FORMULARIO DE RESPUESTAS A LAS OBSERVACIONES PRESENTADAS AL PROYECTO DE PLIEGO DE CONDICIONES DENTRO DEL PROCESO SDA-SASI-20260011

OBJETO: REALIZAR EL MANTENIMIENTO, ACTUALIZACIÓN Y SOPORTE TÉCNICO EN LA HERRAMIENTA PARA LA MESA DE SERVICIOS DE LA SDA

OBSERVANTE 1: SUMIMAS

Observación No. 1:

Componente Aranda Software Local Connector VPN

Síntesis de la observación: *Se solicita aclarar si el componente hace parte de la solución actual, su finalidad y relación con ASMS y ADM, si requiere renovación de licenciamiento, soporte o actualización, y si debe ajustarse el alcance técnico y económico.*

Respuesta Observación 1:

Revisada la observación, la Entidad aclara lo siguiente:

1) Uso actual. La Entidad confirma que, en la parametrización base del servicio vigente, la autenticación de la plataforma Aranda con su Directorio Activo se realiza mediante una conexión VPN. Esta conexión se encuentra instalada, habilitada y en uso. La Entidad no determina que esta conexión corresponda al componente denominado “Aranda Software Local Connector VPN” ni a ningún otro componente específico del catálogo del fabricante; la presente respuesta se refiere a la función descrita (conexión de autenticación con el Directorio Activo) y no a un componente comercial determinado. En todo caso, si el fabricante provee dicha función mediante el componente mencionado, este se entiende comprendido en lo aquí descrito..

2) Finalidad y relación con los productos. La conexión permite la autenticación de usuarios y agentes de la mesa de servicios con el Directorio Activo de la Entidad y la sincronización con éste (Condiciones Técnicas: “Sincronización de la herramienta provista con el Directorio Activo (Ldap) de la Entidad”, y módulo de Autogestión de Contraseñas). Se relaciona con la plataforma Aranda Service Management Suite – ASMS; no tiene relación ni dependencia con Aranda Device Management – ADM. La Entidad precisa que esta conexión se emplea exclusivamente para la comunicación de la plataforma con el Directorio Activo de la Entidad (autenticación de usuarios y agentes, sincronización de usuarios y autogestión de contraseñas): no existen otros servicios

que dependan de ella, ni un mecanismo de autenticación alterno, ni desarrollos o integraciones que impliquen un uso adicional de este servicio.

3) Renovación, soporte y actualización. Dado que la renovación tiene por propósito conservar la configuración actualmente operativa (obligaciones específicas 4 y 5 y numeral 1.7 de la Ficha Técnica), esta conexión se considera incluida dentro de la parametrización propia de la renovación y de la garantía de continuidad y disponibilidad de la plataforma (numerales 1.2 y 1.3). En consecuencia, no requiere licenciamiento, soporte ni actualización por separado, ni constituye un ítem adicional, y su costo se entiende incorporado en el valor de los ítems de renovación ofertados.

4) Ajuste de especificaciones. Al estar incluida en la renovación, no es necesario ajustar las especificaciones técnicas ni económicas del proceso; las cantidades y los ítems relacionados en la Ficha Técnica se mantienen. La red y el Directorio Activo de la Entidad permanecen bajo su administración; al contratista, directamente o a través del fabricante, le corresponde mantener, validar y, de ser necesario, reconfigurar la conexión del lado de la plataforma en la nube, de modo que la autenticación y la sincronización se conserven tal como operan actualmente.

OBSERVANTE 2 : EYC INGENIEROS S.A.S.

Observación No. 1:

La ficha técnica y el proyecto de pliego contemplan el diagnóstico, configuración y parametrización de diversos módulos alineados con ITIL v4, pese a que la necesidad contractual corresponde a la renovación de una plataforma existente. Técnicamente, la validación de configuraciones ya operativas difiere sustancialmente de implementar procesos nuevos, migrar flujos, construir automatizaciones o desarrollar integraciones. Esta indefinición afecta las horas de ingeniería, el plan de trabajo y la estimación económica.

Solicitamos a la Entidad identificar los módulos actualmente implementados, su versión y estado de operación, y aclarar si la obligación comprende únicamente diagnóstico, ajustes y actualización de configuraciones existentes. En caso de requerirse nuevas parametrizaciones, solicitamos definir para cada proceso los entregables, número de flujos, reglas, formularios, integraciones y criterios de aceptación.

