

FICHA TECNICA

1. Objeto: ***“Adquirir certificados digitales de función pública para SIIF Nación y certificados digitales para firma de documentos en el sistema de gestión documental, en token físico y/o HSM, conforme a lineamientos vigentes”.***

Alcance al objeto: El alcance comprende la adquisición, suministro, activación, configuración, renovación y/o reposición, según corresponda, de los certificados digitales de función pública requeridos para la operación del Sistema Integrado de Información Financiera – SIIF Nación, así como de los certificados digitales destinados a la firma electrónica de documentos en el Sistema de Gestión Documental de la entidad, en las modalidades de token físico y/o HSM.

En desarrollo del objeto contractual, se contempla el suministro de **cincuenta y nueve (59) certificados digitales para SIIF Nación, veintidós (22) certificados digitales para la firma de documentos en el Sistema de Gestión Documental y un (1) certificado digital asociado a la facturación electrónica**, para un total de **ochenta y dos (82) certificados digitales**.

Los certificados deberán ser suministrados, activados y configurados de acuerdo con las especificaciones técnicas requeridas por la entidad, así como con los lineamientos establecidos por los administradores de los sistemas y la normatividad vigente aplicable, garantizando su disponibilidad y adecuada operación durante el periodo de vigencia correspondiente.

El contratista deberá garantizar que los certificados digitales suministrados cumplan con las condiciones de **seguridad, autenticidad, integridad, disponibilidad y trazabilidad** requeridas para el desarrollo de las funciones institucionales, la operación de los sistemas de información y la suscripción de documentos electrónicos, así como brindar el soporte técnico necesario para su correcta implementación y funcionamiento durante la vigencia de los certificados.

2. ANTECEDENTES

El Ministerio del Interior requiere garantizar la correcta ejecución presupuestal y financiera, incluyendo el registro de las diferentes etapas del gasto en el Sistema Integrado de Información Financiera de la Nación – SIIF Nación, herramienta oficial administrada por el Ministerio de Hacienda y Crédito Público que permite integrar, centralizar y estandarizar la gestión financiera pública, asegurando la eficiencia en el uso de los recursos y la disponibilidad de información oportuna y confiable.

En cumplimiento de lo establecido en el artículo 2.9.1.1.5 del Decreto 1068 de 2015, las entidades que hacen parte del Presupuesto General de la Nación deben registrar en el SIIF Nación todas las operaciones asociadas a su gestión financiera, conforme a los lineamientos definidos por el Administrador del Sistema.

Para el acceso, autenticación y registro de transacciones en el SIIF Nación, es obligatorio el uso de certificados digitales de función pública, los cuales permiten garantizar la autenticidad, integridad, confidencialidad y no repudio de la información registrada por los usuarios autorizados. Esta obligación se fundamenta en la Ley 527 de 1999, el Decreto 333 de 2014 y en las Circulares Externas 002 de 2021 y 014 de 2025 expedidas por la Administración del SIIF Nación.

En este sentido, los certificados digitales deben ser emitidos por entidades de certificación digital abiertas acreditadas por el Organismo Nacional de Acreditación de Colombia – ONAC y homologadas por el SIIF Nación, garantizando su interoperabilidad y validez dentro del

Ministerio del Interior – Sede Correspondencia

Edificio Camargo, calle 12B N° 8-46, Bogotá D.C., Colombia

Conmutador: (+57) 601 242 7400 - Línea Gratuita: (+57) 01 8000 91 04 03

servicioalciudadano@mininterior.gov.co

www.mininterior.gov.co

sistema. Así mismo, permiten identificar de manera inequívoca al usuario, firmar digitalmente las transacciones y asegurar la trazabilidad de las operaciones realizadas.

De otra parte, en atención a lo dispuesto en la Directiva Presidencial 09 de 2020 y la Circular Externa 039 de 2022 del SIIF Nación, se requiere la adquisición de un certificado de firma digital de persona jurídica, asociado al NIT de la entidad, para la generación y transmisión del documento soporte en adquisiciones realizadas a sujetos no obligados a expedir factura de venta ante la DIAN.

Adicionalmente, la Entidad requiere implementar mecanismos de firma digital para la gestión de documentos electrónicos en la plataforma ControlDoc, solución de gestión documental y firma electrónica (SGDEA), orientada a automatizar, centralizar y controlar la información institucional, permitiendo la creación, firma y gestión segura de documentos, así como la administración de flujos de trabajo como ventanilla única, PQR y trámites contractuales.

