ANEXO No. 1 - ESPECIFICACIONES TÉCNICAS.

Suscripción a la plataforma tecnológica Nauta para la optimización y automatización de los procesos asociados a comercio exterior.

Información General

El presente documento establece los lineamientos que deberá tener en cuenta el contratista para desarrollar el objeto del contrato. No obstante, el contratista tendrá en cuenta que en la ejecución del contrato deberá aplicar sus conocimientos para lograr llevar a cabo y a entera satisfacción el objeto contractual de conformidad con las especificaciones y características técnicas que se describen en el presente documento.

1. Objeto:

Suscripción a la plataforma tecnológica Nauta para la optimización y automatización de los procesos asociados a comercio exterior.

2. Alcance

La presente contratación comprende la suscripción a una plataforma tecnológica especializada para la validación automatizada de declaraciones de importación y sus documentos soporte, con el fin de fortalecer los procesos de control, verificación y seguimiento de las operaciones de comercio exterior de Metro de Medellín Ltda.

El contratista deberá garantizar la disponibilidad y correcto funcionamiento de la solución durante la vigencia contractual, incluyendo, según aplique, los servicios de configuración, parametrización, implementación, soporte técnico, mantenimiento, actualización, acompañamiento funcional y demás actividades requeridas para su adecuada operación. La solución podrá incorporar tecnologías de automatización, analítica de datos, inteligencia artificial o herramientas equivalentes que permitan optimizar los procesos de validación y asegurar el cumplimiento de los niveles de servicio definidos por la Empresa.

Items de la contratación:

Ítem	Descripción	Cantidad Estimada (vigencia del contrato
1	Suscripción o acceso a la plataforma tecnológica incluye, soporte técnico, mantenimiento, actualizaciones, capacitación, acompañamiento funcional, parametrización y demás requerimientos funcionales y de seguridad	14 meses
2	Procesamiento, validación y análisis de cada declaración de importación y sus documentos soporte, conforme a las especificaciones técnicas definidas por Metro de Medellín Ltda	210 consultas máximo durante la vigencia del contrato.

Como mínimo, la plataforma deberá contemplar las siguientes funcionalidades y capacidades:

- Validación en las páginas oficiales de la DIAN de acuerdo con la normativa vigente en cada momento.
  https://muisca.dian.gov.co/WebArancel/DefResultadoConsNomenclaturas.faces

https://normograma.dian.gov.co/dian/compilacion/docs/resolucion_mincomercioit_0057_2015.htm

- Cargue, procesamiento, consulta y trazabilidad de la información de las operaciones de importación gestionadas durante la vigencia.
- Extracción automática de datos y comparación cruzada de la DIM, planillas de preinspección, registro fotográfico, factura comercial, factura de fletes, seguros y demás documentos soporte de los procesos de importación.
- Validación y verificación de la correcta liquidación de tributos aduaneros y demás conceptos aplicables a las operaciones de importación, considerando la información consignada en la declaración de importación y los documentos soporte correspondientes.
- Generación de alertas, observaciones, inconsistencias y reportes de validación y errores.
- Parametrización, ajuste y mejora continua de las reglas, modelos o mecanismos de validación utilizados por la plataforma.
- Acompañamiento funcional especializado y capacitación a los usuarios designados.
- Incorporación, parametrización o habilitación de funcionalidades adicionales que contribuyan al fortalecimiento de los procesos de comercio exterior.

Todo lo anterior, de conformidad con las condiciones contenidas en este documento y en los demás Documentos del Proceso

3. Plazo.

La prestación del servicio tendrá una duración de 14 meses.

4. Requerimientos funcionales

N.°	Requerimiento mínimo
1	Acceso web con autenticación segura, usuarios, perfiles y permisos para mínimo cuatro (4) usuarios concurrentes.
2	Carga individual o masiva de archivos PDF, JPG y PNG, enlace WeTransfer o similares.
3	Extracción automática de datos de la DIM y documentos soporte.
4	Comparación cruzada entre documentos y registros fotográficos.
5	Detección de diferencias, omisiones e inconsistencias con alertas detalladas.
6	Trazabilidad de cargue, procesamiento, revisión, ajustes y cierre.
7	Generación y descarga de reportes de validación.
8	Mecanismos de revisión, retroalimentación y ajuste de parámetros o reglas de validación que permitan mejorar la precisión de los resultados.
9	Consulta histórica de operaciones según permisos.
10	Actualización de reglas conforme a cambios normativos o ajustes aprobados.
11	Validación de conceptos, bases, tarifas, valores liquidados y diferencias de tributos aduaneros.

