:

* 1. **Autoridad Certificadora (Seguriserver ™).**
     1. 2 instancias.
     2. 2 módulos criptográficos HSM.
     3. 2 instancias del servicio de validación de certificados.
  2. **Autoridad Emisora de Sellos de Tiempo (SeguriNotary ™)**
     1. 2 instancias del servicio distribuidos en dos servidores.
  3. **Motor de Firma Electrónica (SeguriSign ™).**
     1. 2 instancias del servicio distribuido en dos servidores.

Se requiere como parte de la renovación del soporte técnico cubrir los ambientes de desarrollo y producción.

1. **Ambiente de desarrollo.** El licenciamiento será para un entorno individual o standalone específicamente una licencia por producto, para bajo rendimiento y enfocado al desarrollo de sistemas y pruebas funcionales.
2. **Ambiente productivo**. Se requiere que el proveedor presente un esquema con tolerancia a fallas, además de un ambiente que permita atender y dar respuesta al volumen de transacciones que el Instituto requiere, el licenciamiento provisto es dos por cada producto es decir dos licencias de SeguriServer, dos licencias de SeguriSign y dos licencias de SeguriNotary.

**Mantenimiento** de la plataforma SeguriData se consideran los siguientes elementos:

1. Autoridad Certificadora (Seguriserver ™).
   * 1. 2 instancias con usuarios ilimitados.
     2. 2 módulos criptográficos HSM.
     3. 2 instancias del servicio de validación de certificados.
2. Autoridad Emisora de Sellos de Tiempo (SeguriNotary ™)
   * 1. 2 instancias del servicio distribuidos en dos servidores.
3. Motor de Firma Electrónica (SeguriSign ™).
   * 1. 2 instancias del servicio distribuido en dos servidores.

El mantenimiento deberá tener acceso a todas las actualizaciones que se liberen ya sea para corregir alguna falla detectada o por efectos de cumplimiento tecnológico asociado a criptografía asimétrica.

Se requiere como parte del mantenimiento cubrir los ambientes de desarrollo y producción.

1. **Ambiente de desarrollo.** El mantenimiento será para un entorno individual o standalone específicamente una licencia por producto, para bajo rendimiento y enfocado al desarrollo de sistemas y pruebas funcionales.
2. **Ambiente productivo**. Se requiere que el proveedor presente un esquema con tolerancia a fallas, además de un ambiente que permita atender y dar respuesta al volumen de transacciones que el Instituto requiere, el licenciamiento provisto es dos por cada producto es decir dos licencias de SeguriServer, dos licencias de SeguriSign y dos licencias de SeguriNotary.

**Como parte del soporte técnico el proveedor deberá proporcionar,** asistencia técnica para los servicios de la plataforma de firma del Instituto Mexicano del Seguro Social, la cual constará de acompañamiento para que personal del IMSS pueda actualizar y/o implementar mejoras sobre la funcionalidad del componente, los servicios web del motor de firma electrónica y la autoridad certificadora para la generación, autenticación de firma electrónica, así como la decodificación de las evidencias criptográficas asociadas al documento firmado y la generación, revocación y búsqueda de certificados digitales. Lo anterior para aplicativos que ya hagan uso del componente o para la integración de nuevos aplicativos.

El proveedor deberá entregar un reporte cada vez que se utilicen los tópicos que cubre la asistencia técnica de integración especializada los cuales consisten en:

* Definición de nuevos requerimientos de firma electrónica avanzada.
* Análisis y diseño para integración de firma electrónica avanzada.
* Asistencia técnica en la construcción de módulos con firma electrónica avanzada.
* Pruebas de funcionalidad.
* Recomendaciones de integración de los componentes de firma electrónica avanzada.
* Actualización de versiones de los componentes.
* Liberación de nuevas integraciones.

La asistencia técnica deberá contener lo siguiente:

* Integración a través de componentes de firma para navegador web.
* /API/ servicios web para la generación de documentos auténticos firmados digitalmente.
* Uso de servicios web (web services) para la conformación de los archivos PDF Signature.
* Será impartida de manera remota, mediante la plataforma de comunicación que el IMSS designe para tal fin.

Al inicio de la asistencia técnica de Integración, el proveedor deberá entregar un documento que contenga el detalle funcional de cada uno de los métodos correspondientes a los servicios web (web services) de Integración.