En este contexto, se hace necesario contar con certificados digitales adicionales que permitan la firma de documentos electrónicos con plena validez jurídica, garantizando la autenticidad, integridad y no repudio de la información, así como su interoperabilidad mediante API o servicios web con el sistema de gestión documental.

Estos certificados deberán garantizar su funcionalidad en SIIF Nación y el sistema de gestión documental (ControlDoc) de manera que el mismo certificado sirva para ambos aplicativos.

Mediante circular externa 014 de 2025, emitida por el Administrador del SIIF Nación informa las Entidades de certificación digital abiertas homologadas en el SIIF Nación son:

1. ANDES SERVICIO DE CERTIFICACION DIGITAL S. A. En token criptográfico y/o servidor seguro (HSM) provisto por ANDES SCD. S.A.
2. CAMERFIRMA COLOMBIA SAS. En token criptográfico y/o servidor seguro (HSM) provisto por CAMERFIRMA SAS.
3. GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A. – GSE. En token criptográfico y/o servidor seguro (HSM) provisto por GSE S.A.
4. LLEIDA SAS En token criptográfico y/o servidor seguro (HSM) provisto por Lleida SAS
5. OLIMPIA IT S.A.S En token criptográfico y/o servidor seguro (HSM) provisto por OLIMPIA IT S.A.S.
6. SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL - CERTICAMARA S.A. En token criptográfico.
7. THOMAS SIGNE Servidor seguro (HSM) provisto por THOMAS SIGNE

Ministerio del Interior – Sede Correspondencia

Edificio Camargo, calle 12B N° 8-46, Bogotá D.C., Colombia

Conmutador: (+57) 601 242 7400 - Línea Gratuita: (+57) 01 8000 91 04 03

servicioalciudadano@mininterior.gov.co

www.mininterior.gov.co



En consecuencia, el Ministerio del Interior requiere adquirir un total de ochenta y dos (82) certificados digitales, almacenados en dispositivo criptográfico tipo token físico (USB) y/o en infraestructura de servidor seguro (HSM), distribuidos así: cincuenta y nueve (59) certificados para la operación del SIIF Nación, veintidós (22) certificados para la firma de documentos electrónicos en la plataforma de gestión documental ControlDoc (SGDEA) y un (1) certificado digital de persona jurídica para los procesos de facturación electrónica y transmisión de documentos electrónicos ante la DIAN.

Lo anterior, con el fin de que los funcionarios, contratistas y directivos del Ministerio del Interior cuenten con los mecanismos de autenticación y firma digital requeridos para el desarrollo de sus funciones y para la operación de los sistemas institucionales que requieran este tipo de certificados

2.1 CODIGOS UNSPSC:

SEGMENTO	FAMILIA	CLASE	PRODUCTO	NOMBRE
32000000	32100000	32101600	32101617	Tarjetas Inteligentes
43000000	43230000	43233200	43233201	Software de servidor de autenticación

2.2 ENTREGA: El contratista deberá realizar la entrega, emisión y/o activación de los certificados digitales requeridos para el SIIF Nación, la firma de documentos electrónicos en la plataforma de gestión documental ControlDoc (SGDEA), la facturación electrónica y demás aplicaciones institucionales que requieran mecanismos de autenticación y firma digital, de manera parcial y/o bajo demanda, conforme a las solicitudes efectuadas por el Ministerio del Interior. Cada entrega o activación deberá realizarse dentro de un plazo máximo de tres (3) días hábiles contados a partir del requerimiento realizado por el supervisor del contrato, una vez cumplidos los requisitos de perfeccionamiento y ejecución contractual. Los certificados digitales no activados o no asignados deberán permanecer disponibles y bajo custodia del contratista hasta tanto sean requeridos por el Ministerio del Interior, por un periodo mínimo de un (1) año contado a partir de su entrega a la Entidad, sin afectar su vigencia. La vigencia de cada certificado digital será de un (1) año contado a partir de su activación individual. Los certificados deberán estar disponibles desde el inicio del contrato y podrán ser emitidos mediante dispositivos criptográficos tipo token físico (USB) y/o mediante infraestructura de servidor seguro (HSM), garantizando en todos los casos su plena compatibilidad y funcionamiento en el SIIF Nación, ControlDoc, los servicios de facturación electrónica definidos por la DIAN y demás plataformas institucionales que determine el Ministerio del Interior