Respuesta Observación 1:

Revisada la observación, la Entidad aclara lo siguiente: La Entidad informa que los componentes actualmente implementados y en operación, en modalidad SaaS, son: Aranda Service Management Suite – ASMS (especialistas y usuarios), versión 9.12.0.61; Aranda CMDB, versión 9.12.0.61; Aranda Query Manager – AQM, versión 9.43.1.7; y Aranda Device Management – ADM, versión 9.25.1.16. A través de ellos se prestan los procesos ITIL v4 relacionados en el numeral 1.7 de la Ficha Técnica.

Por tratarse de la renovación de una plataforma existente y operativa, la obligación comprende únicamente: (i) el diagnóstico inicial sobre el estado de los módulos (obligación específica 9); (ii) la conservación y validación de las configuraciones existentes; y (iii) los ajustes, pruebas y actualización derivados de las versiones estables y mejoras que libere el fabricante durante la garantía (obligaciones específicas 4, 5 y 8).

No se requieren nuevas parametrizaciones, configuraciones de flujos, reglas, formularios, automatizaciones ni integraciones; por ello no se definen entregables por número de flujos o reglas. Las únicas actividades adicionales son las enumeradas en la Ficha: los seis (6) reportes en el módulo AQM (numeral 1.11), la asesoría de integración para el chatbot institucional mediante APIs, la asesoría en elaboración de reportes y la transferencia de conocimiento.

Observación No. 2:

En el numeral 1.2.3 del proyecto de pliego se solicita una certificación expedida directamente por el fabricante que acredite al oferente como distribuidor o partner autorizado para comercializar, renovar, implementar y soportar Aranda ASMS en Colombia. Respetuosamente solicitamos complementar dicho requisito, exigiendo que el oferente acredite, como mínimo, la categoría Silver Partner del fabricante, siempre que esta denominación corresponda a una categoría vigente y verificable dentro de su programa de canales.

La renovación objeto del proceso no se limita a la entrega de licencias: incorpora continuidad de operación en modalidad SaaS, actualización de componentes, parametrización, soporte especializado y escalamiento de incidentes. Por tanto, resulta técnicamente pertinente verificar que el canal dispone de una relación formal y activa con el fabricante, así como de capacidades demostrables para acceder a rutas de escalamiento, actualizaciones, transferencia de conocimiento y recursos de soporte del producto. Una categoría reconocida dentro del programa de canales puede servir como evidencia complementaria de estas capacidades, sin reemplazar la verificación de personal competente ni los acuerdos de soporte.

Solicitamos incluir en el numeral 1.2.3 la acreditación mínima de Silver Partner, mediante certificación vigente emitida directamente por Aranda Software, que identifique expresamente la categoría y su vigencia.

Respuesta Observación 2:

Se acoge parcialmente la observación. La Entidad mantiene como requisito la certificación emitida directamente por el fabricante, con antigüedad no mayor a 30 días calendario, que acredita al oferente como distribuidor o partner autorizado para comercializar, renovar, implementar y prestar soporte técnico del software Aranda ASMS en Colombia. Dicha certificación ya acredita la relación formal y activa con el fabricante que el observante busca verificar.

Para complementar la verificación, el requisito se ajustará para que la certificación indique la categoría o nivel que ostenta el oferente, dentro del programa de canales del fabricante, cuando éste lo contemple, y su vigencia, con carácter informativo: su ausencia, cuando el programa de canales no la contemple, no será causal de rechazo. Se admitirá una certificación general vigente de distribuidor o partner autorizado en Colombia, de modo que la participación de los canales no dependa de una decisión del fabricante en este proceso en particular. No se exigirá una categoría mínima (como Silver Partner), por cuanto se trata de una clasificación comercial del programa de canales y no de una medida técnica definida por la Entidad; exigirla como mínimo restringiría la libre concurrencia de oferentes habilitados por el fabricante sin ser necesaria para garantizar el servicio. La capacidad de soporte se verifica con las obligaciones del proceso: soporte técnico especializado y certificado por el fabricante, escalamiento de Nivel 3 al fabricante con seguimiento hasta el cierre, y cumplimiento de los tiempos de la Tabla 2.

Lo anterior se verá reflejado en los documentos precontractuales.

Observación No. 3:

La ficha técnica fija para incidentes críticos atención de 30 minutos y solución de 1 hora y 30 minutos bajo cobertura 7×24. Sin embargo, en una arquitectura SaaS determinadas fallas de infraestructura, indisponibilidad de plataforma, defectos de producto y restauraciones pueden depender exclusivamente del fabricante, fuera del control directo del integrador. Una obligación de solución sin distinguir la causa raíz puede resultar técnicamente imposible de garantizar.