**Servicios de soporte a los servicios de criptografía (HSM´s).**

El proveedor deberá brindar servicios de Soporte técnico Premium Plus para 2 equipos nShield Connect XC de Entrust, FIPS 140 Versión 2 Nivel 3 o superior como parte de los servicios de criptografía, por un año, la póliza considera el remplazo de equipo, así como las partes, materiales y servicios necesarios para la operación de este siempre que el uso del equipo sea bajo condiciones normales de operación.

**Servicio de Soporte Técnico**

El proveedor deberá entregar el soporte técnico bajo un esquema de 7x24 bajo los niveles de servicio establecidos en presente documento todos los días de la semana (lunes a domingo), con una cobertura de 24 horas.

Asimismo, este servicio podrá ser usado por el administrador del contrato para asistencia técnica en caso de incidentes y resolución de fallas de los productos contratados, para lo cual el proveedor deberá entregar para el licenciamiento de software Seguridata on premises, lo siguiente:

Soporte Técnico bajo un esquema de 7x24. El proveedor deberá considerar que en caso de tener que prestar el servicio en alguno de los centros de datos del IMSS en la Cdmx, Cd. de Monterrey Nuevo León y/o San Luis Potosí S.L.P., deberá incluir por cuenta propia los viáticos de su propio personal.

Dicho soporte se requiere bajo atención en sitio o remota por parte de ingenieros especializados y certificados en el uso y manejo de PKI, con nivel de escalamiento de problemas establecido en el Acuerdo de Nivel de Servicios (ASL). El proveedor deberá entregar una bitácora de sucesos con explicación detallada de las fallas y el motivo de estas y la forma de resolverse.

El proveedor deberá entregar las actualizaciones mayores y menores de los productos contratados de tal manera que se encuentren siempre actualizados y a la vanguardia tecnológica, para lo cual el proveedor deberá entregar para el licenciamiento de software Seguridata on premises, lo siguiente:

**Seguriserver (Autoridad Certificadora)**

* Póliza de mantenimiento para licenciamiento que ampare todos updates y upgrades durante la vigencia del contrato.

**Segurisign (Motor de Firma Electrónica)**

* Póliza de mantenimiento para licenciamiento que ampare todos updates y upgrades durante la vigencia del contrato.

**Segurinotary (Autoridad emisora de sellos de tiempo)**

* Póliza de mantenimiento para licenciamiento que ampare todos updates y upgrades durante la vigencia del contrato.

# Entregables

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Descripción de entregables** | **Tiempo de entrega** |
| **Derecho de uso de Licenciamiento** | Derecho de uso de Licenciamiento por el periodo de la vigencia del contrato para los servicios al IMSS, durante todos los días de la semana (lunes a viernes) durante las 24 horas del día, Esto deberá cubrir los siguientes elementos: | 15 días hábiles posteriores a la notificación de adjudicación |
| **SeguriSign** (Motor de Firma Electrónica) cubre ambiente productivo y ambiente no productivo. |
| **SeguriServer** (Autoridad Certificadora) cubre ambiente productivo y ambiente no productivo. |
| **SeguriNotary** (Autoridad de Sellos de Tiempo) cubre ambiente productivo y ambiente no productivo. |
| **Póliza de Mantenimiento** | Mantenimiento por el periodo de la vigencia del contrato para los servicios al IMSS, con acceso sin costo adicional a los componentes de la plataforma de firma contratado por el IMSS, esta póliza cubre los siguientes elementos incluyendo una bolsa anual de 80 horas de soporte en sitio o conexión remota, más 160 horas de soporte telefónico, mail.: | 15 días hábiles posteriores a la notificación de adjudicación |
| Manuales de Administración y Operación del software |
| Manuales de instalación y administración de los componentes de la solución. |
| Documentación de API´s y Web Services |
| Instaladores con la versión más reciente liberada del software |