3 ESPECIFICACIONES TÉCNICAS DEL OBJETO A CONTRATAR

3.1 CONDICIONES GENERALES

3.1.1 Los certificados digitales deberán ser emitidos por una Entidad de Certificación Digital Abierta, acreditada por el Organismo Nacional de Acreditación de Colombia – ONAC y, cuando aplique, homologada para su uso en el SIIF Nación, de conformidad con las Circulares Externas 002 de 2021 y 014 de 2025 expedidas por el Ministerio de Hacienda y Crédito Público.

3.1.2 Los certificados deberán cumplir con lo establecido en la Ley 527 de 1999 y el Decreto 333 de 2014, así como con las demás normas que los modifiquen o sustituyan.

3.1.3 Los certificados digitales deberán ser de función pública, bajo estándar X.509 V3, con algoritmo de firma SHA2RSA y longitud de clave mínima de 2048 bits.

3.1.4 Los certificados digitales deberán garantizar la autenticidad, integridad, confidencialidad y el no repudio de la información asociada a

Ministerio del Interior – Sede Correspondencia

Edificio Camargo, calle 12B N° 8-46, Bogotá D.C., Colombia

Conmutador: (+57) 601 242 7400 - Línea Gratuita: (+57) 01 8000 91 04 03

servicioalciudadano@mininterior.gov.co

www.mininterior.gov.co

las transacciones y documentos electrónicos firmados.

- 3.1.5 Los certificados digitales ya sea suministrado mediante token físico y/o HSM, deberán permitir su uso para la autenticación de usuarios, la firma digital de transacciones en el SIIF Nación y la firma de documentos electrónicos en el sistema de gestión documental de la Entidad, según corresponda.
- 3.1.6 El proveedor deberá proveer, configurar y documentar, sin costo adicional para la Entidad, las herramientas, servicios, interfaces y componentes necesarios para permitir la integración segura e interoperable de la solución de firma digital con la plataforma de gestión documental ControlDoc (SGDEA) y demás aplicaciones institucionales, incluyendo API, servicios web, mecanismos de autenticación, ambientes de pruebas y producción, documentación técnica, validación de firmas, gestión de certificados, trazabilidad, manejo de errores, controles de seguridad, monitoreo y soporte técnico, garantizando el cumplimiento de la normatividad vigente y la compatibilidad con la infraestructura tecnológica del Ministerio del Interior.
- 3.1.7 El proveedor deberá notificar al Ministerio del Interior y al supervisor del contrato, con por lo menos un (1) mes de anticipación, la fecha de vencimiento de los certificados digitales.

3.2 MODALIDAD A: TOKEN FÍSICO (USB) – APLICABLE PARA SIIF NACIÓN

El proveedor deberá:

- 3.2.1 Los certificados almacenados en dispositivos criptográficos tipo token en físico deberán soportar interfaz PKCS#11, cumplir como mínimo con el estándar FIPS 140-2 Nivel 3, ser compatibles con sistemas operativos Windows 7 o superior (arquitecturas de 32 y 64 bits) e incluir los controladores (drivers), manuales y medios de instalación correspondientes.
- 3.2.2 El proveedor deberá entregar los dispositivos token digitales con su respectivo PIN único, personal e intransferible, garantizar la reposición del token sin costo en caso de falla técnica y proveer soporte para su instalación y uso.
- 3.2.3 El contratista deberá realizar la recolección y disposición final ambientalmente adecuada de los dispositivos criptográficos tipo token que hayan cumplido su vida útil, de conformidad con la normatividad vigente.
- 3.2.4 Esta modalidad aplica exclusivamente para los certificados digitales destinados al acceso, autenticación y firma de transacciones en el SIIF Nación.

