ANEXO DE ESPECIFICACIONES TÉCNICAS

1. OBJETO

Renovar la Suscripción a la plataforma de firmas electrónicas AdobeSign en modalidad software como servicio (SaaS) y suministro de certificados de firma digital.

2. ALCANCE

El objeto descrito tendrá el siguiente alcance:

2.1 Proveer a La Empresa la renovación a la suscripción de la plataforma de Firma Electrónica AdobeSign en modalidad de software como servicio (SaaS) por un período de doce (12) meses cumpliendo con las especificaciones técnicas, la seguridad de la información, disponibilidad y acuerdos de nivel de servicio requeridos por La Empresa en el presente documento.

2.2 El CONTRATISTA debe ofertar de acuerdo con el cuadro del "*Formato de Cotización"* adjunto (Excel) con los rangos de firmas y OTP allí expresados, los valores no pueden ser reajustados.

2.3 La activación de los rangos será a demanda. La Empresa no estará obligada a un mínimo ni a un máximo de consumo, más allá del rango activado.

2.4 Suministrar certificados de firma digital avalados por La ONAC y según necesidad de la Empresa. En ningún caso la Empresa estará obligada a la adquisición de un mínimo de firmas Digitales. Dicho certificado de firma digital puede estar incluido en el portafolio de servicio del contratista o haciendo enlace con los emisores de certificados de firma digital.

2.5 Proveer una bolsa de 50 horas para ejecutar a demanda en la configuración, parametrización, nuevos flujos, integraciones, APIS, Web Services y demás necesidades no contempladas en la suscripción.

3. ESPECIFICACIONES TÉCNICAS Y FUNCIONALES MÍNIMAS REQUERIDAS

A continuación, se describen las funcionalidades y especificaciones técnicas mínimas que debe cumplir el software.

3.1. Especificaciones firma electrónica:

ID	DESCRIPCIÓN
1	Plataforma con interfaz web responsive, adaptada para todos los navegadores (Mozilla, Chrome, Edge, entre otros) y dispositivos (smartphone, tablet, computador) y sistemas operativos (Android, iOS).
2	Multi idioma (como mínimo español e inglés)

ID	DESCRIPCIÓN
3	Validación de la autenticidad de los documentos sin depender de la plataforma (Certificado digital vigente).
4	El certificado debe contener LTV (Long Time Validation) que conserve la validez de la firma electrónica en el tiempo.
5	Permitir cargar anexos, mínimo con las siguientes extensiones: PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, TIFF, TIF, BMP, JPG, JPEG, y PNG.
6	Permite previsualización de los archivos anexos.
7	Los roles y permisos deben ser administrables por la Empresa. Configuración de privilegios de usuarios.
8	Capacidad de integración con otras plataformas tecnológicas como gestor documental, gestor contractual y SAP ERP mediante APIs y Web Service.
9	Informe de auditoría del proceso de firma para cada documento (quién firmó, fecha, hora y en qué orden se dio la firma).
10	Debe garantizar la integridad de los documentos durante el proceso de firma. El documento original no debe contener ninguna marca de agua o alteración diferente a las firmas mismas y todo el contenido que las acredita como auténticas.
11	Debe permitir elegir el orden en que se desea firmar, o firmas sin orden o solo una firma.
12	Permitir cancelación o rechazo por cualquier firmante y permita evidenciar la trazabilidad.
13	Notificaciones automáticas de solicitudes de firmas y de cancelaciones o rechazos, al igual que el documento final firmado, sin alterar la trazabilidad establecida al inicio del proceso.
14	El principal método de autenticación para los firmantes debe ser el correo electrónico corporativo.
15	Debe permitir habilitar factores adicionales de autenticación, por lo menos mediante código de un solo uso (OTP – One Time Password) a través de mensaje de texto o de correo electrónico.
16	Debe soportar el proceso de firma de documentos en los que intervienen 10 o más firmantes tanto internos, externos, y a nivel nacional e internacional.
17	Permite configurar y diferenciar firmas y vistos buenos en el documento.
18	Un único tipo documental (Formato) puede ser enviado masivamente para firmas individuales. (Ejemplo, autorización del tratamiento de datos personales).
19	Debe permitir la descarga de los documentos firmados con su correspondiente trazabilidad del proceso de firma cuando la Empresa lo requiera.
20	Debe permitir la generación de reportes de utilización de la herramienta por: usuario, cantidad de firmas por meses, por grupos de trabajo, cantidad de rechazos, cancelaciones, etc.
21	Debe permitir personalizar el cuerpo de los correos electrónicos con la imagen de LA EMPRESA de modo que se identifique fácilmente que provienen de una fuente segura y corporativa. (alertas y notificaciones provenientes de la plataforma vía correo)
22	Permite participar en un flujo de firmas sin necesidad de realizar un registro en la plataforma, solo requiere autenticación para el momento de la firma.
23	Estampa de tiempo en firmas del documento original.

