



EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS - ESU

NIT 890.984.761-8

CONTRATO No.

202500091

FT-M3-GJ-01

Versión: 11

CONTRATISTA		NIT	TELÉFONO	FECHA DE SUSCRIPCIÓN	
OSP INTERNATIONAL CALA SAS		830105621-7	3165292793	28/05/2025	
REPRESENTANTE LEGAL		CÉDULA	DIRECCIÓN DE CONTACTO		TEL./CEL. CONTACTO
José Heriberto Fernández García		88.159.098	CR 11 B 96 03 OF 502		3165292793
CORREO ELECTRÓNICO		CIUDAD DE EJECUCIÓN	RADICADO REQUERIMIENTO	BIENES O SERVICIOS	DISPONIBILIDAD PRESUPUESTAL
financiera@ospinternational.com		Medellín	20250003395	servicios	2025000557
CONVENIO	CENTRO DE COSTOS	RUBRO PRESUPUESTAL	DESCRIPCIÓN RUBRO	VALOR CONTRATO	COMPROMISO PRESUPUESTAL
No aplica	14034	21202010041201-1/47829 21202020080402-1/83141	LICENCIAS Y SOFTWARE HONORARIOS/CONSULTORIAS	\$360.337.625,5 INCLUIDO IVA	2025000683

OBJETO

El contratista se obliga con la ESU “Prestar los servicios de licenciamiento de Software SM-DOC de los Módulos de ventanilla Única BPM (Procesos Básicos) Expediente Electrónico, Digitalización y Custodia, Mediante un Modelo de Software as a Service (SAAS) anual, sus horas de desarrollo, entrega de toda la información contenida dentro de la aplicación; propiedad de la ESU que se encuentra alojada en la HyperBpm”; de conformidad con los términos y condiciones de contratación y la propuesta presentada por el contratista y aceptada por la ESU, documentos que hacen parte integrante del contrato.

ALCANCE DEL OBJETO

Comprende la prestación integral del servicio de licenciamiento anual para 130 usuarios de Software SM-DOC para la automatización de procesos de contratación de la ESU y de la gestión documental bajo un modelo de software como servicio (SaaS), el cual consta de 5 módulos, Ventanilla Única, BPM (procesos Básicos), Expediente electrónico, Digitalización y Custodia, además de la prestación de servicios de asesoramiento, mediante una bolsa de 200 horas de desarrollo e implementación y puesta en operación de nuevos módulos y/o modificación de los existentes, adaptándose a las necesidades particulares del momento; y los cuales pueden llevarse a cabo tanto de manera presencial como virtual, a través de llamadas telefónicas y conexiones remotas, previa coordinación de las partes.

El proyecto contempla el fortalecimiento de la Gestión de la Seguridad de la Información, incluyendo políticas, controles y mecanismos para garantizar la protección de la información institucional como son:

- a. Políticas de Seguridad:** el proveedor debe tener políticas de seguridad robustas que incluyan la protección de datos, la gestión de accesos y la respuesta a incidentes.
- b. Controles de Acceso:** el proveedor debe implementar controles de acceso basados en roles (RBAC) y utilizar autenticación multifactor (MFA) para proteger los datos sensibles.

Requisitos de ciberseguridad y de la cadena de suministro

Seguridad en la cadena de suministro: El proveedor debe garantizar la seguridad de la solución, infraestructura y datos que soporta el servicio basándose en los controles definidos por la NIST. A continuación, se entrega un resumen de los controles mínimos:

- **Cadena de suministro:** El proveedor y sus terceras partes deben asegurar que la cadena de suministro mantenga sus sistemas actualizados y aplique los parches de seguridad a los componentes que soportan sus procesos.
- **Control de Acceso**
Objetivo: Asegurar que solo usuarios autorizados accedan a los sistemas y datos.
Requerimientos:
 - Autenticación multifactor (MFA).
 - Gestión de roles y privilegios mínimos.
 - Monitoreo y auditoría de accesos.
- **Concienciación y Capacitación**
Objetivo: Garantizar que el proveedor capacite a su personal en seguridad.
Requerimientos:
 - Programas de formación y capacitación en Ciberseguridad con una frecuencia mínima de una vez por semestre, realizando como mínimo un total de dos capacitaciones en el año. Lo anterior, con el objetivo de fortalecer continuamente el conocimiento y la conciencia sobre buenas prácticas de seguridad de la información, amenazas emergentes y cumplimiento de políticas internas
 - Simulaciones de ataques y respuesta a incidentes a la aplicación Web Smart HyperBPM con una frecuencia mínima de 2 veces al año, con su respectivo informe de resultado de hallazgos.
- **Auditoría y Responsabilidad**
Objetivo: Registrar y monitorear actividades para detectar anomalías.
Requerimientos:
 - Implementación de registros de auditoría detallados.
 - Revisión periódica de accesos y acciones dentro del sistema.
 - Revisión de los resultados de auditorías de control TIC, ciberseguridad y seguridad de la información, las cuales se realizarán al producto o servicio contratado (efectuadas por terceros especializados y con independencia).

- **Evaluación y Monitoreo**

Objetivo: Evaluar la seguridad de los servicios SAAS antes, durante y después de su adquisición. El contratista debe tener implementado un sistema de monitoreo continuo para detectar y responder a incidentes de seguridad, así como un proceso o procedimiento claro para notificar a la ESU en caso de un incidente que pueda surtirse frente a los servicios que está soportando.

Requerimientos:

- Pruebas de seguridad en la infraestructura del proveedor. Para este aspecto el proveedor debe suministrar dos veces al año reportes de seguridad (un informe por semestre), fecha que será indicada por el supervisor adscrito a la ESU y de igual manera, el contratista deberá realizar una auditoría externa a su entidad, de la cual deberá suministrar copia de los resultados de la misma (planes de acción y remediaciones), a la ESU.

- Evaluaciones de cumplimiento con estándares de seguridad ITMARK.

- **Gestión de Configuración**

Objetivo: Mantener configuraciones seguras en los sistemas SAAS.

Requerimientos:

- Aplicación de configuraciones seguras por defecto.
- Control de cambios en configuraciones críticas.

- **Planificación de Contingencia**

Objetivo: Establecer estrategias para responder a incidentes y garantizar la continuidad operativa.

Requerimientos:

- Planes de recuperación ante desastres.
- Copias de seguridad y redundancia en sistemas críticos.

- **Identificación y Autenticación**

Objetivo: Proteger la identidad de usuarios y proveedores mediante métodos seguros de autenticación.

Requerimientos:

- Implementación de autenticación biométrica o multifactor.
- Gestión segura de credenciales y contraseñas.

- **Respuesta a Incidentes**

Objetivo: Definir protocolos para gestionar brechas de seguridad en la cadena de suministro.

