SECRETARÍA DE LAS TIC
GRUPO DE INFRAESTRUCTURA TECNOLÓGICA

CONDICIONES MÍNIMAS DE OPERATIVIDAD DEL MÓDULO DE COBRO COACTIVO PARA EL PROCESO DE GESTIÓN DE HACIENDA PÚBLICA A SER CONTRATADO

INTRODUCCIÓN

El presente documento tiene como propósito determinar las necesidades mínimas informáticas del módulo o software de Gestión de Cartera de Impuestos del Municipio de Ibagué, que debe integrarse con el ERP PISAMI, propiedad de la Alcaldía de Ibagué en los módulos de Tesorería, Impuesto Predial Unificado, Industria y Comercio, Reteica, Otros Ingresos y Gestión Documental, buscando con ello optimizar los procesos de cobro y mejorar la eficiencia administrativa.

1. INTEGRACIÓN CON PISAMI:

1.1. Se establece como requerimiento específico la interoperabilidad con el sistema hacendario de la Alcaldía en cuanto a facturación, cartera, pagos, estados, terceros y gestión documental. La integración está dirigida al control de cartera de los impuestos así:

1.2. Forma de lectura de los CDLO o Liquidaciones oficiales de cobro entre el Software de Gestión y PISAMI. (Remisión, aprobación, devolución, Control y verificación, se propone vía API)

1.3. Forma de afectación de estados de Cobro hacia PISAMI. (Condiciones, Estados, Control y verificación, se propone vía API)

1.4. Forma de actualización y consolidación de terceros entre el Software de Gestión cartera y PISAMI (Control y verificación, se propone vía API)

1.5. Condiciones de facturación o liquidación de predios entre Gestión Cartera al realizar cambios catastrales en los predios en PISAMI. (Control y verificación, se propone vía API)

1.6. Forma de afectación a la facturación entre Gestión Cartera y PISAMI. (Conceptos, Control y verificación vía API?)

1.7. Forma de afectación de la Cartera desde Gestión Cartera hacia PISAMI. (Actualización, Control y verificación, se propone vía API)

1.8. Forma de afectación para los diferentes medios de pago PISAMI (PSE, Web Service y Archivo Plano) estableciendo el control y verificación de los pagos y su afectación hacia Tesorería y PISAMI, se propone vía API.

1.9. Forma de afectación con PISAMI Gestión Documental, para poder llevar la trazabilidad de los PQRS que lleguen a la dependencia y los tiempos de respuesta, se propone vía API.

1.10. Forma de notificación a los contribuyentes (registro y consulta), se debe especificar la integridad con el portal de la Alcaldía.

La integración con el ERP PISAMI requiere que se especifiquen los requerimientos de cada software, para definir las adaptaciones necesarias para integrar el software de Gestión de Cartera con PISAMI, lo que implica la presentación por parte de la Empresa del software de Gestión Cartera de los diccionarios de datos y manuales de integración, operación y control.

Este proceso fundamental desde el primer día de operación para garantizar la correcta afectación a las áreas tributarias y hacendarias, que repercute en la entrega y control de la información financiera que requiere la administración y todos los entes de control.

2. TIPO DE LICENCIAMIENTO

2.1. Municipio de Ibagué tendrá la titularidad de la licencia correspondiente al software, que otorga el derecho de utilización del software legal sin vigencia de caducidad.

2.2. Dentro del tipo de licenciamiento, la Alcaldía de Ibagué, tendrá derecho a recibir, sin costo adicional durante la vigencia del contrato, todas las actualizaciones de seguridad, correcciones de errores y mejoras funcionales del software.

3. **SOPORTE TECNOLÓGICO**

3.1. Brindar soporte tecnológico para la orientación de usuarios internos en el uso de las funcionalidades de la herramienta tecnológica, en la generación de reportes con información contenida en la plataforma y en la solución a solicitudes e incidentes de operación del software e inconsistencias en la información.

3.2. Disponer de una herramienta tecnológica o mesa de ayuda (Helpdesk), para proveer el soporte técnico relacionado con la solución ofrecida, cuya administración estará a cargo del MUNICIPIO, quien realizará la asignación de

usuarios, contraseñas, autorización de accesos y permisos.

3.3. Brindar soporte tecnológico para la orientación de usuarios externos en el uso de las funcionalidades de la herramienta tecnológica pública en la generación de recibos, paz y salvos, pagos y PQR, generación de reportes con información contenida en la plataforma y solución a solicitudes e incidentes de operación del software e inconsistencias en la información.