ID	DESCRIPCIÓN
24	Permitir cargar archivos que incluyan gráficos, tablas, imágenes con un peso superior a 25MB.
25	La plataforma debe responder en tiempos que la experiencia de usuario se la más óptima o de ser posible imperceptible. Tanto en la navegación como en la carga de documentos. Se considerará no óptima una navegación con tiempo de espera superior a 5 segundos y una carga de documentos no óptima un tiempo superior a 20 segundos.

- El oferente debe certificar Membresía Platinum y presentar los certificados técnicos y de experiencia que acrediten dicha Membresía. La fecha de emisión del (los) certificado no puede ser superior a 30 días calendario.

- Contar con canales directos de atención con domicilio en Colombia y asistencia en sitio cuando así la Empresa lo requiera.

3.2. Especificaciones para la firma digital

ID	DESCRIPCIÓN
1	Emisión de token tanto físico como virtual, según la necesidad
2	La EMPRESA solicitará los certificados a demanda.
3	Periodicidad de tiempo o vigencia de la firma emitida para un (1) año.
4	Certificado avalado por la ONAC.
5	Brindar asistencia y soporte técnico.
6	Permite revocatoria del certificado de la firma, en casos de retiro del funcionario u otra causalidad.
7	El certificado de la firma debe estar asociado al tipo (función pública), cargo y relación laboral del funcionario de la Empresa.
8	Deberá generarse notificación con antelación del vencimiento del certificado.
9	Emisión de constancia de la vigencia de los certificados emitidos.
10	Se tendrá como máximo 10 días calendario para la entrega del certificado digital.
11	El certificado debe permitir la firma de documentos solicitados por entes gubernamentales y que tenga interoperabilidad con sus respectivos sistemas de información como: Sistema de Certificación Electrónica de Tiempos Laborados – CETIL del Ministerio de Hacienda, documentos de la dirección de antinarcóticos, Superfinanciera, entre otros que pueda requerir la Empresa.
12	Permite la firma de documentos en extensiones como: .PDF, TXT, XBRL, p7z o formatos equivalentes reconocidos para firma digital y archivos de reporte requeridos por entidades de supervisión y control.

ID	DESCRIPCIÓN
13	Permite que en un documento haya firmas múltiples y firmas añadidas, para que dos o más firmantes puedan incorporar nuevas rúbricas o certificados digitales sin invalidar los sellos previos, independientemente del emisor de los otros firmantes.
14	Permite firmar documentos sin bloquearlos para que puedan firmar otras personas, independiente del emisor de los otros firmantes.
15	Permite bloquear el documento cuando es única firma o es el firmante final.
16	Permite la validación posterior de todas las firmas y certificados incorporados al documento, preservando la integridad y autenticidad del contenido firmado.

4. REQUISITOS NORMATIVOS

4.1. El contratista durante la vigencia del contrato deberá cumplir con todas las disposiciones normativas vigentes, por lo tanto, cualquier modificación, o sustitución de las referencias normativas que se realicen en este documento o en cualquiera otro que integre la relación contractual, deberá darse cumplimiento para garantizar la correcta ejecución del objeto, obligaciones y actividades del contrato.

4.2. Manejo de la Información - Protección de Datos Personales:

EL CONTRATISTA en desarrollo de las actividades contratadas por LA EMPRESA, deberá acogerse y garantizar el cumplimiento de la Ley Estatutaria 1581 de 2012, el Decreto 1074 de 2015 y las normas y documentos que los adicionen, complementen o modifiquen.