Solicitamos precisar el punto de inicio y suspensión del cómputo de ANS, distinguir tiempos de respuesta, diagnóstico, escalamiento, mitigación y solución definitiva, y establecer tratamiento diferenciado para incidentes cuya corrección dependa del fabricante o de servicios de terceros. Proponemos medir al contratista sobre actividades bajo su control y exigir trazabilidad del escalamiento y seguimiento hasta el cierre.

Respuesta Observación 3:

Revisada la observación por parte de la Entidad, no se acepta. La Ficha Técnica ya prevé el cómputo y el tratamiento diferenciado que el proponente solicita:

• Inicio del cómputo: el tiempo de atención se cuenta desde la fecha y hora de registro del caso en el MSC por parte de la Entidad, hasta el primer contacto del contratista, quien emite el diagnóstico, plan de acción o solución. Los casos críticos con cobertura 7x24 se reportan por vía telefónica.

• Tiempos diferenciados: la Tabla 2 separa el tiempo de atención (contacto inicial, análisis y diagnóstico) del tiempo de solución.

• Causa raíz: la Tabla 1 asigna las prioridades P1 y P2 únicamente a fallas atribuibles exclusivamente al software provisto por el contratista; los eventos ajenos a la plataforma no se miden bajo esas prioridades.

• Escalamiento al fabricante: el Nivel 3 dispone que el contratista escala el caso, realiza el seguimiento hasta su solución e informa al supervisor del estado y avance, con trazabilidad.

• Suspensión: cuando la solución definitiva no pueda darse en el tiempo de la Tabla 2, la Nota 2 permite acordar con la Entidad la fecha y hora de entrega de la solución; el caso se suspende y no afecta los indicadores, salvo que se reitere, caso en el cual se reabre.

Con ello, el tiempo de solución se mide conforme a la Tabla 2. Cuando la solución definitiva dependa del fabricante, el contratista deberá acreditar el escalamiento y podrá acordarse con el supervisor la fecha de solución en los términos de la Nota 2, sin que ello lo exima de su responsabilidad frente a la Entidad.

Observación No. 4:

Considerando que el objeto contractual comprende mantenimiento, actualización, atención de incidentes, requerimientos y soporte técnico de una herramienta que respalda la mesa de servicios de la entidad, solicitamos incorporar como requisito habilitante técnico que el oferente cuente con certificación vigente ISO/IEC 20000-1, correspondiente al sistema de gestión de servicios.

Esta norma establece requisitos para planificar, diseñar, transicionar, entregar y mejorar servicios de TI bajo un sistema de gestión verificable. Su pertinencia para el proyecto se refleja en la necesidad de administrar niveles de servicio, incidentes, solicitudes, cambios, relaciones con proveedores y mejora continua, particularmente cuando existen compromisos de atención y solución, escalamiento al fabricante y continuidad operativa durante doce meses. La certificación aporta evidencia independiente de que estos procesos se gestionan de manera sistemática y no dependen exclusivamente de prácticas informales.

Solicitamos que la certificación sea emitida por organismo de certificación acreditado, esté vigente al cierre del proceso, identifique al oferente y tenga un alcance relacionado con la prestación, operación o soporte de servicios de tecnologías de la información. Se sugiere verificar expresamente el alcance certificado para evitar que una certificación de actividades ajenas al contrato se considere suficiente.

Respuesta Observación 4:

Revisada la observación por parte de la Entidad, no se acepta, por las siguientes razones: La Entidad considera que exigir la certificación ISO/IEC 20000-1 como requisito habilitante no es necesario ni proporcional al objeto del proceso, que consiste en la renovación de la suscripción SaaS de una plataforma existente y la prestación de soporte y mantenimiento sobre ella. Conforme al artículo 5, numeral 1, de la Ley 1150 de 2007 y al artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015, los requisitos

habilitantes deben ser adecuados y proporcionales a la naturaleza y al valor del contrato, y el Manual para determinar y verificar los requisitos habilitantes de Colombia Compra Eficiente orienta a no exigir condiciones innecesarias para verificar la aptitud del proponente**.** Exigir esta certificación limitaría la concurrencia de oferentes autorizados por el fabricante, sin ser indispensable para garantizar la ejecución

La calidad del servicio se asegura con las obligaciones y mecanismos ya previstos: soporte técnico especializado y certificado por el fabricante, niveles de atención y tiempos de solución por prioridad (Tablas 1 y 2), escalamiento al fabricante con seguimiento hasta el cierre, garantía de disponibilidad del 99,6 %, informes de seguimiento y las garantías contractuales de cumplimiento y calidad del servicio. Si el oferente cuenta con la certificación, podrá aportarla, sin que constituya requisito ni otorgue ventaja en la evaluación.