Requerimientos:

- Procedimientos de notificación y mitigación rápida.
- Equipos de respuesta ante incidentes especializados.

- **Protección de Medios**

Objetivo: Proteger la integridad de medios físicos y digitales utilizados en la cadena de suministro.

Requerimientos:

- Cifrado de medios de almacenamiento.

- Control de acceso a dispositivos y datos sensibles.

- **Seguridad en la Adquisición de Sistemas y Servicios**

Objetivo: Asegurar que los productos y servicios adquiridos con terceras partes cumplan con estándares de seguridad.

Requerimientos:

- Evaluación de proveedores antes de la compra.
- Inclusión de requisitos de seguridad en contratos.
- Auditorías de seguridad en productos adquiridos.

ESPECIFICACIONES DEL BIEN O SERVICIO A CONTRATAR: El servicio se compone de los siguientes componentes

COMPONENTE 1: SERVICIOS DE LICENCIAMIENTO SAAS.

Comprende la prestación integral del servicio de licenciamiento de Software SM-DOC Para la automatización de procesos de contratación de la ESU y de la gestión documental bajo un modelo de software como servicio (SaaS), este servicio se proporciona en una plataforma de Nube de Google Cloud Platform del proveedor e incluye la implementación, actualización y soporte. La infraestructura en la nube cuenta con las condiciones necesarias para garantizar seguridad, estabilidad, alta disponibilidad y confianza en los servicios.

Para la solución SaaS: OSP realizará los procedimientos necesarios para asegurar el “Recovery Point Objective” (RPO = 4 horas) o punto de Recuperación en el Tiempo y el “Recovery Time Objective” (RTO = 4 horas) o Tiempo de Recuperación, definidos de acuerdo con las políticas administrativas de recuperación de la Entidad.

Se realizarán “snapshots” dos veces al día para cada servidor durante las horas hábiles (operación) para garantizar el RPO y RTO definidos.

Cada “snapshot” se guardará por tres días y luego se procederá a su borrado. Cada “snapshot” asegura la recuperación completa del servidor y sus datos al momento de su ejecución, garantizando la recuperación total de la operación.

Nota: En caso de requerirse la migración del sistema hacia otra plataforma o aplicación, el CONTRATISTA brindará a la ESU el acompañamiento especializado necesario durante todo el proceso. Esto incluye la migración de toda la información contenida dentro de la aplicación —es decir, los datos específicos que los usuarios introducen, consultan o manipulan en HyperBPM (como usuarios, imágenes, entre otros)—, así como la puesta a punto y adecuación de dicha información en la nueva plataforma.

El sistema consta de cinco módulos:

1. **Módulo Ventanilla única:** Permite la recepción y organización de documentos internos y externos, facilitando el control del flujo documental. Funcionalidades incluyen la generación de números de radicado, escaneo y carga de documentos, adjuntar metadatos y realizar búsquedas parametrizadas en el repositorio.

2. **Módulo BPM:** Se deriva del proceso iniciado en la ventanilla Única y gestiona la correspondencia según los tramites establecidos por la entidad, permite configurar procesos, enviar y almacenar documentos y gestionar notificaciones y alarmas para garantizar respuestas ágiles.
3. **Módulo Expediente Electrónico:** El Módulo de Expediente Electrónico de SM-DOC asegura la disponibilidad y gestión a largo plazo de documentos electrónicos conforme a la normativa vigente. Sus funcionalidades incluyen la creación, modificación, consulta y foliado electrónico de expedientes. Se integra con firma electrónica y certificadora digital, se ajusta a la estructura organizacional y cumple con estándares de metadatos y TRD.
4. **Módulo Digitalización:** El Módulo de Digitalización de SM-DOC simplifica el escaneo de documentos en varios formatos y permite su visualización y consulta. Incluye funcionalidades como la indexación manual o automática, integración con firmas electrónicas y certificación digital, y facilita la búsqueda y recuperación de documentos. Se pueden configurar permisos de acceso y realizar auditorías de operaciones para garantizar la seguridad y el cumplimiento normativo.
5. **Modulo Custodia:** Este módulo administra y conserva documentos según las TRD de la entidad, cumpliendo con la regulación. Gestiona inventarios documentales en bodega, permite elaborar registros de inventario, generar códigos de barras, y reportar inventarios por unidad y tipo. Facilita la importación/exportación de archivos, modela estructuras de bases de datos y ubicaciones físicas, y ofrece consultas y escaneo de documentos según políticas de Gestión Documental.

El servicio de licenciamiento SAAS para la HyperBPM está destinado a un máximo de 130 usuarios.

El servicio de licenciamiento SAAS para la HyperBPM incluye el soporte y mantenimiento por un año de operación, de acuerdo con la vigencia de la licencia (un año), lo cual corresponde al Soporte Remoto 5x8 (niveles 2 y 3) de acuerdo con los ANS del servicio, lo que implica que se ofrece asistencia técnica de forma remota durante cinco días a la semana y por ocho horas al día, de lunes a viernes en horario laboral. Además, se proporcionará soporte a través de correo electrónico, línea telefónica, Skype y acompañamiento personalizado durante el proceso de migración a la nueva plataforma. Igualmente, se garantizará la entrega completa de toda la información contenida dentro de la aplicación HyperBpm referente a la operación de la ESU.

Entregables:

- Certificado de la licencia para el software HyperBPM por un año, contado a partir del 1 de junio del 2025 hasta el 31 de mayo del 2026 que incluya el soporte, mantenimiento.
- Enlace de acceso y Usuarios de acuerdo con el Contrato.
- El contratista deberá entregar al supervisor designado por la ESU, un informe mensual de las actividades desarrolladas, así como las evidencias que lo respalden. El informe mensual deberá presentarse los primeros cinco (5) primeros días hábiles del mes, y detallará la ejecución en los componentes administrativo, técnico, legal y financiero. Así mismo deberá presentar al momento de la terminación del contrato un informe final con el detalle de la ejecución administrativo, técnico, legal y financiero.
- Se solicita que toda la información contenida dentro de la aplicación HyperBpm (base de datos de usuarios, notificaciones, gestor documental, repositorio de imágenes, firmas, entre otros), referente a la operación de la entidad ESU; la cual está actualmente almacenada en la plataforma Hyper BPM; información que es propiedad de la ESU, sea entregada en un disco duro físico Externo SSD (Solid State Drive), suministrado por el contratista, asegurando que toda la información contenida en las bases de datos, repositorios de archivos esté completa, actualizada, estructurada conforme a la documentación

técnica de la herramienta, y adecuadamente preparada para su migración a otra plataforma. Esta entrega debe garantizar que los datos estén en un formato estándar y accesible, sin alteraciones ni omisiones, con el fin de facilitar su integración y traslado de manera eficiente, segura y sin generar costos adicionales para la ESU. Es esencial que la estructura de la información contenida dentro de la aplicación HyperBpm, los esquemas y las relaciones entre las tablas estén preservados, y que la información proporcionada sea compatible con las herramientas y procesos de migración que serán utilizados para la nueva plataforma. Asimismo, se debe incluir cualquier documentación técnica relevante que facilite la comprensión y el uso de la información contenida dentro de la aplicación HyperBpm durante el proceso de migración de ser necesaria a otra plataforma o aplicación, realizar el debido acompañamiento a la ESU, en la migración a una nueva plataforma de gestión empresarial.