EL CONTRATISTA, actuará en calidad de Encargado de las bases de datos que trate en virtud del contrato, por lo tanto, deberá garantizar el cumplimiento de los principios aplicables al tratamiento de datos personales, en especial, legalidad, libertad, transparencia, seguridad, confidencialidad, circulación restringida, finalidad, legalidad, entre otros.

El tratamiento que realice EL CONTRATISTA por cuenta de LA EMPRESA debe efectuarse con la finalidad exclusiva de la prestación de los servicios objeto del presente contrato, por lo que EL CONTRATISTA asume el compromiso expreso de no utilizar la información y/o documentación suministrada para cualquier propósito distinto que no sea la prestación de los servicios objeto del presente contrato.

EL CONTRATISTA deberá tomar las medidas apropiadas desde el punto de vista administrativo, técnico, humano, personal y físico para salvaguardar la información y los datos personales que trate, contra pérdida, robo, fuga, manipulación indebida, acceso no autorizado o fraudulento, modificación, divulgación y/o destrucción; adoptando buenas prácticas de seguridad de la información, según la criticidad de la información personal que trate; y así garantizar que esos datos no serán usados, comercializados, cedidos, transferidos y/o no serán sometidos a cualquier otro tratamiento contrario a las finalidades autorizadas por los Titulares y las estipuladas en la Política de Tratamiento de Información y Datos Personales de LA EMPRESA.

EL CONTRATISTA deberá realizar los ajustes a los documentos de tratamiento de datos personales (Términos y condiciones, solicitados en su plataforma de firma electrónica), acorde a la necesidad de la Empresa y exclusivamente para las finalidades expuestas en el anexo de transmisión de datos.

Lo anterior implica que, el CONTRATISTA debe contemplar exponer los términos y condiciones entregados por la Empresa Metro en su anexo de transmisión de Datos. No obstante, revisados los términos y condiciones de la plataforma ofertada, LA EMPRESA podrá aceptarlos o validarlos sin necesidad de algún ajuste adicional.

Los términos y condiciones de la plataforma ofertada deberán estar en idioma español.

5. REQUISITOS DE SEGURIDAD Y PRIVACIDAD 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 los servicios adquiridos con terceros sean prestados bajo un ambiente controlado que permita la mitigación de los riesgos asociados al uso de servicios de computación en la nube, servicios web y el hosting o almacenamiento de información en internet, y cumplan con las siguientes características mínimas de seguridad:

5.1. 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.

Debe presentar certificación con la información solicitada en este numeral, ya sea emitido por su proveedor de computación en nube o por el representante legal del oferente.

5.2. 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 27001:2022, SOC 1, SOC 2, SOC 3.

Debe presentar certificación con el cumplimiento de este numeral, ya sea emitido por su proveedor de computación en nube o por el representante legal del oferente.

5.3. 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).

Debe presentar certificación informando las metodologías o buenas prácticas que usa, ya sea emitido por su proveedor de desarrollos o por el representante legal del oferente.

5.4. Independencia de la Información

La solución SaaS deberá contar con mecanismos de **segregación lógica de datos, control de acceso y aislamiento entre clientes (tenants)** que impidan el acceso, consulta, modificación, transferencia o exposición no autorizada de la información de LA EMPRESA.

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

5.5. Seguridad del aplicativo 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). [1]

Debe presentar certificación con el cumplimiento de este numeral, emitido por el representante legal o gerente de tecnologías del oferente.

5.6. Intercambio seguro de información

La solución debe soportar el cifrado de los datos en el tránsito. En caso de requerirse la integración de esta con otros sistemas de información de LA EMPRESA, será establecida a través de la creación de una red privada virtual (VPN, por sus siglas en inglés) sitio a sitio entre el servicio o aplicación web del proveedor y LA EMPRESA.
El proveedor debe hacerse cargo del suministro y configuración del cliente VPN IPsec de tipo site-to-site que sea compatible con el firewall de la Empresa y una IP pública a la cual se le puedan configurar las reglas de acceso.

[1] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

En caso de ser requerido, el proveedor deberá suministrar a LA EMPRESA los datos de direccionamiento IP privado y público que sean necesarios para establecer reglas en los dispositivos de seguridad que permitan el intercambio seguro de información entre las partes.