3.4. El canal de comunicación que debe almacenar todas las incidencias y atender el soporte lógico debe ser la mesa de ayuda o HelpDesk, sin embargo, los canales de la línea telefónica, el aplicativo web o el correo electrónico podrán ser utilizados para eventos de emergencia, no obstante, los requerimientos que se realicen por estas vías de comunicación deben ser trasladados a la mesa de ayuda para dejar la trazabilidad completa.

3.5. La gestión del servicio de soporte debe poder radicar, gestionar y escalar una incidencia o ticket, dejando el debido registro de la trazabilidad y seguimiento aplicando los tiempos de respuesta definidos en el acuerdo de nivel de servicios.

3.6. La herramienta tecnológica o mesa de ayuda de soporte (Helpdesk), debe permitir adjuntar documentos que soporten la solicitud y a su vez debe controlar los tiempos de respuesta de estos requerimientos en lo posible en forma de semáforo, de conformidad con los niveles de servicio acordados y generar el reporte por fechas de las incidencias o soportes.

3.7. Disponer de mínimo un ingeniero de soporte en horario laboral, por cada 30 usuarios que utilicen el Software de Gestión de Cartera, en su operación y un ingeniero de soporte en sitio

3.8. Brindar mínimo 50 horas de capacitación en el manejo operativo del sistema a los usuarios internos.

3.9. El soporte tecnológico tendrá los siguientes tiempos de atención por parte del CONTRATISTA:

Nivel de atención	Tipo Requerimiento	Condición	Tiempo Atención
Primer Nivel	Son situaciones de soporte funcional que no requieren ser escalados al grupo de desarrollo de software, la incidencia no afecta la operación del módulo reportado y/o suspenden el servicio parcial o totalmente.	Es atendido por la mesa de ayuda o personal de soporte, corresponde a situaciones de soporte funcional o capacitación. Este tipo de incidencia no afecta el servicio total o parcial del sistema de operación.	Hasta dos (2) horas hábiles después de haber registrado en el módulo asignado o informado por el medio autorizado.
Segundo Nivel	Son requerimientos de incidentes que afectan parcialmente los procesos.	Requiere intervención de profesional especializado de desarrollo y la actualización al módulo.	Hasta seis (6) horas hábiles después de haber registrado en el módulo asignado o informado por el medio autorizado.
Tercer nivel	Son requerimientos de incidentes que afectan la operación de los módulos que implican desarrollo, rediseño o ajustes debido a una nueva normatividad o mejora.	Requieren intervención de profesional especializado de desarrollo y la actualización al módulo.	Hasta ocho (8) horas hábiles después de haber registrado en el módulo asignado o informado por el medio autorizado.
Cuarto Nivel	Cuando se presenta una falla total del sistema que le impida prestar los servicios al software, esto quiere decir, una caída total del sistema, sin recuperación de servidores, disponibilidad de la red y sistemas de bases de datos.	Requiere intervención total del proveedor de la solución tecnológica que garantice el restablecimiento del servicio y la continuidad del proceso.	Inmediato, después de haber registrado en el módulo asignado o informado por el medio autorizado.
HORARIO DISPONIBILIDAD			

Nivel de atención	Tipo Requerimiento	Condición	Tiempo Atención
Lunes a viernes de 7:00 am a 5:00 pm en jornada continua. Y cuando se determine horario especial los días sábados o festivos, dispuesto por la Alcaldía e informado con mínimo dos (2) días de antelación.			

4. MOTOR DE BASE DE DATOS

4.1 El motor de base datos utilizado para el almacenamiento de la información generada a través de los servicios Cloud, debe ser una base de datos relacional en su versión más reciente y estable.

4.2 El proveedor debe especificar el motor de base datos utilizado.

4.3 Debe soportar transacciones ACID:

A (Atomicidad): La operación se ejecuta completa o no se ejecuta nada (no queda a medias).
C (Consistencia): Garantiza que los datos pasen de un estado válido a otro también válido.
I (Aislamiento): Cada transacción se ejecuta de manera independiente, sin interferencia de otras.
D (Durabilidad): Una vez confirmada una transacción, sus datos quedan guardados, incluso si hay una falla del sistema.

5 . LENGUAJE DE PROGRAMACIÓN

5.1 El contratista debe emitir una certificación del lenguaje de programación usado en el desarrollo del software y las versiones mínimas.