Requisitos de Ciberseguridad para el Proveedor

El proveedor deberá cumplir, como mínimo, con las siguientes condiciones durante la ejecución del contrato:

- Divulgar las características, funciones y vulnerabilidades de ciberseguridad de sus productos y servicios durante la vida útil del producto o el plazo de servicio.
- Proporcionar y mantener un inventario actualizado de componentes (por ejemplo, lista de materiales de software o hardware) para productos críticos.
- Verificar a sus empleados y protegerse contra amenazas internas.
- Presentar evidencia de la implementación de prácticas de seguridad aceptables mediante, por ejemplo, auto certificación, conformidad con estándares conocidos, certificaciones o inspecciones.

Gestión del cambio

El proveedor deberá implementar un proceso formal de gestión de cambios que incluya el registro, evaluación, aprobación e implementación de modificaciones que afecten el servicio, garantizando trazabilidad y mínimo impacto para la operación.

Al respecto, el contratista debe asegurar que cualquier cambio en los servicios o en la infraestructura del proveedor sea evaluado y aprobado antes de su implementación. La ESU debería hacer pruebas y dar conformidad y aceptación de los cambios. Para ello; ante cualquier modificación, el contratista asegurará la debida documentación y evaluación en términos de seguridad

Continuidad del Negocio y Recuperación ante Desastres

El proveedor deberá contar con un Plan de Continuidad del Negocio y un Plan de Recuperación ante Desastres (BCP/DRP), debidamente documentados y probados, que garanticen la disponibilidad del servicio ante contingencias o eventos mayores. En este orden de ideas, el contratista y la ESU, deben realizar pruebas periódicas y copias de seguridad de manera regular, para los servicios críticos que estén considerados dentro del servicio SAAS

Seguridad en el intercambio de información

Se deberán cumplir las siguientes reglas y protocolos de seguridad durante el intercambio de información entre la organización y el contratista, incluyendo subcontratistas:

El contratista deberá garantizar la confidencialidad, integridad y trazabilidad de la información suministrada por la entidad, de acuerdo con lo establecido en el acta de confidencialidad, aplicando las medidas de seguridad correspondientes conforme a los lineamientos definidos.

Copias de seguridad y restauración

El proveedor deberá garantizar la realización periódica de copias de seguridad; de manera mensual, de toda la información contenida en la HyperBpm, con mecanismos de cifrado, almacenamiento seguro y posibilidad de restauración inmediata. Se deberá establecer una política de retención y pruebas periódicas de recuperación.

Así mismo, el contratista deberá realizar los siguientes controles:

- Planificación de contingencias: Definir estrategias de respaldo y recuperación para garantizar la disponibilidad de los datos en caso de incidentes.
- Copias de seguridad y tiempos de retención requeridos para la información. Para ello, el contratista debe disponer de copias en disco. Ahora bien, con relación a los tiempos de retención de las copias de seguridad, cabe indicar que serán definidas según las disposiciones internas de la ESU, así como por las normas y regulaciones de cumplimiento existentes para el proceso tercerizado por la ESU.
- Gestión de la configuración: Asegurar que las copias de seguridad reflejen la configuración actualizada de los sistemas críticos.
- Protección de medios: Garantizar que los dispositivos de almacenamiento de respaldo sean resguardados contra accesos no autorizados o pérdidas accidentales.
- Autenticación e identificación: Implementar controles para acceder a los sistemas de respaldo y restauración de manera segura.
- Respuesta a incidentes: Contar con procedimientos para restaurar información de manera rápida en caso de una brecha de seguridad o falla del sistema.
- Integridad de sistemas e información: Asegurar que las copias de seguridad sean confiables y no hayan sido alteradas.
- Adquisición de sistemas y servicios: Incorporar requisitos de respaldo en la compra y desarrollo de nuevas soluciones tecnológicas.
- Monitoreo y auditoría: Supervisar la efectividad de los procesos de respaldo y recuperación, asegurando su correcto funcionamiento.

Acuerdos niveles de servicio

Los acuerdos de nivel de servicio (ANS) estarán sujetos a los compromisos internos establecidos por la Empresa para la seguridad y soluciones Urbanas - ESU, y el contratista debe alinearse a los mismos acordes a las capacidades y compromisos del presente objeto contractual.

Se establecen de forma detallada los Acuerdos de Nivel de Servicio (ANS) con el propósito de garantizar que los servicios prestados por el proveedor se cumplan. Estos indicadores deberán incluir aspectos como la disponibilidad del servicio, los tiempos de respuesta, la seguridad de la información, entre otros criterios relevantes.

Asimismo, en caso de incumplimiento de los ANS establecidos, se deberán indicar claramente las afectaciones en la facturación. Por ejemplo, si no se cumple con el porcentaje de disponibilidad definido, este incumplimiento deberá reflejarse en un descuento proporcional en el monto facturado. Además, el no cumplimiento reiterado de los ANS será causal de terminación del contrato.

El proveedor debe proporcionar los siguientes niveles de soporte:

Primer Nivel: Este es el nivel de soporte inicial, responsable de las incidencias básicas de la Entidad. El principal trabajo de un especialista de Nivel 1 es reunir toda la información de la Entidad y determinar la incidencia mediante el análisis de los síntomas (este lo asume el personal entrenado de la ESU, atendiendo fallas de tipo conexiones, o problemas básicos de soporte).

Segundo Nivel: Está basado especialmente en el grupo help desk del proveedor, donde sus integrantes hacen soporte técnico remoto, teniendo en cuenta áreas del conocimiento más especializadas. El soporte de segundo nivel lo realizan personas especializadas en redes de comunicación, sistemas de información, sistemas operativos, bases de datos, entre otras.

Tercer Nivel: En este nivel se encuentra el equipo con mayor capacidad técnica del proveedor, donde se escalan los incidentes que no pudieron ser resueltos en los niveles 1 y 2; donde se apoya también la investigación y desarrollo de soluciones a los problemas nuevos o desconocidos.