|  |  |  |
| --- | --- | --- |
| **Servicios de asistencia técnica de integración** | Carta entrega del servicio, con la descripción de las actividades realizadas en el servicio de acompañamiento y asistencia técnica de integración. | 15 días hábiles posteriores a la coordinación con el personal del IMSS, puntualmente los responsables de IDSE |
| Documento de diseño de la integración con diagramas de secuencia. |
| **Servicios soporte técnico y mantenimiento de criptografía (HSM´s).** | 1 póliza de Póliza de Soporte Premium Plus para 2 equipos nShield Connect XC de Entrust, FIPS 140 Versión 2 Nivel 3 o superior. A partir de la entrega del equipo. La póliza considera el remplazo de equipo, así como las partes, materiales y servicios necesarios para la operación de este siempre que el uso del equipo sea bajo condiciones normales de operación. | 15 días hábiles posteriores a la fecha de notificación de adjudicación |
| La póliza cubre cualquier incidencia de hardware o software que pueda ocurrir con cualquiera de los módulos criptográficos solicitado siempre que el uso del equipo sea bajo condiciones normales de operación. |

# Garantía de producción y/o distribución de software.

A través de la garantía de los servicios requeridos, el proveedor deberá garantizar el software incluido en su propuesta durante la vigencia del contrato, asegurando su correcto funcionamiento para los servicios de instalación y configuración, transferencia de conocimientos, asistencia técnica de integración.

El administrador del contrato participará involucrando al personal que considere necesario para la adecuación de estándares, la revisión, y autorización de los productos terminados, así como de las respectivas autorizaciones de los resultados de pruebas de los componentes de acuerdo con las fechas establecidas con el proveedor. De no cumplirse lo antes mencionado, el resultado del desarrollo de este proyecto se verá afectado en los mismos parámetros de tiempo y costo, por lo que será necesario realizar una evaluación de dichos impactos, y las responsabilidades de cada parte en estos impactos.

* El proveedor deberá entregar:
  + Versiones actuales de productos SeguriData: SeguriSign, SeguriServer y SeguriNotary.
  + Asistencia técnica que facilitarán el uso y consumo de las nuevas versiones desplegadas.
  + Acceso a los servicios de criptografía, podría ser vía VPN, con el propósito de revisar el estado de salud de los componentes con los que se provee este servicio.

# Acuerdo de Nivel de Servicios (ASL)

El Objetivo General del Acuerdo de Nivel de Servicio que requiere el Instituto consiste en la emisión de información y solución de problemas, y de manera efectiva y oportuna soporte a los productos y servicios de marca Seguridata, instalados en el IMSS.

# 

# Definiciones

Se deberá entender por parte del proveedor que las palabras y términos que a continuación se relacionan en este documento, tendrán el significado que se precisa, ya sea que se usen en particular o de manera general:

**Incidente de Disponibilidad de Plataforma:** Cualquier evento o suceso que no es parte de la operación normal del software, que ocasiona o puede ocasionar una interrupción total en el servicio que proporciona el propio software, afectando así completamente la operación cotidiana y eficiente del servicio que la IMSS ofrece.

**Incidente de Operación:** Cualquier evento o suceso derivado de la incorrecta operación de los usuarios afectando así la operación cotidiana y eficiente de los usuarios finales, mismo que requiere apoyo para aclarar todas aquellas dudas sobre la correcta operación de la plataforma.

**Soporte telefónico:** Cuando ocurre un incidente y el IMSS se comunica telefónicamente el proveedor para describir la falla. El ingeniero recopila algunos datos cómo: el servicio del que se trata, fecha y hora de momento en el que sucedió el incidente, bajo qué circunstancias se presenta el caso o incidente; así como los datos de la IMSS y del contacto que está reportando el incidente. Una vez que el Ingeniero efectué el levantamiento de información pertinente, deberá enforcarse a resolver lo más rápido posible el incidente para reanudar la operación normal del servicio.

**Infraestructura SaaS de marca SeguriData:** Se refiere a la modalidad de implementación de “Aplicaciones como un Servicio” (Software as a Service) en la que la IMSS consume recursos y servicios para el procesamiento de información en la Nube deSeguriData, la plataforma es administrada portecnologíaSeguriData.

**Servicios en la nube:** Hace referencia a un conjunto de recursos para el proceso de información electrónica y que son expuestos en distintas verticales de negocio ofrecidos a través de internet o en redes privadas.

**Reclamación:** Hace referencia a una reclamación presentada al proveedor por el IMSS en virtud de los acuerdos de nivel de servicio en que se indica el incumplimiento de la disponibilidad de los servicios y la posible retribución de servicios al IMSS.