Observación No. 5:

Las obligaciones específicas 1.8 y 1.9 requieren un plan de contingencia en cinco días hábiles y contemplan planes BCP/DRP y posibles pruebas. Dado que la infraestructura SaaS es administrada por el fabricante, el contratista puede documentar y ejecutar procedimientos de coordinación y escalamiento, pero no necesariamente administrar los respaldos, la replicación o la recuperación física y lógica del servicio.

Solicitamos precisar que el BCP/DRP exigido al contratista corresponde a los procedimientos de continuidad del servicio contratado, coordinación, comunicaciones, escalamiento y recuperación dentro de sus competencias, pudiendo soportarse en los planes y certificaciones del fabricante. También solicitamos especificar los RTO/RPO aplicables y el alcance, frecuencia y responsabilidades de cualquier prueba requerida.

Respuesta Observación 5:

Revisada la observación, la Entidad precisa lo siguiente: El plan de contingencia exigido al contratista (numerales 1.8 y 1.9) corresponde a los procedimientos de continuidad del servicio contratado: coordinación, comunicaciones, escalamiento y recuperación dentro de las competencias del contratista, y podrá soportarse en los planes y certificaciones del fabricante aplicables al servicio SaaS. La administración de la infraestructura y la ejecución de los respaldos y de la replicación del servicio están a cargo del fabricante; el contratista garantiza ante la Entidad que se realicen, conforme al numeral 2.4, y responde por su gestión y acreditación.

Los objetivos de tiempo y punto de recuperación (RTO/RPO) serán los de la política vigente del fabricante para el servicio, que el contratista deberá informar al supervisor; la Entidad no fija valores propios. En cuanto a las pruebas, el numeral 1.9 no exige la ejecución de pruebas periódicas: la Entidad se reserva la potestad de solicitar la evidencia de los resultados del más reciente plan ejecutado, que podrá ser el del fabricante.

Observación No. 6

La ficha técnica incorpora obligaciones relacionadas con rendimiento, seguridad, escalabilidad y funcionalidades integradas. En un entorno SaaS compartido, las pruebas de estrés intrusivas o las evaluaciones de infraestructura subyacente pueden estar restringidas por las políticas del fabricante, y no todas las interfaces o ambientes están bajo control del contratista.

Solicitamos precisar las pruebas efectivamente exigibles al contratista, sus métricas y criterios de aceptación, el ambiente autorizado, los límites de carga y la necesidad de autorización previa del fabricante. Proponemos aceptar evidencias técnicas oficiales del proveedor SaaS para controles y pruebas sobre infraestructura que no sea administrada directamente por el contratista.

Respuesta Observación 6:

Revisada la observación, la Entidad la acoge y precisa lo siguiente: Las verificaciones del numeral 1.1 son pruebas funcionales de desempeño sobre el servicio contratado (carga de usuarios, recurrencia, usabilidad y escalabilidad), no intrusivas, y no comprenden evaluaciones de la infraestructura subyacente administrada por el fabricante. Se realizarán en la ventana y condiciones acordadas con el supervisor y, cuando las políticas del fabricante lo requieran, previa autorización de éste y sin exceder los límites de carga que establezca.

El criterio de aceptación es el informe técnico que consolide la metodología, los resultados y las conclusiones, validado por el supervisor. Para los controles y pruebas sobre infraestructura que no administre directamente el contratista, se aceptará evidencia técnica oficial del fabricante.

Observación No. 7

El proceso diferencia un plazo contractual de ejecución limitado y un período de 12 meses de suscripción, mantenimiento y soporte desde la activación. Esta estructura requiere identificar qué entregables deben recibirse durante la ejecución y cuáles se cumplen durante la garantía, para evitar exigir anticipadamente actividades que dependen de solicitudes posteriores o de eventos futuros.

Solicitamos publicar una matriz de hitos y entregables que separe activación de licencias, diagnóstico, parametrizaciones, transferencia de conocimiento, informes, seis reportes AQM y soporte de garantía, indicando para cada actividad su plazo, responsable, evidencia y mecanismo de recibo a satisfacción. Confirmar que las obligaciones de soporte durante los 12 meses no se consideran incumplidas por no estar ejecutadas al cierre del primer mes contractual.