5.7. Políticas de Seguridad Informática internas del Proveedor

EL proveedor seleccionado, al inicio del contrato, deberá suministrar a LA EMPRESA un documento que describa las políticas de seguridad de la información implementadas al interior de su empresa y deberá certificar que los empleados que harán parte de la ejecución del contrato cuentan con el conocimiento y apropiación de estas.

Debe presentar certificación con el cumplimiento de este numeral, emitido por el representante legal o gerente de tecnologías del oferente.

5.8. 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, a los siguientes correos: seguridaddigital@metrodemedellin.gov.co. abenavidez@metrodemedellin.gov.co

Debe presentar certificación con el cumplimiento de este numeral, emitido por el representante legal o gerente de tecnologías del oferente.

5.9. Auditorías de seguridad.

Antes de la puesta en producción y por lo menos cada seis (6) meses el proveedor, con sus propias herramientas o través de un tercero autorizado, deberá realizar auditorías técnicas de seguridad sobre el aplicativo o servicio web y la infraestructura que lo soporta con el fin de identificar posibles vulnerabilidades técnicas que pongan en riesgo la información de LA EMPRESA y la disponibilidad del servicio. Entre las pruebas requeridas se resaltan las pruebas de penetración (Pentesting) o hacking ético y escaneo de vulnerabilidades sobre aplicaciones web (web application scan). El informe de las auditorías de seguridad realizadas y las remediaciones aplicadas deberán ser entregados a LA EMPRESA.
En caso de que LA EMPRESA lo requiera podrá realizar sus propias auditorías técnicas sobre el servicio contratado, con la previa aprobación del proveedor y con la coordinación y planificación de ambas partes, sin que esto implique sobre costos, ni afectación del servicio.

El resultado del análisis de vulnerabilidades será compartido con el proveedor para que este realice la remediación de las vulnerabilidades encontradas en un plazo acordado entre las partes.

Debe presentar certificación con el cumplimiento de este numeral, emitido por el representante legal o gerente de tecnologías del oferente, esta auditoria técnica de seguridad no podrá haber sido realizada en un tiempo mayor a 5 meses a partir del inicio del contrato.

5.10. Entrega de los datos almacenados y destrucción de la información almacenada.

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 diez (10) 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 quince (15) 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 borrado de la información.

5.11. Logs del servicio

La solución debe mantener un registro de actividades de usuario fácilmente accesible para LA EMPRESA, con el fin de examinar las actividades realizadas por cada usuario de la aplicación. Debe permitir parametrizar que el único usuario autorizado para acceder al log o registro de actividades sea el usuario Administrador u otro indicado por LA EMPRESA.
El periodo de retención de los logs debe ser mínimo de 30 días calendario.

El Proveedor al inicio del contrato debe entregar las credenciales y capacitar al administrador delegado de la Empresa en como consultar dichos logs.

5.12. Acuerdos de Nivel de Servicio (ANS) y Métricas del servicio

La aplicación o servicio web debe tener una disponibilidad mínima del 99,9% al año, equivalente a 43156.8 minutos/mes con respecto a una disponibilidad esperada de 24/7. La disponibilidad de infraestructura no incluye las paradas planificadas. Los tiempos de indisponibilidad del servicio por actualización de la plataforma que requiera paradas planificadas o trabajos programados deberán ser informados con mínimo 24 horas de anticipación el supervisor técnico por parte de LA EMPRESA, para el debido plan de comunicaciones interna y gestión del cambio.

El proveedor debe contar con las herramientas que permitan medir el cumplimiento de estas métricas. El informe resultante de dichas mediciones debe ser reportados al supervisor técnico del contrato cada 60 días a partir de la orden de inicio y hasta finalizar el vínculo contractual.

El proveedor debe presentar certificación con el cumplimiento de este numeral, emitido por el representante legal o gerente de tecnologías del oferente. Dicho certificado debe expresar de manera clara cuál es la disponibilidad mínima anual tanto en porcentaje como en minutos.

5.13. Recuperación ante desastres

El proveedor debe garantizar la recuperación y continuidad del servicio ante problemas físicos o lógicos en un tiempo máximo de 2 hora, sin pérdidas de información para LA EMPRESA.

El proveedor debe presentar certificación con el cumplimiento de este numeral, emitido por el representante legal o gerente de tecnologías. Dicho certificado debe expresar de manera clara cuál es el esquema de DRP con el cual cuenta y si cumple con el tiempo mínimo solicitado por la EMPRESA.