5.2 El contratista debe garantizar y certificar que todos los frameworks, librerías y componentes empleados en el desarrollo, implementación o mantenimiento del software han sido seleccionados y configurados de acuerdo con los lineamientos de desarrollo seguro establecidos por estándares internacionales reconocidos.

6. CARACTERÍSTICAS DEL SERVICIO EN LA NUBE

6.1 **Procesamiento:**

6.1.1 Hosting virtual de mínimo: 4 procesadores de doble núcleo, memoria RAM 16 GB, almacenamiento o disco de 960 GB SSD.

6.1.2 Escalabilidad: Debe permitir autoescalado vertical y horizontal

6.2 Almacenamiento:

6.2.1 Almacenamiento de BD: capacidad hasta 10 Terabytes de acuerdo con la necesidad total del sistema,
6.2.2 Disco sólido SSD con IOPS garantizado y redundancia.

6.3 Ancho de Banda

6.3.1 Ancho de banda 500 Mbps mínimo garantizado
6.3.2 Conectividad segura con certificado SSL por partner reconocido con huella digital y capacidad de encriptación de SHA-256 y SHA-2, la cual brinda una medida de seguridad para las transacciones electrónicas que realiza un usuario, mediante técnicas de encriptación los datos no pueden ser vulnerados por terceros.

7. MANTENIMIENTO:

7.1 Actualizar funcionalidades o características del sistema, las cuales serán establecidas conjuntamente entre el contratante y el contratista, con el objeto de poder brindar una correcta atención y disponibilidad de los servicios dados por la entidad territorial.

7.2 Las actualizaciones que requieran de ventanas de mantenimiento, serán programadas con previo visto bueno del supervisor

7.3 Las actualizaciones establecidas serán desarrolladas durante el término de ejecución del contrato de acuerdo a los niveles de servicio establecidos en el numeral 3.

7.4 Para las nuevas actualizaciones que surjan, se establecerán los alcances y viabilidad técnica a través de mesa de trabajo que se reunirá en un tiempo no mayor a 15 días calendario. De las conclusiones de este se dispondrá un instructivo de uso.

8. COPIAS DE RESPALDO

8.1 Backups diarios automáticos de la instancia, base de datos y documentos digitales o electrónicos

8.2 El contratista realizará la capacitación y acompañamiento a la Secretaría de las TIC para descargar la información.

8.3 Ejecutar y enviar el Backup o respaldos de datos y documentos digitales o electrónicos según las especificaciones definidas conjuntamente con las secretarias de hacienda y TIC:

8.4 El respaldo de datos se remitirá a la Alcaldía en un formato zip o rar que contenga la información en estructura de base de datos en formato SQL con hash de verificación (aún en las entregas automáticas), diccionario de datos y documentos digitales o electrónicos, en la periodicidad establecida y cuando se le requiera.

8.5 El Contratista deberá entregar a la Alcaldía un Manual de Especificación Técnica que detalle el procedimiento completo de generación y entrega del respaldo de información, incluyendo el diccionario de datos correspondiente. Este manual se elaborará conforme a los lineamientos acordados con la Secretaría de Hacienda y la Secretaría TIC, de modo que permita a estas dependencias recuperar la información en cualquier momento, de acuerdo con la Política de Seguridad de la Información y los requerimientos de los entes de control.

9. SEGURIDAD

9.1 Emisión de certificado de hosting emitido por partner reconocido.

9.2 Emisión de certificado de SSL emitido por partner reconocido

9.3 El sistema de información debe contener un módulo de administración de usuarios y módulo de auditoría que será gestionado o administrado por la Alcaldía de Ibagué, de conformidad con las políticas de seguridad de la información POL POL-SIG-502, numeral 9. Política control de Accesos y 12.7 Consideraciones sobre auditoría de sistemas de información.

9.4 Las pistas de auditoría deben permitir monitorear las conexiones a las bases de datos, en su ingreso, salida y modificaciones de los datos de manera directa o por medio del aplicativo de Gestión de Cartera.

9.5 Los Log de auditoría deben proporcionar información relevante para soportar procesos de auditoría y para contribuir al cumplimiento de las políticas de seguridad de la información

9.6 Instalación y actualización de parches de seguridad de los sistemas operativos que soporta la aplicación o correcciones críticas que afecten al Software, dentro de un plazo no mayor a diez (10) días hábiles contados desde su disponibilidad, generando un reporte que evidencie la actuación, en el que se describan las vulnerabilidades atendidas y el procedimiento de despliegue.