Respuesta Observación 7:

Una vez revisada la observación, se acepta. La Entidad se permite presentar la siguiente matriz, elaborada con las obligaciones y entregables de la Ficha Técnica, que no los modifica; en caso de discrepancia, prevalecerá lo establecido en la Ficha Técnica y en el Estudio Previo:

Hito / entregable	**Plazo**	**Responsable**	**Evidencia**	**Recibo a satisfacción**
Renovación y activación de la suscripción SaaS y habilitación de las licencias	Dentro del plazo de ejecución (1 mes desde el acta de inicio)	Contratista (con el fabricante)	Certificación del fabricante (Entregable 1)	Validación del supervisor
Cronograma de actividades, (obligación 4)	5 días hábiles desde el acta de inicio	Contratista	Cronograma	Aprobación del supervisor
Plan de contingencia (numeral 1.8)	5 días hábiles desde el acta de inicio	Contratista	Documento del plan	Supervisor
Diagnóstico inicial de los módulos (obligación 9)	Al inicio del contrato, dentro del plazo de ejecución	Contratista	Informe de diagnóstico	Supervisor
Arquitectura y manuales (numerales 2.5 y 2.6; Entregables 2 y 3)	Primeros 20 días desde el acta de inicio	Contratista	Documentos (admite documentos oficiales del fabricante)	Supervisor
Verificación de configuración, activación y acceso (1.6) y pruebas funcionales de desempeño (1.1)	Dentro del plazo de ejecución	Contratista	Informe escrito e informe técnico	Supervisor
Transferencia de conocimiento: 3 sesiones de 2 horas (1.5; Entregable 4)	Dentro del plazo de ejecución	Contratista	Material audiovisual de las sesiones	Supervisor
Mecanismo de acceso de solo lectura a los datos (Entregable 5)	Dentro del plazo de ejecución	Contratista (con el fabricante)	Documento de entrega de credenciales o del mecanismo equivalente	Supervisor

Hito / entregable	Plazo	Responsable	Evidencia	Recibo a satisfacción
Seis reportes AQM (1.11; Entregable 7)	Solicitudes dentro del plazo de ejecución; entrega en la ejecución o en la garantía; informe de avance dentro de la ejecución	Contratista; la Entidad solicita por escrito	Reportes publicados y funcionando; informe de reportes	Acta de recibo a satisfacción del supervisor
Compromiso de soporte firmado por el representante legal (Entregable 8)	Dentro del plazo de ejecución	Contratista	Documento firmado	Supervisor
Soporte y mantenimiento durante la garantía (numeral 2; Tablas 1 y 2); reporte de casos escalados cuando se requiera (Entregable 6)	12 meses desde la activación de la suscripción	Contratista	Casos atendidos y reportes de escalamiento	Informes de ejecución del supervisor
Informe final de disponibilidad y tiempos de caída (Entregable 9)	Al finalizar el período de garantía	Contratista	Informe con indicadores de disponibilidad	Supervisor

Se confirma que las obligaciones de mantenimiento y soporte durante los doce (12) meses de la garantía, contados desde la activación de la suscripción, no se consideran incumplidas por no estar ejecutadas al cierre del plazo de ejecución de un (1) mes, conforme a la nota del plazo de ejecución de la Ficha Técnica. Tampoco se exigirán anticipadamente actividades que dependan de solicitudes posteriores o de eventos futuros, como los reportes AQM pendientes (que pueden entregarse en la garantía) o las actualizaciones del fabricante

Observación No. 8

Dado que la solución Aranda ASMS se presta en modalidad SaaS y procesa información asociada a usuarios, activos, incidentes, solicitudes y configuraciones de la entidad, solicitamos incorporar como requisito técnico la acreditación de controles de seguridad para servicios en la nube conforme a ISO/IEC 27017, mediante certificación o atestación verificable aplicable al alcance del servicio.

ISO/IEC 27017 proporciona directrices de controles de seguridad de la información específicas para servicios en la nube, complementando los controles generales de ISO/IEC 27002. En este contrato son relevantes la segregación de responsabilidades entre proveedor SaaS y contratista, el control de accesos privilegiados, la protección de información durante administración y soporte, la gestión de cambios, el registro de actividades y el tratamiento de incidentes de seguridad en entornos

compartidos. Estas medidas reducen riesgos de exposición, alteración o indisponibilidad de la información y favorecen la trazabilidad de las actividades técnicas.