3.3 MODALIDAD B: CERTIFICADOS ALMACENADOS EN SERVIDOR SEGURO (HSM)

- 3.3.1 Para los certificados almacenados en servidor seguro (HSM), el proveedor deberá garantizar:
- Acceso al certificado mediante mecanismos de autenticación robusta, incluyendo doble factor de autenticación.
 - Integración y compatibilidad con el cliente de firma digital del SIIF Nación y con el terminador de VPN Juniper o la solución que haga sus veces, requerido para la autenticación, validación y operación de los certificados digitales dentro del sistema, garantizando su correcto funcionamiento para el acceso, autenticación y firma de transacciones.
 - Integración mediante API o servicios web con la plataforma de gestión documental ControlDoc (SGDEA) y demás aplicaciones institucionales.
 - Disponibilidad del servicio 7x24x365.
 - Provisión de controladores, software o mecanismos de acceso necesarios para su uso.

3.3.2 Esta modalidad aplica para los certificados digitales utilizados en el SIIF Nación y para aquellos destinados a la firma

Ministerio del Interior – Sede Correspondencia

Edificio Camargo, calle 12B N° 8-46, Bogotá D.C., Colombia

Conmutador: (+57) 601 242 7400 - Línea Gratuita: (+57) 01 8000 91 04 03

servicioalciudadano@mininterior.gov.co

www.mininterior.gov.co

de documentos electrónicos en la plataforma de gestión documental ControlDoc (SGDEA), conforme a los requerimientos técnicos de cada sistema.

3.4 CERTIFICADO DIGITAL DE PERSONA JURÍDICA PARA FACTURACIÓN ELECTRÓNICA

- 3.4.1 El contratista deberá suministrar un (1) certificado digital tipo token físico de persona jurídica asociado al NIT del Ministerio del Interior, destinado a la firma, validación y transmisión de facturación electrónica, documentos soporte en adquisiciones efectuadas a sujetos no obligados a facturar y demás documentos electrónicos requeridos por la DIAN.
- 3.4.2 Dicho certificado deberá garantizar compatibilidad con las plataformas tecnológicas definidas por la DIAN y tendrá una vigencia de un (1) año contado a partir de su activación individual.

3.5 REQUISITOS FUNCIONALES Y DE SEGURIDAD

- 3.5.1 Cada certificado deberá contener como mínimo la siguiente información:
- Nombre del titular
 - Correo electrónico
 - Ciudad
 - Entidad
 - Número de identificación
 - NIT de la entidad
 - Cargo o rol
- 3.5.2 Los certificados deberán permitir la identificación inequívoca del titular y su asociación con las transacciones o documentos electrónicos firmados, garantizando autenticidad, integridad y no repudio.
- 3.5.3 Los certificados deberán ser compatibles con los mecanismos de autenticación y firma requeridos tanto por el SIIF Nación como por la plataforma de gestión documental ControlDoc (SGDEA).
- 3.5.4 El proveedor deberá garantizar la disponibilidad de mecanismos de validación del estado del certificado, tales como CRL (Lista de Revocación de Certificados) y OCSP (Online Certificate Status Protocol), con disponibilidad 7x24x365.

3.6 CONDICIONES TÉCNICAS

El proveedor deberá garantizar:

- 3.6.1 Compatibilidad total con el SIIF Nación y con la plataforma de gestión documental ControlDoc (SGDEA), conforme a los requerimientos de cada sistema.
- 3.6.2 Uso de protocolos seguros de comunicación (HTTPS/TLS 1.2 o superior), sin requerir apertura de puertos adicionales a los estándares, salvo aquellos estrictamente necesarios y previamente autorizados por la Entidad.
- 3.6.3 Disponibilidad de servicios de validación de certificados, incluyendo:
- CRL (Lista de Revocación de Certificados)

Ministerio del Interior – Sede Correspondencia

Edificio Camargo, calle 12B N° 8-46, Bogotá D.C., Colombia

Conmutador: (+57) 601 242 7400 - Línea Gratuita: (+57) 01 8000 91 04 03

servicioalciudadano@mininterior.gov.co

www.mininterior.gov.co

- OCSP (Online Certificate Status Protocol) con disponibilidad 7x24x365.
- 3.6.4 Mecanismos de integración seguros mediante API o servicios web para la firma digital en la plataforma ControlDoc y otras aplicaciones institucionales.
- 3.6.5 Generación de registros de auditoría (logs) asociados a la emisión, uso, validación y revocación de los certificados digitales.