5. Acuerdos de niveles de servicio.

La solución deberá tener una disponibilidad mínima del noventa y nueve coma nueve por ciento (99.9%), excluyendo mantenimientos programados acordados. La atención ordinaria se prestará de lunes a viernes, de 8:00 a. m. a 6:00 p. m., en días hábiles.

Prioridad	Definición	Respuesta inicial	Solución estimada
Crítica	Plataforma no disponible o error que	< 2 horas	< 8 horas

	impide procesar operaciones.		
Alta	Funcionalidad limitada, lentitud severa o degradación sin detener toda la operación.	< 4 horas	< 24 horas
Media/Baja	Consultas, dudas funcionales, reportes menores o solicitudes de información.	< 8 horas	< 48 horas

6. Seguridad de la información

Metro de Medellín Ltda. Reconoce la información como un activo valioso de la organización que permite la generación e incremento del valor. Por tanto, es exigencia que sus servicios se presten bajo un ambiente controlado que permita la mitigación de los riesgos asociados a este tipo de servicios. Con base a esto, es necesario que el servicio SaaS ofertado cuente con las siguientes características mínimas de seguridad.

7. Localización de los datos.

El proveedor de servicios en la nube debe informar desde la etapa PRE CONTRACTUAL y durante la vigencia del contrato el nombre del proveedor de computación en la nube o centro de datos y en qué lugar estarán alojados los datos durante todo el ciclo de vida, de modo que LA EMPRESA pueda evaluar los riesgos asociados al tipo y clasificación de la información y requisitos legales aplicables a la información que comparte, transmite, transfiere o almacena en los servicios o infraestructura de cómputo en la nube que son ofrecidos. Cualquier cambio en la ubicación de los datos por parte del proveedor deberá ser analizado y aprobado por parte de LA EMPRESA.

8. Centro de Datos.

La aplicación o servicio debe estar alojada en un centro de datos de alta disponibilidad, en este caso debe ser con un proveedor de computación en nube que cumpla altos estándares de fiabilidad, escalabilidad y seguridad. El proveedor de nube en el cual se encuentre alojada la información de LA EMPRESA o que sea responsable de soportar el funcionamiento de la aplicación SaaS, debe cumplir como mínimo con las certificaciones en seguridad de la información ISO 27001:2013, SOC 1, SOC 2, SOC3.

9. Navegación segura.

La aplicación o servicio web debe soportar el acceso a través de navegación segura, es decir, deberá contar con certificado digital https con validación extendida emitido por una entidad certificadora reconocida. El proveedor debe suministrarlo y configurarlo en la solución. Es responsabilidad del proveedor asignar y suministrar el direccionamiento público requerido para la URL a la cual accederán los usuarios de la plataforma. La solución deberá soportar la configuración e instalación de certificados digitales suministrados por LA EMPRESA en caso de requerir que sea accedida de manera segura a través de un dominio o subdominio propiedad de LA EMPRESA.

10. Independencia de la Información.

El proveedor debe garantizar la independencia y seguridad de la información almacenada por LA

EMPRESA.

El proveedor debe suministrar a LA EMPRESA el diagrama que describa la arquitectura del servicio ofertado.

11. Diagrama de Arquitectura del Servicio.

EL OFERENTE, al inicio del contrato, debe suministrar a LA EMPRESA el diagrama que describa la arquitectura del servicio ofertado con la descripción y direccionamiento IP de los diferentes componentes. Esta información será utilizada por LA EMPRESA para definir las reglas de navegación en los equipos de seguridad perimetral y delimitar las auditorías de seguridad.

12. Desarrollo Seguro de la Aplicación o Servicio.

EL proveedor debe informar si para el servicio o aplicación ofrecida y sus componentes, utiliza metodologías o buenas prácticas para el desarrollo seguro de software. A continuación, algunas de las más utilizadas:

- Proyecto abierto de seguridad de aplicaciones web (OWASP, por sus siglas en inglés)
- Ciclo de vida de desarrollo de seguridad de Microsoft (Microsoft SDL, por sus siglas en inglés).
- Modelo de Madurez para Aseguramiento de Software (SAMM, por sus siglas en inglés).