Solicitamos que el oferente acredite la aplicación de ISO/IEC 27017 dentro de un sistema de gestión de seguridad de la información con alcance pertinente a los servicios de nube que administra o soporta. Como ISO/IEC 27017 es una guía de controles y no una norma autónoma de requisitos de certificación equivalente a ISO/IEC 27001, se propone admitir evidencia formal verificable por ejemplo, certificado ISO/IEC 27001 con alcance y declaración de aplicabilidad que incluya controles ISO/IEC 27017, o atestación independiente equivalente. Cuando los controles de infraestructura SaaS dependan directamente de Aranda, deberá admitirse también evidencia del fabricante, junto con la delimitación documentada de responsabilidades del oferente.

Respuesta Observación 8:

Revisada la observación por parte de la entidad, no se acepta. Conforme al artículo 5, numeral 1, de la Ley 1150 de 2007 y al artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015, los requisitos habilitantes deben ser adecuados y proporcionales a la naturaleza y al valor del contrato; la seguridad de la información se exige y verifica como obligación de ejecución, en los términos que se indican a continuación. La Entidad reconoce que ISO/IEC 27017 es una guía de controles de seguridad para servicios en la nube y no una norma certificable autónoma. La seguridad del servicio y de los datos ya se exige en la Ficha Técnica: integridad, confidencialidad, cifrado, trazabilidad y disponibilidad de los datos, y protección con firewall, antivirus y detección de intrusos (numeral 1.4); respaldos conforme a ISO/IEC 27001 y a la Ley 1581 de 2012 (numeral 2.4); y el compromiso de confidencialidad y seguridad de la información (obligación 11).

Para la infraestructura SaaS administrada por el fabricante, se aceptarán las políticas, certificaciones e informes oficiales vigentes del fabricante, junto con la delimitación de responsabilidades prevista en el numeral 1.3 de la Ficha Técnica, sin que se exija al oferente una acreditación adicional.

OBSERVANTE 3 : NETWORKTEC

Observación No. 1

Numerales objeto de la observación

Numeral 5.2.5 «Requerimientos adicionales» de los Estudios Previos; obligaciones específicas No. 6 y No. 7 (soporte Nivel 3 a través de partner autorizado); Entregable No. 1; Condiciones Técnicas de la Ficha Técnica.

Texto que se solicita incorporar

El oferente debe ser como mínimo Partner silver de la solucion ofertada, garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe Anexar la Certificación del Fabricante junto a su propuesta la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.

Fundamento técnico

1. *La condición de «partner autorizado» no acredita por sí sola capacidad técnica. El numeral 5.2.5 exige únicamente que el oferente sea distribuidor/partner autorizado, sin distinguir su nivel. Sin embargo, el fabricante segmenta su canal en Colombia en categorías (Gold y Silver), cuya diferencia está en la cuota de ventas y, sobre todo, en que ambos niveles deben contar con personal comercial y técnico certificado en la solución. Un aliado sin categoría puede comercializar la renovación sin disponer de ingenieros certificados, lo que no es coherente con lo que exige el contrato. Fijar el nivel Silver como mínimo equivale a exigir el primer escalón del programa que garantiza personal técnico certificado; no se exige el nivel más alto.*
2. *Coherencia con la obligación específica No. 6. La Entidad exige «soporte técnico especializado y certificado por parte del fabricante para la totalidad de los módulos contratados». El nivel de partner es la forma objetiva en que el propio fabricante acredita que el oferente tiene esa certificación técnica sobre los módulos de ASMS (Consola de Administración, CMDB, ADM, AQM, entre otros).*
3. *Escalamiento Nivel 3 y cumplimiento de ANS. La obligación No. 7 define que el Nivel 3 lo presta el fabricante «canalizado a través de EL CONTRATISTA en su calidad de partner autorizado». La Tabla 2 exige para casos críticos atención en 30 minutos y solución en 1 hora 30 minutos, con cobertura 7x24. Estos tiempos solo son alcanzables si el partner resuelve la mayor parte de los casos con su propio equipo certificado y tiene canales formales de escalamiento prioritario ante el fabricante, condiciones asociadas a los niveles categorizados del canal.*
4. *Complejidad del licenciamiento. El contrato no es una venta estándar: implica renovar en modalidad SaaS un licenciamiento perpetuo adquirido en 2016 sobre Aranda Service Desk V8, cuya equivalencia con ASMS 9 fue certificada por el fabricante el 7 de mayo de 2025, con cambio de nomenclatura (19 usuarios concurrentes, 10 nombrados y 1.200 ADM, Tabla 3). El Entregable No. 1 exige además una certificación del fabricante que relacione la renovación de todos los productos adquiridos a perpetuidad. Un partner con experiencia en licenciamiento de las diferentes soluciones del fabricante reduce el riesgo de errores de equivalencia, licencias no habilitadas o demoras en la activación.*
5. *Tiempo de respuesta en la provisión de la solución. La renovación, actualización y transferencia de conocimiento deben completarse en máximo un (1) mes, y la Entidad se encuentra en contingencia desde el vencimiento de la suscripción anterior. La referencia al menor tiempo de*

respuesta en el suministro cobija la activación de las licencias y el despliegue de los agentes de Aranda Device Management sobre los 1.200 equipos de cómputo de la Entidad, actividades que un partner categorizado ejecuta con prioridad ante el fabricante.