Tipo de prioridad tiempo de atención y escalamiento, tiempo de respuesta a nivel de servicio

Concepto	Tiempo de Respuesta	Tiempo de Solución Temporal	Tiempo de Solución Definitiva
FALLAS CRÍTICAS	Hasta 1 Hora	Máximo 4 horas	Máximo 5 días
FALLAS INTERMEDIAS	Hasta 2 Horas	Máximo 8 horas	Máximo 10 días
FALLAS LEVES	Hasta 8 horas	Máximo 48 horas	Máximo 15 días

Crítico: Las fallas críticas generan indisponibilidad total de los servicios y requieren una atención muy rápida; de acuerdo con el diagnóstico realizado se realizarán las acciones necesarias para recuperar el servicio, sin embargo, es posible implementar acciones de contingencia que permitan recuperar el servicio en el menor tiempo posible (Tiempo de solución Temporal) sin tener aún una solución definitiva, la cual deberá estar completada dentro de los tiempos de Solución Definitiva.

Medio: Generan indisponibilidad parcial, es posible que una parte de los servicios este por fuera sin afectar la totalidad de estos. De acuerdo con el diagnóstico realizado se tomarán las acciones necesarias para recuperar los servicios con indisponibilidad, es posible implementar acciones de contingencia que permitan su recuperación en el menor tiempo posible (Tiempo de solución Temporal) sin tener aún una solución definitiva, la cual deberá estar completada dentro de los tiempos de Solución Definitiva.

Bajo: No implican indisponibilidad de los servicios, sin embargo, son situaciones que afectan de alguna forma el desempeño de la plataforma. Se atenderán dentro de los tiempos definidos para este caso.

COMPONENTE N°2: DESARROLLOS

Prestación de servicios de asesoramiento mediante el desarrollo e implementación y puesta en operación de nuevos módulos y/o modificación de los existentes, adaptándose a las necesidades particulares del momento; y los cuales pueden llevarse a cabo tanto de manera presencial como virtual, a través de llamadas telefónicas y conexiones remotas, previa coordinación de las partes.

Se implementará un proceso de seguimiento y revisión de los servicios del proveedor para asegurar que se mantenga un nivel adecuado de seguridad de la información, garantizando que los desarrollos implementados cumplan con los estándares establecidos.

Debido a los constantes avances en el desarrollo de plataformas y a las crecientes necesidades tecnológicas de nuestra entidad, hemos identificado la necesidad de mantenernos a la vanguardia en soluciones digitales. Por lo tanto, será indispensable contar con el apoyo del equipo técnico de OSP INTERNATIONAL CALA S.A.S. para la entrega de toda la información contenida dentro de la aplicación HyperBpm referente a la operación de la ESU, actualmente alojada en la plataforma Hyper BPM, Cabe resaltar que caso de requerirse la migración del sistema hacia otra plataforma o aplicación, el CONTRATISTA se obliga con la ESU a brindar el debido acompañamiento especializado durante todo el proceso. Las actividades asociadas serán estimadas según el esfuerzo técnico requerido, y su ejecución se facturará bajo un esquema por horas.

El servicio de las horas de desarrollo se prestará por demanda en virtud de los requerimientos de la ESU durante la vigencia del contrato, que permitan el cumplimiento y las parametrizaciones especiales para el funcionamiento y operación del desarrollo.

Estimación de Horas de Desarrollo: La cantidad de horas de desarrollo se determinan según el historial de contratación que antecede este proceso con las cuales se pretende atender las necesidades de mejoras en los procesos que tiene la organización y que repercute en la mejora de funcionalidades de algunos de los módulos.

- Total de Horas Estimadas: 200 horas
- Tipo de Servicio: Bolsa de horas
- Perfil del Personal Asignado: Consultoría/Desarrollo Nivel Profesional (Semi Senior)

Detalles del Servicio:

- Personal Asignado: El contratista debe garantizar que el personal asignado sea idóneo y posea la experiencia necesaria para realizar las tareas requeridas. Se requiere disponibilidad de consultoría/desarrollo de nivel profesional (Semi Senior) durante las horas especificadas.
- Especificaciones: Las horas de desarrollo se suministrarán según lo requiera la entidad para la implementación de los diferentes módulos descritos.

Nota: En caso de requerirse la migración del sistema hacia otra plataforma o aplicación, se brindará acompañamiento especializado durante todo el proceso. Las actividades asociadas serán estimadas según el esfuerzo técnico requerido, y su ejecución se facturará bajo un esquema por horas.

Descripción del Trabajo:

- Configuración y desarrollo de los módulos de:
 1. Ventanilla Única
 2. BPM (Gestión de Procesos)
 3. Expediente Electrónico
 4. Custodia de Documentos
 5. Digitalización

- Procedimiento de Horas de Desarrollo

El contratista deberá seguir un procedimiento detallado para gestionar las horas de desarrollo, el cual incluirá los siguientes aspectos:

- Entrega de la necesidad: Se especificará cómo se entregará la necesidad de desarrollo por parte de la ESU al contratista.
- Definición de la Fecha Esperada de Funcionamiento del Desarrollo: Se establecerá la fecha límite para la entrega y funcionamiento del desarrollo.
- Tiempo Estimado del Desarrollo en Horas: Se estimará el tiempo necesario para completar el desarrollo en horas.
- Duración del Desarrollo: Se determinará la duración total del proceso de desarrollo, desde la recepción de la necesidad hasta la entrega final.
- Seguimiento y Periodicidad: Se establecerá un plan de seguimiento que incluirá la periodicidad de las reuniones y se dejarán actas de los mismos para registrar los avances.
- Entregable del Desarrollo: Se especificarán los entregables esperados al finalizar el desarrollo.
- Período de Estabilización (si aplica): En caso de ser necesario, se definirá un período de estabilización para asegurar el correcto funcionamiento del desarrollo.
- Entrada en Operación: Se detallará el proceso para la puesta en operación del desarrollo una vez finalizado y validado.
- Definición de los Requerimientos Técnicos: Se establecerán los requerimientos técnicos que la ESU debe cumplir para que el proveedor pueda realizar el desarrollo de manera efectiva.

Este procedimiento garantizará el cumplimiento de los estándares de calidad y eficiencia en la ejecución de los desarrollos requeridos por la ESU.

PLAZO

La duración del presente contrato será desde la aprobación de la garantía; por parte de la Unidad de Gestión Jurídica de la ESU, hasta el 31 de diciembre de 2025

El plazo del contrato podrá ser modificado antes de su vencimiento mediante documento suscrito por las partes, previa verificación de la necesidad o conveniencia por parte del supervisor, teniendo en cuenta el cumplimiento del contrato, los precios y las condiciones de ejecución del contrato.