9.7 Monitoreo de vulnerabilidades: realizar, al menos trimestralmente, escaneos automáticos de vulnerabilidades o análisis de componentes de terceros en el Software contratado, documentando los resultados y presentado informe a la Alcaldía, indicando hallazgos de severidad alta o crítica y las acciones correctivas implementadas.

9.8 Registro de incidentes de seguridad: Mantener un registro inmodificable (bitácora) de los incidentes o eventos de seguridad detectados, incluyendo: fecha/hora, descripción del incidente, impacto estimado, acciones tomadas y fecha de cierre. Poner dicha bitácora a disposición de la Alcaldía dentro de un plazo máximo de cinco (5) días hábiles contados desde la incidencia.

9.9 Acceso seguro y autenticación: El Software debe contar con mecanismos de autenticación robustos (control de sesiones activas, caducidad de contraseñas y bloqueo por intentos fallidos) de conformidad con las políticas de seguridad de la información (9.2 Gestión de acceso a usuarios y 9.4.Gestión de acceso a sistemas y aplicaciones).

9.10 Firewall a través de grupos de seguridad con funcionamiento como un firewall virtual para las instancias EC2 y RDS los cuales permiten controlar y tomar medidas sobre el tráfico IP entrante y saliente, generando un reporte mensual de logs de seguridad. Firewall: Nueva Generación Virtual, Sesiones Concurrentes como mínimo 200.000.

9.11 Uso de WAF para proteger aplicaciones web de ataques comunes.

9.12 El proveedor deberá entregar e implementar un Plan de Continuidad del Servicio y Recuperación ante Desastres (BCP y DRP), que incluya sitios de respaldo (on-premise o cloud), tiempos máximos de recuperación (RTO) y pérdida aceptable de datos (RPO), y una simulación semestral documentada del plan.

10 PROTOCOLO DE MIGRACIÓN

10.1 El proveedor debe suministrar un documento que contenga el protocolo de migración, previamente aprobado por las secretarias de Hacienda y TIC, el cual debe incluir: Pasos detallados para exportar e importar datos, Validación de calidad e integridad de datos migrados, Roles y responsabilidades durante migración, Plan de retroceso en caso de falla, cronograma de pruebas piloto y validación en ambiente de preproducción.

11. ENTREGABLES

11.1 Respaldo Diario. Respaldo de datos de lo determinado en el numeral 8 y diccionario de datos.

11.2 Informe de incidencias y servicios estableciendo como mínimo: nivel de soporte, fecha de solicitud, solicitante, descripción de la solicitud, atendido por, fecha solución, causa o razón de la incidencia y solución generada. Soporte tecnológico numeral 3.

11.3 Informe de la instalación y actualización de parches de seguridad según lo descrito en el numeral 9.6

11.4 Reporte de monitoreo de vulnerabilidades del que trata el numeral 9.7

11.5 Informe de incidentes de seguridad mencionados en el numeral 9.8

11.6 Informe de las nuevas actualizaciones, incluyendo cronogramas, actas, estado de avances, manual de usuario según lo determinado en el numeral 7.3 Y 7.4

11.7 Informe mensual del firewall mencionado en el numeral 9.10

11.8 Informe de funcionamiento inicial de todos los módulos

11.9 Informe de funcionamiento final de todos los módulos

11.10 Informe de interoperabilidad definido en el numeral 1

11.11 Licencia de uso de Software

11.12 Certificado de hosting emitido por partner reconocido. Numeral 9.1

11.13 Certificado de SSL emitido por partner reconocido, numeral 9.2

11.14 Certificado de las capacidades del servicio de nube, back up, firewall, y motor

de base de datos Numeral 6 y 4.2

11.15 Certificado del lenguaje de programación y demás requerimientos del numeral 5.1

11.16 Documento que contenga el protocolo de migración. Numeral 10.1

11.17 Plan de continuidad de negocio. Numeral 9.12

11.18 Manual de usuario final, administrador y técnico en formato editable y PDF, Actualizado por versión.

12. ADICIONALES

12.1 Acuerdo de confidencialidad y transparencia de la información, conforme al modelo suministrado por la entidad, que será proporcionado dentro de la ejecución del contrato.

12.2 Acuerdo de cumplimiento de las políticas de seguridad de la información y protección de datos, conforme al modelo proporcionado por la entidad, indicando el acto administrativo de su adopción, que será suministrado dentro de la ejecución del contrato.