5.14. Seguridad de los equipos de cómputo y legalidad de software

EL CONTRATISTA O ALIADO DE NEGOCIO debe garantizar que la información intercambiada con LA EMPRESA o recolectada bajo su autorización será procesada o almacenada en equipos de cómputo y servidores autorizados, que cuenten con sistema operativo legal y actualizado a sus últimas versiones estables y con soporte técnico del fabricante y que tengan instalado software antivirus de uso corporativo, completamente actualizado y con soporte del fabricante.

Asimismo, debe certificar que posee y ha adquirido de manera legal la licencia o la autorización para el uso de los programas, software, aplicativos y hardware que utilizará para el desarrollo del objeto contractual.

El proveedor debe presentar certificación con el cumplimiento de este numeral, emitido por el representante legal o gerente de tecnologías

5.15. Conexión de equipos a las redes de LA EMPRESA

En caso de que EL CONTRATISTA o ALIADO DE NEGOCIO para cumplir con el objeto contractual requiera tener acceso autorizado al sistema, red o a algún recurso tecnológico de LA EMPRESA, se obliga a observar y a cumplir la política de seguridad de la información establecida, asimismo, acepta los controles de ciberseguridad implementados, entre los cuales se resaltan mas no se limita a los siguientes:

- **Para equipos de CONTRATISTAS o ALIADOS DE NEGOCIO que requieren conexión directa a las redes de La Empresa:**
    - Instalación antivirus corporativo de La Empresa en los equipos de contratistas en sitio
    - Monitoreo y control de uso del servicio de internet corporativo
    - Monitoreo y protección mediante dispositivos de seguridad perimetral
    - Control del inventario de hardware y software

- Seguimiento periódico al uso de software legal
- Control de acceso mediante controlador de dominio
- Políticas de seguridad a nivel de red
- Intervenciones de hardware y software controlados por la mesa de servicios de La Empresa
- Borrado seguro de la información de La Empresa y formateo del equipo al finalizar la relación contractual

- **Para equipos de CONTRATISTAS o ALIADOS DE NEGOCIO que requieren conexión a través de software de conexión remota o a través de VPN a los sistemas de información o redes de La Empresa:**
  - Software de conexión remota debe ser licenciado para uso corporativo
  - Se verifica el cumplimiento de los requisitos de **Seguridad de los equipos de cómputo y legalidad de software** por parte de La Empresa para conexiones VPN
  - Instalación de cliente VPN de La Empresa una vez autorizada la conexión
  - Monitoreo y protección de las conexiones VPN mediante dispositivos de seguridad perimetral.
  - Control de acceso mediante dispositivos de seguridad perimetral.
  - Políticas de seguridad a nivel de red
  - Borrado seguro de la información de La Empresa al finalizar la relación contractual

5.16. Almacenamiento en nube

En los casos en que la transmisión se realice para efectos de almacenamiento en nube, EL ENCARGADO deberá presentar el DPA (Data Processing Addendum o Data Processing Agreement) en su versión oficial en español, que tenga suscrito o regule la relación con el proveedor de nube con el que se presentó al proceso de la referencia, cuyo contenido deberá encontrarse alineado con este anexo de transmisión de datos personales y deberá contener como mínimo los siguientes elementos:

1. Que exprese con claridad la calidad respecto de la cual actuará el proveedor de nube, la cual deberá ser como Encargado del tratamiento de los datos.
2. Que dentro de la legislación aplicable por las partes, se encuentre incluido el RGPD (Reglamento General de Protección de Datos).
3. Que contenga una cláusula o aparte donde señale que uno de los tratamientos que puede realizar, es el almacenamiento de los datos.
4. Que contenga una cláusula o aparte que contenga o se refiera a las medidas de seguridad de la información que ofrece para garantizar la protección de los datos.
5. Que el documento cuente con una referencia respecto al tratamiento de los datos del proveedor de la nube con sus subcontratistas.
6. Que haga referencia al procedimiento para la atención y respuesta a peticiones de los Titulares de los datos.
7. Que deje expresa la obligación de notificar en caso de requerimiento de entidades públicas o administrativas.
8. Que contenga una cláusula o aparte que contenga o se refiera a las obligaciones de confidencialidad del proveedor de nube y su personal.
9. Que deje expresa la obligación de notificar los incidentes de seguridad que se presenten.
10. Que el documento indique que se permite la realización de auditorías para verificar el cumplimiento de las obligaciones relacionadas en él.