6. *Certificación a nombre de la Entidad y con vigencia no mayor a 30 días. Una carta genérica de distribución puede haber sido expedida para otro proceso o haber perdido vigencia. La certificación dirigida a la SDA confirma que el fabricante conoce el proceso y respalda al oferente para este contrato específico, y la fecha reciente acredita que el nivel de partner está vigente al momento de ofertar. Este plazo es el mismo que la Entidad ya adoptó en el numeral 5.2.5, por lo que no introduce una carga nueva.*

Fundamento jurídico

El artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015 ordena que los requisitos habilitantes sean adecuados y proporcionales a la naturaleza y al valor del contrato. El requisito solicitado se relaciona directamente con las obligaciones 6 y 7 y con los ANS de la Tabla 2, es verificable de forma objetiva (cumple / no cumple) y no otorga puntaje, en los términos del artículo 5 de la Ley 1150 de 2007. Tampoco restringe la competencia: existen varios partners Gold y Silver en Colombia, el nivel exigido es el mínimo categorizado y, en caso de proponentes plurales, puede mantenerse la regla de la Nota 1 del numeral 5.2.5 (que al menos uno de los integrantes lo acredite). Su inclusión desarrolla los principios de planeación y responsabilidad (artículos 25 y 26 de la Ley 80 de 1993) y el deber de fijar reglas objetivas, justas y claras (artículo 24, numeral 5, de la misma ley).

Solicitud concreta

Incorporar el texto propuesto en el numeral 5.2.5 de los Estudios Previos, en el pliego de condiciones definitivo y en las Condiciones Técnicas de la Ficha Técnica, manteniendo las Notas 1 y 2 actuales de dicho numeral

Respuesta Observación 1:

Revisada la observación, la Entidad la acoge parcialmente. La Entidad mantiene como requisito la certificación emitida directamente por el fabricante, con antigüedad no mayor a 30 días calendario, que acredita al oferente como distribuidor o partner autorizado para comercializar, renovar, implementar y prestar soporte técnico del software Aranda ASMS en Colombia. Se ajustará el numeral 5.2.5 del Estudio Previo en dos aspectos: (i) no se exigirá que la certificación esté expedida a nombre de la Secretaría Distrital de Ambiente ni dirigida al presente proceso, y se admitirá una certificación general vigente de distribuidor o partner autorizado en Colombia, de modo que la designación de los canales que participan no dependa de una decisión del fabricante en este proceso en particular (artículo 24, numeral 5, de la Ley 80 de 1993; artículo 5 de la Ley 1150 de 2007); y (ii) deberá indicar la categoría o nivel que ostenta el oferente dentro del programa de canales del fabricante, cuando éste lo contemple, y su vigencia, con carácter meramente informativo: su ausencia, cuando el programa de canales no la contemple, no será causal de rechazo. Se mantienen las Notas 1 y 2 de dicho numeral, lo cual se verá reflejado en los documentos precontractuales.

No se acoge la exigencia de una categoría mínima (Silver), por las siguientes razones:

1. El observante señala que la diferencia entre las categorías del canal radica en la cuota de ventas y en contar con personal certificado por el fabricante. En cuanto a la cuota de ventas, se trata de una clasificación comercial del programa de canales y no de una medida técnica definida por la Entidad. En cuanto al personal certificado, la Entidad no lo deja a la categoría del partner: lo exige directamente como obligación de ejecución, esto es, soporte técnico especializado y certificado por el fabricante para la totalidad de los módulos (obligación 6), cuyo cumplimiento se verifica durante la supervisión del contrato. De este modo, la capacidad técnica que el observante busca asegurar con la categoría Silver queda garantizada de forma más directa que con una categoría comercial, que no implica por sí misma que el personal asignado al contrato esté certificado, y sin restringir la concurrencia de oferentes autorizados por el fabricante.

2. El Nivel 3 de soporte lo presta el fabricante, canalizado por el contratista, quien escala el caso, hace seguimiento hasta su solución y responde ante la Entidad (obligación 7). Ese escalamiento depende de la relación formal y activa del partner con el fabricante, que la certificación exigida acredita, y no de una categoría comercial.