13. Seguridad web

EL OFERENTE debe informar si tiene implementada alguna protección para la aplicación web mediante un WAF (Web Application Firewall) y especificar el nivel de protección configurado

14. Seguridad en aplicativos de software como servicio (SaaS).

El proveedor debe garantizar la seguridad del aplicativo y la infraestructura de hardware y software que lo soporta, cumpliendo como mínimo con las mejores prácticas descritas en ISO27001:2013 en cuanto al manejo de usuarios, contraseñas, puertos abiertos, servicios habilitados, separación de ambientes, definición de permisos, versiones actualizadas, (endurecimientos de hardware y software).

El proveedor deberá tener implementados controles técnicos de seguridad de la información, por ejemplo, un cortafuegos para aplicaciones web (WAF, por sus siglas en inglés), que reduzcan la posibilidad de que se exploten vulnerabilidades críticas como las mencionadas en el top 10 del Open Web Application Security Project (OWASP).

El proveedor deberá describir y entregar evidencia de los controles con los que cuenta.

15. Políticas de seguridad de la información.

El CONTRATISTA debe suministrar a La Empresa un documento que describa las políticas de seguridad informática implementadas sobre la infraestructura que compone el servicio ofrecido, en caso de que estas políticas estén en construcción debe notificar esta situación y un estimado de cuando se entregará

16. Reporte y atención de Incidentes de Seguridad Informática.

EL proveedor seleccionado, al inicio del contrato, debe enviar a LA EMPRESA un documento que

describa los procedimientos que tiene establecidos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes de seguridad informática. Igualmente, deberá certificar que tiene identificados y realiza una adecuada evaluación, tratamiento, control y seguimiento de los riesgos informáticos asociados al servicio contratado. En dicho procedimiento deberán estar claramente establecidos los tiempos que aplican para la investigación de los incidentes y su reporte a las partes interesadas.

Para la gestión e investigación de los incidentes de seguridad, el proveedor deberá garantizar el cumplimiento de los requisitos legales aplicables.

EL OFERENTE deberá reportar a LA EMPRESA los eventos o incidentes de seguridad que afecten o tengan el potencial de afectar la prestación del servicio contratado, la información intercambiada entre las partes, los sistemas de información de LA EMPRESA o la información alojada en estos, y todas aquellas situaciones de alto riesgo que sean detectadas por los sistemas de monitoreo y control o en auditorías que realiza el proveedor con sus recursos. De la misma forma deberá informar a LA EMPRESA los planes de remediación aplicados o por aplicar.

17. Entrega de los datos almacenados.

En caso de finalización del contrato por vencimiento del tiempo contratado u otros motivos, el proveedor deberá entregar un archivo que contenga toda la información de LA EMPRESA y sus colaboradores que se encuentre almacenada en las bases de datos de la aplicación o servicio contratado. El formato del archivo entregado será definido entre las partes con el fin de que la información que contenga sea completamente accesible por LA EMPRESA sin depender del proveedor. El plazo máximo para la entrega de la información a LA EMPRESA es de cuarenta y cinco (45) días calendario una vez solicitada.

Una vez finalizada la relación comercial la información de LA EMPRESA y sus colaboradores que se encuentre almacenada en las bases de datos de la aplicación o servicio contratado debe ser destruida con procedimientos que garanticen la no recuperación de esta. El proveedor una vez realizado el borrado seguro de la información y en un plazo máximo de cuarenta y cinco días (45) días calendario contados a partir de la fecha fin del servicio contratado, deberá suministrar una certificación firmada por el representante legal en la que brinde información sobre el procedimiento aplicado, así como las herramientas de hardware y software, técnicas o algoritmos utilizados para el borrador de la información.

En caso de que LA EMPRESA desee dar continuidad al servicio le informará al proveedor para que suspenda el procedimiento de borrado seguro de la información, el proveedor se da por informado con el inicio del proceso precontractual.

18. Obligaciones técnicas del contratista.

- Cumplir el alcance, requerimientos, entregables, ANS y condiciones de seguridad.
- Contar con personal idóneo para la prestación del servicio, con conocimientos en plataformas tecnológicas, seguridad de la información y normativa aduanera colombiana.
- Mantener disponible la plataforma y atender incidentes y requerimientos.
- Garantizar confidencialidad, integridad, disponibilidad y trazabilidad.
- Someter a aprobación los cambios que afecten operación, arquitectura, ubicación de datos o seguridad.
- Corregir sin costo adicional los defectos atribuibles al servicio o a los desarrollos.

- Mantener actualizada la documentación y transferir conocimiento para el personal de comercio exterior de La Empresa.