11. Que cuente con una cláusula o aparte que haga referencia al procedimiento de eliminación y devolución de los datos.
Teniendo en cuenta que este tipo de documentos están dirigidos a las empresas sujetas al Reglamento General de Protección de Datos del Espacio Económico Europeo, será necesario certificar que el DPA que se adjunte aplicará a Colombia dentro del alcance geográfico de cumplimiento.

En caso de que EL CONTRATISTA o ALIADO DE NEGOCIO desde la etapa precontractual no pueda dar cumplimiento de alguno de los requisitos específicos de seguridad de la información y dependa de la entrega material del bien o servicio para su verificación, se debe establecer y ejecutar un protocolo de pruebas que permita verificar el cumplimiento de estos antes de la entrega y recibo a satisfacción de los bienes o antes de la puesta en productivo y entrega a operación de los servicios a LA EMPRESA.

6. ESQUEMA DE SOPORTE TÉCNICO

6.1. Niveles de escalamiento ante incidentes y requerimientos.

Servicios de resolución de incidencias mínimo de 10x5 en horario hábil laboral colombiano de 07:30am a 05:30pm. Se exceptúan los festivos nacionales.

El primer nivel de soporte debe estar localizado en Colombia. El segundo nivel o superior de soporte se acepta desde cualquier parte del mundo, siempre y cuando la comunicación sea dada en idioma español.

El tiempo de respuestas se establece según los siguientes datos:

Severidad incidencia	**Tiempo Máximo de Respuesta**
Alta *	2 horas
Media	4 horas
Baja	8 horas
Consultas	8 horas**

(*) Tiempo de respuesta ante caídas. La recuperación ante desastres y restablecimiento del servicio sin pérdida de información son máximo 2h.

(**) La respuesta inicial a las consultas debe darse en un tiempo menor o igual a 8 horas desde su comunicación por parte de LA EMPRESA.
El tiempo máximo de respuesta es el intervalo de tiempo desde la notificación de la incidencia hasta que EL CONTRATISTA evalúe y emprenda acción correctora.

La medición y seguimiento del tiempo de respuesta se realizará a través de la herramienta de gestión de incidencias usada para el seguimiento del servicio.

6.2. Procedimiento de escalamiento.

EL CONTRATISTA desde el inicio del contrato debe informar a LA EMPRESA la cadena de escalamientos que estará disponible para la atención de los diferentes niveles de incidentes y requerimientos reportados por LA EMPRESA. En esta deberá indicar el nombre, número telefónico, correo electrónico del (de los) funcionario (s) que hará las veces de punto de contacto o gerente de proyecto entre LA EMPRESA y EL CONTRATISTA.
La creación de las solicitudes de servicio se debe poder realizar por teléfono, vía correo electrónico o mediante un software de Help Desk o similar dispuesto por EL CONTRATISTA para gestionar las solicitudes.

EL CONTRATISTA deberá indicar el procedimiento de escalamiento, en el cual debe incluir como mínimo los datos de contacto y tiempos de respuesta.

6.3. Registro de Incidentes y Requerimientos

EL CONTRATISTA llevará un registro con todos los incidentes y requerimientos escalados. El reporte debe contener mínimo:
- Un número de caso.
- Fecha y hora en que fue reportado
- Descripción de la solicitud
- Clasificación del evento o solicitud reportada
- Fecha y hora de la solución.
- Solución detallada.

El informe resultante de dichas mediciones debe ser reportados al supervisor técnico del contrato cada 60 días a partir de la orden de inicio y hasta finalizar el vínculo contractual. En el mismo informe indicado en el numeral 5.12 de este documento.

7. DOCUMENTACIÓN

EL CONTRATISTA entregará a LA EMPRESA la documentación técnica y comercial que de conformidad con la naturaleza del objeto del contrato requiera LA EMPRESA durante su desarrollo. LA EMPRESA podrá hacer uso de toda la información entregada por EL CONTRATISTA con motivo del contrato, sin ninguna restricción, con propósitos de operación de la plataforma.