4. REQUISITOS MINIMOS PARA LA PRESTACIÓN DEL SERVICIO

4.1 SOPORTE Y OPERACIÓN

El proveedor deberá:

- 4.1.1 Proveer soporte técnico para la firma de transacciones en el SIIF Nación y para la firma de documentos electrónicos en la plataforma ControlDoc (SGDEA).
- 4.1.2 Definir y suministrar los procedimientos para:
- Emisión
 - Activación
 - Renovación
 - Revocación de certificados
- 4.1.3 Garantizar la protección, confidencialidad, integridad y correcto uso de la información asociada a los certificados digitales.
- 4.1.4 brindar soporte técnico de instalación, configuración y uso de los certificados digitales en horario de lunes a viernes de 8:00 a.m. a 5:00 p.m., sin perjuicio de la disponibilidad permanente de los servicios de validación y consulta de certificados.
- 4.1.5 Realizar el desbloqueo y/o reactivación de los certificados digitales y sus mecanismos de acceso, incluyendo dispositivos criptográficos tipo token físico (USB) y/o credenciales en servidor seguro (HSM), cuando se presenten bloqueos por intentos fallidos de autenticación, sin costo adicional para la Entidad, en un término no mayor a tres (3) días hábiles contados a partir de la solicitud del supervisor del contrato.
- 4.1.6 Disponer de un canal de atención y soporte con tiempos de respuesta acordes a la criticidad del servicio, garantizando la continuidad operativa de los sistemas.

4.2 GESTIÓN DE CERTIFICADOS

- 4.2.1 El contratista deberá permitir el cambio de titularidad del certificado sin costo adicional, en los casos de traslado de dependencia, cambio de funciones o retiro del funcionario o contratista.
- 4.2.2 Garantizar que dicho cambio de titularidad, revocación, reasignación y/o emisión de un nuevo certificado se realice en un plazo máximo de tres (3) días hábiles contados a partir de la solicitud del supervisor del contrato.
- 4.2.3 En los casos de retiro del titular, el proveedor deberá realizar la revocación del certificado y, de ser requerido por la Entidad, permitir la reasignación o emisión de un nuevo certificado, sin costo adicional y sin afectar la disponibilidad de los certificados contratados.
- 4.2.4 El proveedor deberá garantizar la gestión integral del ciclo de vida de los certificados digitales (emisión, activación, suspensión, revocación y renovación), tanto para los utilizados en el SIIF Nación como para la plataforma de gestión documental ControlDoc (SGDEA).

Ministerio del Interior – Sede Correspondencia

Edificio Camargo, calle 12B N° 8-46, Bogotá D.C., Colombia

Conmutador: (+57) 601 242 7400 - Línea Gratuita: (+57) 01 8000 91 04 03

servicioalciudadano@mininterior.gov.co

www.mininterior.gov.co

4.3 OBLIGACIONES ADICIONALES DEL CONTRATISTA

- 4.3.1 El contratista deberá garantizar que los certificados digitales, independientemente de su modalidad (token físico o HSM), sean 100% compatibles con el SIIF Nación y con la plataforma de gestión documental ControlDoc (SGDEA), conforme a los requerimientos técnicos de cada sistema. En el caso de los certificados destinados al SIIF Nación, estos deberán estar homologados para su uso en dicho sistema.
- 4.3.2 Entregar certificación de transferencia de propiedad de los certificados digitales a favor del Ministerio del Interior, en la cual se relacionen, según corresponda, los seriales de los dispositivos criptográficos tipo token emitidos y/o la identificación de los certificados almacenados en servidor seguro (HSM).
- 4.3.3 Así mismo, deberá indicarse que los certificados no activados o no asignados permanecerán disponibles para la Entidad hasta tanto sean requeridos, bajo un esquema de activación bajo demanda, y que la vigencia de cada certificado será de un (1) año contado a partir de su fecha de activación individual. Igualmente, se deberá garantizar un plazo mínimo de un (1) año adicional, contado a partir de la entrega, para la activación de los certificados.
- 4.3.4 Garantizar la emisión, funcionamiento, soporte técnico y renovación del certificado digital de persona jurídica destinado a los procesos de facturación electrónica del Ministerio del Interior, asegurando compatibilidad con las plataformas y servicios definidos por la DIAN.

Dicha certificación deberá estar suscrita por el representante legal del contratista.

- 4.3.5 El contratista deberá garantizar la disponibilidad, control y trazabilidad de los certificados digitales contratados, incluyendo mecanismos de consulta sobre su estado (activo, inactivo, revocado, vencido), tanto para los certificados asociados al SIIF Nación como para la plataforma ControlDoc.