VALOR

El valor del presente contrato asciende a la suma de **TRESCIENTOS SESENTA MILLONES TRESCIENTOS TREINTA Y SIETE MIL SEISCIENTOS VEINTICINCO PESOS CON CINCUENTA CENTAVOS M/L (\$360.337.625.50) IVA INCLUIDO**

FORMA DE PAGO

El valor del contrato se pagará de la siguiente manera:

1. Se realizará mediante un pago único para el licenciamiento SAAS de un (01) año de la plataforma HyperBPM por valor de **TRESCIENTOS VEINTICINCO MILLONES OCHOCIENTOS NOVENTA Y CUATRO MIL DOSCIENTOS SESENTA Y CINCO PESOS CON CINCUENTA CENTAVOS M/L (\$325.894.265.50) IVA EXCLUIDO**, previa presentación de la factura y recibo a satisfacción del informe de ejecución y el Certificado de la licencia para el software HyperBPM por un año.
2. El pago correspondiente a las 200 horas de desarrollo se realizará de manera parcial, conforme al servicio de horas debidamente ejecutadas y aprobadas por el supervisor del contrato. Este proceso será validado mediante el informe de ejecución y las evidencias pertinentes. El valor por hora establecido es de **CIENTO SETENTA Y DOS MIL DOSCIENTOS DIECISÉIS PESOS CON OCHO DÉCIMOS (\$172.216,8) IVA INCLUIDO**, lo que totaliza la suma de **TREINTA Y CUATRO MILLONES, CUATROCIENTOS CUARENTA Y TRES MIL TRESCIENTOS SESENTA PESOS M/L (\$34.443.360) IVA INCLUIDO**.
3. El incumplimiento en razón al servicio prestado (no cumplimiento de los ANS), por parte del contratista generará un impacto directo en la facturación. Así las cosas, de presentarse un incumplimiento por parte del contratista, el porcentaje del incumplimiento (indicado por el supervisor), será directamente proporcional al descuento a ser realizado en la factura del periodo correspondiente. De igual manera, cabe resaltar que; en caso de ser reiterativo el incumplimiento, será causal de terminación unilateral sin perjuicio de los daños ocasionados a la ESU por dicho suceso.

Según lo señalado, debe tenerse en cuenta lo siguiente:

- ✓ La respectiva factura debe cumplir con los requisitos de las normas fiscales establecidas en el Artículo 617 del Estatuto Tributario. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato y, el concepto del bien o servicio que se está cobrando.
- ✓ El contratista deberá acreditar la efectiva prestación del servicio y/o producto por medio de una constancia de recibo firmada por el beneficiario. Una vez aprobada la constancia de recibo por parte del supervisor del contrato, éste emitirá el recibo a entera satisfacción del producto y/o servicio contratado.
- ✓ Las retenciones en la fuente a que hubiere lugar y todo impuesto, tasa o contribución directa o indirecta, Nacional, Departamental o Municipal que se cause por razón de la celebración, ejecución y pago de este Contrato serán a cargo exclusivo del contratista.

- ✓ En virtud del Contrato entre los impuestos, tasas y contribuciones que se generen estarán a cargo del contratista. En todo caso, corresponde al contratista sufragar todos los impuestos, tasas y contribuciones entre otros, que le correspondan de conformidad con la normatividad vigente.
- ✓ Una vez recibida a satisfacción la factura o cuenta de cobro correspondiente, la ESU tendrá treinta (30) días calendario para proceder a su pago.
- ✓ Al momento de entregar la factura, ésta deberá estar acompañada con el certificado de pago de aporte de sus empleados al Sistema de Seguridad Social Integral y a las entidades que administran recursos de naturaleza parafiscal; y la carta donde se especifique la entidad y el número de cuenta bancaria a la cual se le deberá realizar el pago.
- ✓ Para el caso de proveedores que se encuentren obligados a facturar electrónicamente, la facturación deberá ser remitida al correo electrónico facturacion@esu.com.co y la fecha límite para la recepción de las mismas estará sujeta a las fechas definidas en la circular 01 del 08 de enero de 2025, documento donde adicionalmente se define la elaboración del recibo a satisfacción por parte del supervisor designado y el proceso de cierre contable en calidad de empresa industrial y comercial del estado.

CRUCE DE CUENTAS

Con la firma del presente contrato el contratista autoriza a la ESU, para que, al momento de efectuar cualquier pago a su nombre, de manera automática y sin previo aviso, la ESU realice cruce de cuentas para compensar los dineros que el contratista adeuda a la Entidad por cualquier concepto, salvo que sobre los mismos se tenga suscrito un acuerdo de pago entre las partes.

LUGAR DE EJECUCIÓN

La entrega de todos los servicios se hará en el Distrito especial de Ciencia, Tecnología e Innovación de Medellín o en el sitio que le defina la ESU, previa coordinación con el supervisor del contrato.

GARANTÍA CONTRACTUAL

El Contratista se obliga a constituir a favor de “La Empresa para la Seguridad y Soluciones Urbanas - ESU”, una garantía única de las expedidas para Entidades estatales que ampare el cumplimiento de las obligaciones contractuales, otorgada por una compañía de seguros autorizada para operar en Colombia por la Superintendencia Financiera y preferiblemente con poderes decisorios en la Ciudad de Medellín:

Garantías y Mecanismos de cobertura del riesgo: El Contratista se obliga a garantizar el cumplimiento de las obligaciones surgidas a favor de la ESU, con ocasión de la ejecución del contrato, de acuerdo con la siguiente tabla:

AMPARO	SUFICIENCIA	VIGENCIA
Cumplimiento del contrato	20%	Igual a la vigencia del contrato y seis (6) meses más
Calidad del servicio	20%	Igual a la vigencia del contrato y seis (6) meses más

PARÁGRAFO 1: El contratista deberá modificar el monto de la garantía cada vez que sea necesario, en razón del incremento del contrato o la afectación por reclamaciones. Si el contratista se negare a constituir o a reponer la garantía exigida, la ESU directamente solicitará a la Compañía de Seguros la

modificación de la misma, además podrá dar por terminado el contrato en el estado en que se encuentre, sin que haya lugar a reconocer o pagar indemnización alguna.

PARÁGRAFO 2: Al recibo del contrato, el contratista contará con máximo dos (2) días hábiles para la constitución de la póliza única de cumplimiento y entrega de la documentación respectiva.

OBLIGACIONES DEL CONTRATANTE

La ESU en desarrollo del presente contrato tendrá los siguientes derechos y deberes:

- Documentación del sitio existente o necesaria durante el desarrollo.
- Garantizar que el proveedor cumpla con las políticas de seguridad, normas de seguridad de la información y ciberseguridad que tiene establecida la ESU
- Disponibilidad del recurso humano requerido durante la ejecución
- Oportunidad en la entrega de los elementos, documentos, datos y reportes necesarios y solicitados por el gerente de proyectos encargado para el eficiente y eficaz cumplimiento del objeto contractual.
- Designar a un funcionario para la Supervisión del contrato
- Pagar al contratista el valor del contrato dentro del término y condiciones pactadas, previa certificación de cumplimiento.
- Expedir las certificaciones a que haya lugar
- Liquidar al contrato en el término establecido en el contrato y en la ley.