**Abono de servicio:** deberá considerarse como un porcentaje del de tiempo mensual del servicio que el proveedor deberá en su caso abonar a la IMSS en virtud de una reclamación justificada.

**Conectividad externa:** Es el tráfico de red bidireccional a través de los protocolos admitidos como UDP y TCP que se puede enviar y recibir de una dirección IP pública***.***

# Perfil del proveedor

Se requiere un escrito firmado por el representante legal del proveedor en el cual manifieste que cuenta con las capacidades para emitir certificados Digitales considerando este como documento electrónico que emite una Autoridad, el cual identifica al firmante y establece un vínculo entre él y su la clave privada, con un certificado digital y un sistema de criptografía que en su caso generen firmas electrónicas avanzadas.

Así como la de un proveedor acreditado por la Secretaría de Economía como Prestador de Servicios de Certificación (PSC) autorizado como una Autoridad para emitir certificados digitales con validez jurídica que permiten sustituir una firma autógrafa por firma electrónica para efectos legales.

Así mismo que cuente con la acreditación de la constancia de conservación de mensajes de datos (Constancia NOM151) el cual representa un documento electrónico, emitido bajo los lineamientos definidos en la Norma Oficial Mexicana NOM-151-SCFI-2002, que permite garantizar que la información electrónica de la cual se le solicita una constancia existió en un tiempo y características específicos.

# Condiciones técnicas de aceptación de entregable

|  |  |  |
| --- | --- | --- |
| **No** | **Entregable que deberá sustentar el servicio** | **Plazo de entrega** |
| **1** | El proveedor deberá entregar carta membretada en original y firma autógrafa de su Representante Legal que ampare la activación del Licenciamiento de Seguridata en el Instituto Mexicano del Seguro Social, bajo las condiciones indicadas en el presente anexo y su compromiso de cumplimiento de los niveles de servicio establecidos en el presente anexo. | Dentro de los primeros 15 días hábiles posteriores a la notificación de la adjudicación. |
| **2** | El proveedor deberá entregar carta membretada en original y firma autógrafa de su Representante Legal que ampare la activación del **Soporte Técnico** para el Licenciamiento de Seguridata en el Instituto Mexicano del Seguro Social, bajo las condiciones indicadas en el presente anexo y su compromiso de cumplimiento de los niveles de servicio establecidos en el presente anexo. | Dentro de los primeros 15 días hábiles posteriores a la notificación de la adjudicación. |
| **3** | El proveedor deberá entregar la Carta de confidencialidad en original y firma autógrafa, donde se manifieste que guardará confidencialidad de aquella información, documentos y accesos a infraestructura de cómputo que le sean entregados por el Instituto y que sean debidamente marcados como información confidencial, conforme a los plazos establecidos en la Ley Federal de Transparencia y Acceso a la Información Pública o las que apliquen en el momento de la contratación. | Única vez, dentro de los primeros 15 días hábiles posteriores a la notificación del fallo. |
| **4** | Reporte de actividades del Soporte técnico, por medios electrónicos donde se especifique el cumplimento de los niveles de servicio requeridos en el presente anexo y se enlisten las actividades realizadas durante el periodo que se reporta. | Mensual, dentro de los primeros 5 días hábiles posterior a cada mes durante la vigencia del contrato. |
| **5** | Reporte de actividades de asistencia técnica, por medios electrónicos donde se especifique las actividades realizadas en la asesoría acorde con en el presente anexo y se enlisten las actividades realizadas durante el evento que se reporta. | Mensual, dentro de los primeros 5 días hábiles posterior a cada mes durante la vigencia del contrato. |

Los entregables anteriormente mencionados, deberán ser validados por el administrador del contrato y/ o en su caso a quien este designe por escrito a fin de ser validados y aceptados en tiempo y forma y a entera satisfacción del Instituto.