5. SERVICIO POSTVENTA:

Como parte integral de la garantía de calidad del servicio, este deberá garantizar durante la ejecución contractual y durante la vigencia de los certificados digitales adquiridos, según corresponda, un servicio postventa y de soporte técnico que permita asegurar su correcta activación, instalación, configuración, utilización y funcionamiento.

El servicio postventa y soporte deberá comprender, como mínimo, las siguientes actividades:

- Brindar soporte y asistencia técnica relacionada con los certificados digitales suministrados y los dispositivos o mecanismos asociados a estos, cuando aplique.
- Atender y gestionar los incidentes, requerimientos y dificultades que se presenten durante la activación, instalación, configuración o utilización de los certificados.
- Gestionar oportunamente las novedades asociadas a los certificados digitales, incluyendo aquellas relacionadas con su estado, vigencia, funcionamiento, bloqueo o indisponibilidad.
- Realizar la reposición, reexpedición o sustitución de los certificados o elementos asociados cuando haya lugar a ello, de conformidad con las condiciones del servicio y las causas que originen la solicitud.
- Brindar acompañamiento técnico frente a las dificultades que puedan presentarse en la activación, instalación, configuración y utilización de los certificados digitales en los sistemas institucionales.
- Gestionar la renovación de los certificados o brindar el acompañamiento necesario para su renovación, cuando corresponda y de acuerdo con las condiciones de vigencia contratadas.

Ministerio del Interior – Sede Correspondencia

Edificio Camargo, calle 12B N° 8-46, Bogotá D.C., Colombia

Conmutador: (+57) 601 242 7400 - Línea Gratuita: (+57) 01 8000 91 04 03

servicioalciudadano@mininterior.gov.co

www.mininterior.gov.co

- Informar oportunamente a la entidad sobre situaciones que puedan afectar la continuidad, seguridad o disponibilidad de los certificados digitales suministrados.
- Atender las solicitudes de soporte dentro de los tiempos establecidos por la entidad, garantizando oportunidad en la atención y solución de los incidentes reportados.
- Prestar los demás servicios complementarios que resulten necesarios para garantizar la correcta operación, disponibilidad y funcionalidad de los certificados digitales adquiridos, siempre que se encuentren relacionados con el objeto contractual.

El contratista deberá disponer de los canales de atención necesarios para la recepción y seguimiento de solicitudes de soporte, así como de personal con la capacidad técnica requerida para atender los incidentes y requerimientos que formule la entidad.

Las actividades de soporte, asistencia técnica, gestión de novedades, reposición, reexpedición y demás servicios asociados deberán prestarse sin generar costos adicionales para la entidad cuando correspondan a obligaciones derivadas de la correcta prestación del servicio contratado o a situaciones atribuibles al contratista o al proveedor de los certificados.

6. LUGAR DE PRESTACIÓN DEL SERVICIOS

La prestación del servicio se realizará en la ciudad de Bogotá D.C., en las instalaciones del Ministerio del Interior y/o de manera remota, según la modalidad de los certificados digitales (token físico o HSM), garantizando su correcto funcionamiento en el SIIF Nación y en la plataforma de gestión documental ControlDoc.

7. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será hasta el 31 de diciembre de 2026, una vez cumplidos los requisitos de perfeccionamiento y ejecución del contrato.

No obstante, los certificados digitales deberán estar disponibles desde el inicio del contrato, y su entrega y/o activación se realizará de manera parcial y/o bajo demanda, conforme a las solicitudes de la Entidad, dentro de un plazo máximo de tres (3) días hábiles contados a partir del requerimiento del supervisor del contrato.

La vigencia de cada certificado digital será de un (1) año contado a partir de su activación individual.

8. VALOR DE LA OFERTA ECONÓMICA

La oferta económica se debe presentar acorde al cumplimiento de este anexo técnico, con la descripción y relación de los valores que debe incluir todos los costos, IVA y los demás gastos directos e indirectos, inherentes al cumplimiento satisfactorio del contrato, inclusive los imprevistos, gastos de administración, impuestos, contribuciones y utilidades del contratista.

Estos precios no estarán sujetos a revisiones y cambios durante la vigencia 2026 y ejecución del contrato.