OBLIGACIONES DEL CONTRATISTA

El contratista en desarrollo del presente contrato tendrá los siguientes derechos y obligaciones:

- Cumplir con el objeto del contrato y las especificaciones técnicas que se relacionan en la propuesta presentada y aceptada por la ESU, que hacen parte integrante del mismo y con cada una de las condiciones esenciales del objeto a contratar que se relacionan en los documentos y estudios previos.
- Designar una persona encargada de gestionar, comunicar y apoyar permanentemente el presente objeto contractual, la cual servirá de enlace entre las partes.
- Facilitar la labor de la supervisión dando respuesta oportuna a las observaciones, hallazgos o requerimientos que se realicen como máximo tres días hábiles después de haberse comunicado al contratista. Aplicar todas las recomendaciones sugeridas por el supervisor que estén acorde con el objeto contractual, además, acatar o responder a las indicaciones o requerimientos que haga la ESU, que conduzcan a un mejor cumplimiento de las obligaciones contractuales.
- El contratista deberá entregar al supervisor designado por la ESU, un informe mensual de las actividades desarrolladas, así como las evidencias que lo respalden. El informe mensual deberá presentarse los primeros cinco (5) primeros días hábiles del mes, y detallará la ejecución en los componentes administrativo, técnico, legal y financiero. Así mismo deberá presentar al momento de la terminación del contrato un informe final con el detalle de la ejecución administrativo, técnico, legal y financiero.
- El contratista y su personal deberán firmar acuerdos de confidencialidad y se comprometen a no divulgar, reproducir o utilizar la información sensible o reservada de la entidad, salvo autorización expresa de la ESU.
- Cumplir de buena fe con el objeto del contrato a suscribir, de conformidad con la propuesta adjunta, la cual hace parte integral del contrato.
- Designar un representante para efectos de facilitar y agilizar el manejo de la información entre las partes.

- Presentar las Observaciones y recomendaciones para el buen desarrollo del contrato
- Cumplir con el objeto contractual acordado en la forma, cantidad, lugar, fechas y especificaciones requeridas por la ESU.
- Constituir las garantías que le sean exigidas en el presente contrato y mantenerlas vigentes por el tiempo estipulado por la ESU.
- Acreditar el pago de aportes parafiscales y seguridad social para cada uno de los pagos
- Acatar los requerimientos y observaciones que con ocasión de la ejecución del contrato le hagan el supervisor y/o la contratante.
- El contratista deberá contar con el acuerdo de confidencialidad.
- Brindar el apoyo del equipo técnico de OSP INTERNATIONAL CALA S.A.S. para la entrega de toda la información contenida dentro de la aplicación HyperBpm referente a la operación de la ESU, así como para llevar a cabo y asegurar la migración de dicha información hacia una nueva plataforma de gestión empresarial. Esta migración debe incluir la optimización de los datos con el fin de mejorar la productividad y garantizar la adaptabilidad a futuras demandas tecnológicas.
- Asegurar de que los datos estén cifrados tanto en tránsito como en reposo, estableciendo políticas claras para la protección de datos y la gestión de la información.
- El contratista será responsable por cualquier tipo de vulneración e impacto en la exposición, pérdida, integridad de datos; entre otros aspectos relevantes con la seguridad de los datos.
- El contratista deberá divulgar las características, funciones y vulnerabilidades de ciberseguridad de sus productos y servicios durante la vida útil del producto o el plazo de servicio.
- El contratista debe proporcionar y mantener un inventario actualizado de componentes (por ejemplo, lista de materiales de software o hardware) para productos críticos.
- El contratista debe verificar por seguridad a sus empleados y protegerse contra amenazas internas.
- El contratista debe presentar evidencia de la implementación de prácticas de seguridad aceptables mediante, para lo cual deberá acreditar y aportar la certificación de ITMARK. Así mismo debe implementar un proceso de autocertificación, conformidad con estándares conocidos, certificaciones o inspecciones.
- El contratista debe presentar evidencia de la implementación de prácticas de calidad, para lo cual deberá acreditar certificación de la ISO9001. Ahora bien, si dicha certificación se encuentra en trámite de expedición, la misma deberá ser aportada cuando el ente acreditador la expida. Al respecto dicho compromiso no podrá superar 1 mes después de la aprobación de las pólizas por parte de la ESU.
- El proveedor deberá garantizar la realización periódica de copias de seguridad de toda la información contenida en la HyperBpm de manera mensual, con mecanismos de cifrado, almacenamiento seguro y posibilidad de restauración inmediata. Se deberá establecer una política de retención y pruebas periódicas de recuperación. Así mismo, el contratista deberá realizar los siguientes controles:
 - Planificación de contingencias: Definir estrategias de respaldo y recuperación para garantizar la disponibilidad de los datos en caso de incidentes.
 - Copias de seguridad y tiempos de retención requeridos para la información. Para ello, el contratista debe disponer de copias en disco. Ahora bien, con relación a los tiempos de retención de las copias de seguridad, cabe indicar que serán definidas según las disposiciones internas de la ESU, así como por las normas y regulaciones de cumplimiento existentes para el proceso tercerizado por la ESU.
 - Gestión de la configuración: Asegurar que las copias de seguridad reflejen la configuración actualizada de los sistemas críticos.
 - Protección de medios: Garantizar que los dispositivos de almacenamiento de respaldo sean resguardados contra accesos no autorizados o pérdidas accidentales.

- Autenticación e identificación: Implementar controles para acceder a los sistemas de respaldo y restauración de manera segura.
 - Respuesta a incidentes: Contar con procedimientos para restaurar información de manera rápida en caso de una brecha de seguridad o falla del sistema.
 - Integridad de sistemas e información: Asegurar que las copias de seguridad sean confiables y no hayan sido alteradas.
 - Adquisición de sistemas y servicios: Incorporar requisitos de respaldo en la compra y desarrollo de nuevas soluciones tecnológicas.
 - Monitoreo y auditoría: Supervisar la efectividad de los procesos de respaldo y recuperación, asegurando su correcto funcionamiento.
- El contratista debe tener implementado un sistema de monitoreo continuo para detectar y responder a incidentes de seguridad, así como un proceso o procedimiento claro para notificar a la ESU en caso de un incidente que pueda surtirse frente a los servicios que está soportando.
 - Cumplir con las regulaciones y estándares aplicables, como ley de datos personales de Colombia y de otros países que les aplique a proveedores - clientes con los que la ESU tiene relación.
 - Las demás que tengan relación directa con la naturaleza y objeto del presente contrato.

SUPERVISIÓN

La Supervisión del Contrato estará a cargo del Profesional Universitario Grado 2 de la Oficina Estratégica del área de Tecnologías de la Información -TI, o quien haga sus veces o quien designe el ordenador del gasto; el cual ejercerá las obligaciones y responsabilidades de acuerdo con lo establecido en el Manual de Contratación de la Entidad.