12.3 Toda novedad o desarrollo que se efectué con ocasión del presente contrato, para la entrega de información deberá conservar la estructura solicitada en el presente documento y anexada de ser necesario a los diccionarios de datos, los manuales de control y operación así como a los backup y el documento de protocolo de migración.

PARÁGRAFO PRIMERO. Es menester determinar los tiempos previstos para la entrega de los productos con las calidades solicitadas por el contratante, de acuerdo a lo anterior es necesario partir de la suscripción del acta de inicio, momento en el cual las partes del contrato Supervisores y Contratista mediante acuerdo construyan y materialicen el cronograma de entrega de los productos discriminados derivados de las obligaciones específicas, se aclara que estas entregas no serán los REPORTES de actividades para el cobro de las cuentas, sino la entrega de lo solicitado en las obligaciones citadas teniendo en cuenta la calidad y los tiempos acordados entre las partes. Finalmente, se hace hincapié que estos productos serán parte del insumo para las diferentes cuentas de cobro.

PARÁGARAFO SEGUNDO: El Proveedor debe aportar certificación de cumplimiento de la norma ISO IEC 25000, ISO 27001, ISO 29119 e ISO IEC 25012 o en su defecto aportar certificación en la cual declara y garantiza que el software

objeto del contrato ha sido desarrollado siguiendo buenas prácticas de desarrollo seguro, basadas en estándares y guías internacionalmente reconocidos, con el propósito de minimizar vulnerabilidades y asegurar la confiabilidad, integridad y confidencialidad de la solución.

El proveedor una vez se culmine el plazo de ejecución del contrato deberá garantizar la continuidad del acceso al servicio a la nube de Gestión de Cartera y soporte remoto por un término no menor a 30 días calendario contados a la fecha de finalización del contrato, la cual no incluye el servicio de mantenimiento y actualización de la plataforma.

13 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

El CONTRATISTA se obliga y compromete a desarrollar las siguientes obligaciones:

13.1 Utilizar la información confidencial para el desarrollo del objeto establecido en el presente clausulado.

13.2 No podrá revelar ni entregar a terceros ninguna información confidencial, total ni parcialmente, salvo autorización previa, expresa y escrita por parte de, para cada caso.

13.3 Al finalizar las actividades encomendadas deberá entregar la información inmediatamente al MUNICIPIO de acuerdo al manual.

13.4 Guardar confidencialidad sobre esa información y no emplearla en beneficio propio o de terceros mientras conserve sus características de confidencialidad o mientras sea manejada por EL MUNICIPIO hasta que una autoridad competente lo requiera.

PARÁGRAFO PRIMERO: El Contratista en su calidad de proveedor del software de gestión de cartera, será responsable por los errores en el funcionamiento del sistema, pérdida de datos, inexactitudes en el procesamiento de la información tributaria o cualquier detrimento patrimonial que se cause al MUNICIPIO, cuando dichos eventos sean atribuibles a fallas en el software, defectos técnicos, omisiones en el mantenimiento, errores de programación, fallas en actualizaciones o deficiencias en el soporte técnico proporcionado.

PARÁGRAFO SEGUNDO: El contratista se obliga a garantizar el principio de reversibilidad, , asegurando que, en caso de terminación, cesión o no renovación del contrato, voluntaria o anticipada, por cualquier causa, se realizará la entrega íntegra, ordenada, actualizada y accesible de toda la información y datos

generados, almacenados o procesados por el software durante la vigencia del contrato.

Esta obligación incluye, sin limitarse a:

a) La entrega, sin costo adicional, de la totalidad de los datos en un formato estructurado, interoperable y reutilizable (por ejemplo, CSV, XML o JSON), y documentos digitales o electrónicos acompañado de su respectiva documentación técnica que permita su uso por parte del MUNICIPIO o de un nuevo proveedor.

b) La transferencia de los registros históricos, logs de auditoría, trazabilidad y configuraciones aplicadas, garantizando su integridad, disponibilidad y no alteración.

Documento inicial del 2024/04/29

Elaborado por: Ingeniera Doris Galeano Profesional Especializado

Ingeniero Diego Aranguren Asesor Despacho

Documento Actualizado el 2024/06/11

Actualizado por: Ingeniero Diego Aranguren Asesor Despacho

Documento Actualizado el 2025/06/03

Actualizado por: Ingeniera Doris Galeano Profesional Especializado

Ingeniero Diego Aranguren Asesor Despacho

VILMA YANETH RIVERA MARROQUIN
Secretaria de las TIC

Redactó: Doris Galeano
Diego Aranguren P