# Niveles de servicio acordados que deberán cumplirse

Descripción de prioridades de incidentes y especificación de tiempos de respuesta y solución

Las prioridades para atender los requerimientos de soporte técnico, las definirán las Partes con base en los siguientes criterios:

|  |  |  |  |
| --- | --- | --- | --- |
| Prioridad 1  (Critica) | Prioridad 2  (Alta) | Prioridad 3  (Media) | Prioridad 4  (Baja) |
| Interrupción de trabajo | | | |
| La falla de la aplicación impide que el usuario realice sus tareas o afecta algún módulo significativo del sistema y su funcionamiento es inestable o nulo | La falla de la aplicación impide que el usuario realice sus tareas o afecta a una significativa porción de sus trabajos. | La falla de la aplicación causa que el usuario no pueda desarrollar algunas pequeñas porciones de sus trabajos, pero todavía están habilitados para completar la mayoría de otras tareas. Puede además incluir preguntas y requerimientos de información | La falla de la aplicación causa que el usuario no esté disponible para realizar una mínima porción de sus trabajos, pero todavía están habilitados para completar la mayoría de las tareas. |
| Número de clientes afectados | | | |
| La caída de la aplicación afecta a un alto número de usuarios | La caída de la aplicación afecta a un número considerable de usuarios | La caída de la aplicación afecta a un bajo número de usuarios | La caída de la aplicación afecta a uno o dos usuarios. |
| Solución alternativa | | | |
| No es aplicable una solución alternativa para el problema (Ej., el trabajo no puede ser hecho de otra forma). | Hay una solución alternativa aceptable e implementada para el problema (Ej., el trabajo puede realizarse de alguna otra manera). | Puede o no ser aceptable una solución alternativa para el problema. | Es probable que haya una solución alternativa aceptable para el problema incluyendo un sistema en clúster. |

# Tiempo de respuesta de acuerdo con la prioridad del incidente

|  |  |  |  |
| --- | --- | --- | --- |
| Prioridad del incidente | Impacto en IMSS | Respuesta de servicio al cliente | Tiempo de resolución |
| Crítica | Severo | 1 hora | El tiempo máximo de resolución es de 4 horas, después del tiempo de respuesta inicial |
| Alta | Urgente | 3 horas | El tiempo de resolución máximo aceptable es de 8 horas. |
| Media | Importante | 6 horas | El tiempo de resolución máximo aceptable es de 16 horas. |
| Baja | Orden de trabajo / no critico | 1 día hábil | El tiempo de resolución máximo aceptable es de 24 horas. |

# 

# Horarios y medios de comunicación al área de soporte requeridos por el IMSS

EL IMSS requiere una atención de soporte técnico en un horario de soporte en días hábiles para soporte 7x24: 9:00 am - 6:00 pm de lunes a viernes (Días Laborales).

# 

# Soporte después del horario hábil en días hábiles

El IMSS requiere horarios disponibles para soporte después del horario de días hábiles mediante la página Web del proveedor, o por correo electrónico (comprende de 6:01p.m. - 8:59 a.m. de lunes a viernes en días laborales y las 24 Horas sábados y domingos)

# Ciclo del proceso de Soporte Técnico de atención de incidentes

**

# Requerimientos de arquitectura tecnológica

No aplica.

# Restricciones e interfaces con otros elementos

No aplica.

# Pruebas requeridas, método de evaluación y el resultado mínimo que debe obtenerse al ejecutar las pruebas

No aplica.

# Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud

No aplica.

# Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior.

No aplica.

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

Se requiere que el proveedor acredite las capacidades para emitir certificados Digitales considerando este como documento electrónico que emite una Autoridad, el cual identifica al firmante y establece un vínculo entre él y su la clave privada. Con un certificado digital y un sistema de criptografía que en su caso generen firmas electrónicas avanzadas.

Así como la de un proveedor acreditado por la Secretaría de Economía como Prestador de Servicios de Certificación (PSC) autorizado como una Autoridad para emitir certificados digitales con validez jurídica que permiten sustituir una firma autógrafa por firma electrónica para efectos legales.

Así mismo que cuente con la acreditación de la constancia de conservación de mensajes de datos (Constancia NOM151) el cual representa un documento electrónico, emitido bajo los lineamientos definidos en la Norma Oficial Mexicana NOM-151-SCFI-2002, que permite garantizar que la información electrónica de la cual se le solicita una constancia existió en un tiempo y características específicos.

# Firmas de elaboración, revisión y aprobación

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaboró** | **Cargo** | **Firma** | **Fecha** |
| José Antonio Martínez Sánchez | Coordinador Técnico A80 |  | 05/01/2026 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Revisó y Aprobó** | **Cargo** | **Firma** | **Fecha** |
| Fausto Mario Díaz Cabrera | Titular de la Coordinación de Desarrollo Tecnológico |  | 06/01/2026 |