EL CONTRATISTA deberá suministrar la documentación en idioma español.

8. OBLIGACIONES GENERALES DE LAS PARTES

Las partes se comprometen a lo siguiente:

8.1. Obligaciones Generales de la EMPRESA:

- Exigir y verificar el cumplimiento del contrato y sus anexos.
- Poner a disposición del CONTRATISTA la información que posea LA EMPRESA y que sea necesaria para la ejecución del contrato.

- Hacer las observaciones pertinentes a las actividades e informes que presente EL CONTRATISTA durante el desarrollo del contrato.
- Revisar y aprobar oportunamente las facturas que presente EL CONTRATISTA y realizar el pago en la forma pactada.
- Evaluar y calificar el desempeño del CONTRATISTA durante la ejecución del contrato, de acuerdo con lo estipulado en el Sistema de Calidad de LA EMPRESA.
- Todas las demás actividades inherentes a la debida ejecución y cumplimiento del contrato.

PARAGRAFO PRIMERO. Si LA EMPRESA encuentra que los servicios derivados de las actividades contratadas, no se ajustan a los requerimientos hechos por ésta, solicitará el reemplazo o ajuste de los mismos, sin que por ello LA EMPRESA adquiera obligaciones económicas adicionales con EL CONTRATISTA.

PARÁGRAFO SEGUNDO. En el evento en que no se hubieran realizado totalmente los aportes correspondientes, la Entidad pública deberá retener (retención en garantía), del pago final, las sumas adeudadas al sistema en el momento de la liquidación y efectuará el giro directo de dichos recursos a los correspondientes sistemas con prioridad a los regímenes de salud y pensiones según lo estipulado en el artículo 50 Ley 789 de 2002.

8.2. Obligaciones Generales del CONTRATISTA

- Dar cumplimiento al objeto y alcance del contrato de acuerdo con lo establecido en el presente documento y en sus anexos.
- Realizar, por su cuenta y riesgo, todas las actividades necesarias para cumplir con las obligaciones derivadas del Contrato, de acuerdo con las mejores prácticas técnicas y administrativas usuales en servicios de esta naturaleza.
- Estar en permanente comunicación con el Supervisor del contrato.
- Facilitar la labor de seguimiento y control que realiza el supervisor, atendiendo y dando respuesta oportuna a las observaciones o requerimientos que se realicen.
- Disponer por su cuenta y riesgo del personal idóneo, así como de los recursos logísticos, necesarios para desarrollar el contrato.
- Aportar todo su conocimiento y experiencia para desarrollar adecuadamente el objeto del contrato de conformidad con lo requerido por el contratante.
- Cumplir con las normas de gestión ambiental, así como con las normas de seguridad y salud en el trabajo que rijan durante la vigencia del presente contrato y atender las acciones y evidencias que deben presentarse de conformidad con los anexos del contrato.
- Realizar todos los pagos de honorarios y/o salarios, parafiscales e indemnizaciones a que haya lugar e igualmente dar cumplimiento a las normas de afiliación y pago de seguridad social integral (salud, pensiones y riesgos), que le correspondan de acuerdo con el personal que llegare a emplear en la ejecución del contrato, en las cuantías establecidas por la ley y oportunamente. Deberá demostrar, cuando sea requerido por LA EMPRESA el aporte a los sistemas de seguridad social integral y parafiscal (Art. 50 Ley 789 de 2002) que le corresponda.
- Cumplir con los plazos previstos en este Contrato y sus anexos.
- Manejar con la debida confidencialidad la información a que tenga acceso, así como la producida a lo largo de la ejecución del contrato.
- Reportar la información relacionada con la ejecución del contrato o que tenga incidencia en ella cuando sea requerida por el contratante.

- Cumplir con las obligaciones que legal y estatuariamente le corresponden a su rol.
- Asumir especiales obligaciones de cuidado y custodia de los bienes que la EMPRESA le lleguen a entregar para el debido desarrollo de las obligaciones a cargo y en consecuencia estará obligado a hacer el correspondiente reintegro en especie o en dinero cuando por su culpa se produzca daño o perdida, sin que esto excluya la indemnización de perjuicios. Lo anterior sin perjuicio de las acciones que del hecho se puedan predicar.
- Todas las demás actividades inherentes a la debida ejecución y cumplimiento del contrato.