INDEMNIDAD

De conformidad con el reglamento de contratación de la ESU el Contratista se obliga a indemnizar a la Entidad con ocasión de la violación o el incumplimiento de las obligaciones previstas en el presente Contrato. El Contratista se obliga a mantener indemne a la ESU de cualquier daño o perjuicio originado en reclamaciones de terceros que tengan como causa sus actuaciones hasta por el monto del daño o perjuicio causado y hasta por el valor del presente Contrato. Igualmente, el Contratista mantendrá indemne a la Entidad por cualquier obligación de carácter laboral, o relacionadas que se originen en el incumplimiento de las obligaciones laborales que el Contratista asume frente al personal, subordinados o terceros que se vinculen a la ejecución de las obligaciones derivadas del presente Contrato.

CLÁUSULA PENAL PECUNIARIA

De conformidad con el artículo 1592 del Código Civil Colombiano, las partes convienen que en caso de incumplimiento del contratista en las obligaciones del contrato, o de la terminación del mismo por hechos imputables a él, pagará a la ESU en calidad de cláusula penal pecuniaria una suma equivalente al diez por ciento (10%) del valor total del contrato. El valor pactado de la presente cláusula penal es el de la estimación anticipada de perjuicios, no obstante, la presente cláusula no impide el cobro de todos los perjuicios adicionales que se causen sobre el citado valor. Si lo anterior no fuere posible, se cobrará por la vía judicial. Las partes convienen, conforme lo establece el artículo 1600 del código civil, que podrá pedirse a la vez la pena y la indemnización de perjuicios a que hubiere lugar.

EXCLUSIÓN DE RELACIÓN LABORAL

El contratista ejecutará el objeto de este contrato con plena autonomía técnica y administrativa, sin relación de subordinación o dependencia, por lo cual no se generará ningún tipo de vínculo laboral.

CESIÓN DEL CONTRATO

EL contratista no podrá ceder total o parcialmente su posición contractual sin la autorización previa, expresa y escrita de la ESU. EL contratista tampoco podrá ceder total o parcialmente derechos u obligación contractual alguna sin la autorización previa, expresa y escrita de la ESU.

UTILIZACIÓN DE MECANISMOS DE SOLUCIÓN DIRECTA EN LAS CONTROVERSIAS CONTRACTUALES

La ESU y el contratista buscarán solucionar en forma ágil, rápida y directa las diferencias y discrepancias surgidas de la actividad contractual. Para tal efecto, al surgir las diferencias acudirán al empleo de los mecanismos de solución de controversias contractuales, a la conciliación, a la amigable composición o a la transacción. En todo caso, la implementación de los anteriores mecanismos estará supeditada a la necesidad del servicio por parte de la ESU o de sus clientes.

CONFIDENCIALIDAD

En caso que exista información sujeta a alguna reserva legal, las partes deben mantener la confidencialidad de esta información, la cual deberá estar previamente marcada como tal, para ello, debe comunicar a la otra parte que la información suministrada tiene el carácter de confidencial. Cada una de las partes acuerda mantener la confidencialidad de la información Confidencial de la otra parte durante un periodo de tres años contados a partir de la fecha de revelación.

TERMINACIÓN

El presente contrato se podrá dar por terminado por las siguientes causas: 1) Cuando se alcance y se cumpla el objeto del contrato. 2) Por mutuo acuerdo de las partes. 3) Cuando por razones de fuerza mayor o caso fortuito se haga imposible el cumplimiento del objeto contractual. 4) Por el incumplimiento administrativamente declarado por parte de la ESU de cualquiera de las obligaciones establecidas en el contrato. 5) Por vencimiento del término fijado para la ejecución del mismo. 6) Por las demás causales señaladas en la Ley.

LIQUIDACIÓN

El contrato será objeto de liquidación dentro de los cuatro (4) meses siguientes a su terminación. Dentro de este plazo, las partes acordarán los ajustes, revisiones y reconocimientos a que haya lugar, de los cuales quedará constancia en el acta de liquidación. Si es del caso, para la liquidación se exigirá al CONTRATISTA la ampliación de la vigencia de los amparos y garantías para avalar las obligaciones que deba cumplir con posterioridad a la extinción del contrato. En todo caso la liquidación del contrato estará sujeta a las disposiciones del reglamento de contratación de la ESU.

INHABILIDADES E INCOMPATIBILIDADES

El contratista con la firma del presente contrato declara bajo la gravedad de juramento que no se encuentra incurso en ninguna de las inhabilidades e incompatibilidades consagradas en la Constitución y la Ley. La contravención a lo anterior dará lugar a las sanciones de ley.

TRATAMIENTO DE DATOS

El contratista asume la obligación de proteger los datos personales a los que acceda con ocasión del contrato, así como las obligaciones que como responsable o encargado le correspondan acorde con la Ley 1581 de 2012 y sus decretos reglamentarios en cuanto le sean aplicables. Por tanto, deberá adoptar las medidas de seguridad, confidencialidad, acceso restringido y de no cesión en relación con los datos personales a los cuales accede, cualquiera que sea la forma de tratamiento. Las medidas de seguridad que deberán adoptarse son de tipo lógico, administrativo y físico acorde a la criticidad de la información personal a la que accede y/o recolecta, para garantizar que este tipo de información no será usada, comercializada, cedida, transferida y no será sometida a tratamiento contrario a la finalidad comprendida en lo dispuesto en el objeto contractual. En caso de tratarse de datos sensibles, de niños, niñas y adolescentes, tales como origen racial, organizaciones sociales, datos socioeconómicos, datos de salud, entre otros, las medidas de seguridad a adoptar serán de nivel alto. El contratista aportará, para la formalización del contrato, copia de su Política de Protección de Datos Personales y de Seguridad de la Información a la ESU, la cual deberá dar cumplimiento a lo establecido en las disposiciones referente a protección de datos personales. El contratista, con la presentación de la oferta manifiesta que conoce la Política de Protección de Datos de la ESU y que, de ser aceptada la oferta en el proceso del asunto, acepta y se compromete a dar cumplimiento a lo establecido en ella y demás protocolos establecidos por la ESU para el tratamiento de datos personales. Igualmente, El contratista se compromete a informar y hacer cumplir a sus trabajadores las obligaciones contenidas en esta cláusula y las demás que contenga la normativa referente a la protección de datos personales, asimismo los trabajadores del contratista deben conocer y aceptar la Política de Protección de Datos Personales de la ESU. El contratista indemnizará los perjuicios que llegue a causar a El contratante como resultado del incumplimiento de las leyes 1266 de 2008 y 1581 de 2012, aplicables al tratamiento de la información personal, así como por las sanciones que llegaren a imponerse por violación de la misma. El incumplimiento de las obligaciones derivadas de esta cláusula se considera como un incumplimiento grave por los riesgos legales que conlleva el indebido tratamiento de datos personales, y en consecuencia será considerada justa causa para la terminación del contrato, y dará lugar al cobro de la cláusula penal pactada, sin necesidad de ningún requerimiento, a los cuales renuncia desde ahora

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SG - SST)

El contratista deberá encontrarse en las adaptaciones que den lugar para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), de conformidad con el Decreto 1072 de 2015, así como sus modificaciones y los documentos que los complementen. En todo caso previo el inicio de la ejecución del contrato, el contratista deberá presentar las evidencias de las acciones realizadas en la implementación del mencionado, y el cumplimiento de la tabla de valores de la Resolución 0312 de 2019 del Ministerio del Trabajo.

DOCUMENTOS DEL CONTRATO

1- Disponibilidad y compromiso presupuestal. 2- Cedula de Ciudadanía. 3- Propuesta presentada por el contratista. 4- RUT. 5- Certificado de Existencia y Representación legal. 6- Certificado de paz y salvo aportes al sistema de seguridad social y parafiscal. 7- Certificado de antecedentes disciplinarios. 8- Certificado de antecedentes fiscales. 9. Certificado de antecedentes judiciales. 10- Registro Nacional de Medidas Correctivas - RNMC. 11- Solicitud de propuesta comercial y propuesta - Consulta de Inhabilidades de la Ley 1918 de 2018 y Decreto 753 de 2019 - 12- Demás documentos que se deriven del presente contrato.

NATURALEZA JURÍDICA DEL CONTRATO

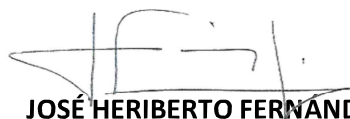
Este Contrato se rige por las normas comerciales y civiles, y especialmente, por el Reglamento de Contratación de la Entidad, expedido por la Junta Directiva de la ESU.

DOMICILIO

El domicilio contractual es el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.

POR LA ESU,

CAMILO ZAPATA WILLS
Gerente

POR EL CONTRATISTA,

JOSÉ HERIBERTO FERNÁNDEZ GARCÍA
Representante Legal

Aprobó:	Laura Alexandra Sepúlveda Marín - Secretaria General	
Aprobó:	Nathalia Restrepo Caro - Subgerente Administrativa y Financiera	
Revisó:	Andrés Felipe Sierra Arango - Profesional Universitario Especializado - Unidad de Gestión Jurídica	
Proyectó:	Lina Marcela Restrepo Toledo - Profesional Universitario - Unidad de Bienes y Servicios	

Viafirma Documents CERTIFICA que el documento con referencia número RQGP1748471303658R641 fue generado a partir de la captura de las siguientes evidencias electrónicas que se enumeran a continuación y que éstas no fueron alteradas desde el momento de su captura, demostrando así la integridad del documento

Resumen del proceso

REMITENTE

Lina Marcela Restrepo Toledo

ORIGEN DE LA SOLICITUD

Panel web

CÓDIGO DE SOLICITUD

RQGP1748471165056T774 / RQGP1748471303658R641

IDENTIFICADOR DE FIRMA

CRQG-POAH-OF1O-TEJE-Q174-8616-6956-86

HASH DEL DOCUMENTO

9fce5c90b137d9d3f7a1..

- Recibido
28/05/2025 17:28:23 COT
- Completada
30/05/2025 09:51:57 COT

Firmas y otras evidencias



Firma manuscrita de Lina Marce ...

✓✓ Completada



Firma manuscrita de Andrés Fel ...

✓✓ Completada



Firma manuscrita de Carlos Val ...

✓✓ Completada



Firma manuscrita de Nathalia R ...

✓✓ Completada



Firma manuscrita de LAURA ALEX ...

✓✓ Completada



Firma manuscrita de CAMILO ZAP ...

✓✓ Completada



Sello del documento

✓✓ Completada

Histórico del proceso

FECHA	ACCIÓN	DETALLE
28/05/2025 17:28:23 COT	Solicitud recibida	Panel web - lmr*****@esu.com.co
28/05/2025 17:28:24 COT	Email de acceso enviado	lmr*****@esu.com.co
28/05/2025 17:28:26 COT	Documento creado	Contrato 202500091.pdf
28/05/2025 17:29:40 COT	Documento Leído	
28/05/2025 17:29:51 COT	Firma recibida	Firma manuscrita de Lina Marcela Restrepo



FECHA	ACCIÓN	DETALLE
28/05/2025 17:29:51 COT	Email de acceso enviado	asj*****@esu.com.co
28/05/2025 17:31:12 COT	Firma recibida	Firma manuscrita de Andrés Felipe Sierra Arango
28/05/2025 17:31:12 COT	Email de acceso enviado	cva*****@esu.com.co
29/05/2025 10:07:01 COT	Firma recibida	Firma manuscrita de Carlos Valencia Osorio
29/05/2025 10:07:02 COT	Email de acceso enviado	nre*****@esu.com.co
29/05/2025 11:44:10 COT	Firma recibida	Firma manuscrita de Nathalia Restrepo Caro
29/05/2025 11:44:11 COT	Email de acceso enviado	lse*****@esu.com.co
29/05/2025 14:45:28 COT	Firma recibida	Firma manuscrita de LAURA ALEXANDRA SEPÚLVEDA MARÍN
29/05/2025 14:45:29 COT	Email de acceso enviado	cza*****@esu.com.co
30/05/2025 09:51:14 COT	Firma recibida	Firma manuscrita de CAMILO ZAPATA WILLS
30/05/2025 09:51:38 COT	Firma digital	VIAFIRMA COLOMBIA - CLOUD SERVICES - VIAFIRMA CO

Todo el que aporte y/o exhiba una impresión como ésta, podrá, a requerimiento, aportar el fichero digitalmente firmado. Los datos en él reflejados están respaldados por matriz electrónica, a disposición de los órganos judiciales o arbitrales que precisen verificación.

De conformidad con la normativa de Protección de Datos de carácter personal aplicable se informa que sus datos personales han sido facilitados por el emisor identificado más arriba, con la exclusiva finalidad de acreditar la autenticidad de la transacción a la que se refiere este certificado.

El soporte que incorpora las firmas electrónicas de las transacciones tiene la consideración de prueba documental, de acuerdo con la normativa aplicable en el Espacio Económico Europeo. Puede consultar las condiciones del servicio contratado de tercera parte de confianza en la dirección : <https://www.viafirma.com/politica-de-cookies/>



Viafirma custodiará los registros informáticos generados en las transacciones realizadas, que son acreditativos de todo lo antedicho, de acuerdo con contrato suscrito entre Viafirma y el emisor.