3. La equivalencia del licenciamiento adquirido en 2016 con ASMS ya fue certificada por el fabricante (comunicación del 7 de mayo de 2025) y las cantidades están definidas en la Ficha Técnica; la renovación no es una nueva adquisición. El riesgo de errores de equivalencia o de licencias no habilitadas se controla con la certificación del fabricante del Entregable 1 y la validación del supervisor.

4. Los tiempos de ejecución, los ANS de la Tabla 2 y la disponibilidad son obligaciones exigibles al contratista, respaldadas por las garantías de cumplimiento y calidad del servicio, con independencia de su categoría. El objeto no incluye suministro de equipos, y la renovación conserva la configuración y los componentes ya operativos.

5. Exigir una categoría mínima restringiría la concurrencia de oferentes autorizados por el fabricante sin ser necesaria para garantizar la ejecución, lo que no resulta proporcional al objeto del proceso (artículo 5, numeral 1, de la Ley 1150 de 2007 y artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015), norma que el observante invoca pero que, aplicada a este proceso, no justifica exigir una categoría comercial mínima. Por ello se adopta el ajuste descrito, que permite a la Entidad verificar la categoría y vigencia sin limitar la participación.

En consecuencia, no se incorpora el texto propuesto ni se modifican las Condiciones Técnicas de la Ficha Técnica.

Observación No. 2

Mesa de servicios certificada en Sistema de Gestión de Servicios

Numerales objeto de la observación

Obligación específica No. 7 (estructura de soporte Nivel 1, 2 y 3; Tabla 1 «Niveles de Prioridad» y Tabla 2 «Tiempos de Atención y Solución»); numerales 1.2 (disponibilidad 99,6 %), 1.7 (módulos alineados a ITIL v4), 1.8 y 1.9 (plan de contingencia, BCP y DRP); Entregables No. 6 y No. 8.

Texto que se solicita incorporar

> *El oferente debe contar con una mesa de servicios y/o mesa de ayuda que esté certificada bajo la norma internacional vigente del Sistema de Gestión de Servicios en su versión más reciente, aplicable a los procesos de seguridad y soporte de servicios. Esta certificación asegurará la calidad, gestión y mejora continua de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida directamente al oferente por el ente certificador autorizado.*

Fundamento técnico

1. ***El núcleo del contrato durante 12 meses es un servicio de soporte.*** *Según la obligación No. 7, el Nivel 2 lo presta «la mesa de ayuda de EL CONTRATISTA a través del MSC», que registra los casos, reúne la información, los resuelve o los escala, y es la base para medir los ANS. Es decir, la calidad del servicio que recibirá la SDA depende directamente de cómo opere la mesa de servicios del contratista. La Entidad no puede auditar esos procesos antes de adjudicar; la certificación es la evidencia objetiva de que existen y funcionan.*
2. ***La norma internacional vigente es la ISO/IEC 20000-1:2018.*** *Es el estándar certificable que especifica los requisitos de un Sistema de Gestión de Servicios (SGS), adoptado en Colombia como NTC-ISO/IEC 20000-1. ITIL v4, que la Entidad exige en el numeral 1.7, es un marco de buenas prácticas pero no es certificable para una organización; la ISO/IEC 20000-1 es la vía para que un tercero independiente acredite que esas prácticas se aplican.*
3. ***Correspondencia directa con las obligaciones del pliego.*** *Los procesos que audita la norma coinciden con lo que la SDA le exige al contratista:*

Exigencia del proceso	***Requisito de ISO/IEC 20000-1:2018***
Atención de incidencias y requerimientos por prioridad (Oblig. 7, Tablas 1 y 2)	*8.6.1 Gestión de incidentes; 8.6.2 Gestión de solicitudes de servicio*
Seguimiento de ANS y reporte de solicitudes escaladas (Entregable 6)	*8.3.3 Gestión del nivel de servicio; 9.1 Seguimiento, medición y análisis*

Exigencia del proceso	*Requisito de ISO/IEC 20000-1:2018*
Escalamiento Nivel 3 ante el fabricante (Oblig. 7)	*8.3.4 Gestión de proveedores*
Corrección de errores y fallas del software (2.2)	*8.6.3 Gestión de problemas*
Implementación de actualizaciones y versiones (Oblig. 8)	*8.5.1 Gestión del cambio; 8.5.3 Gestión de la entrega y el despliegue*
Disponibilidad del 99,6 % e informe de downtime (1.2, Entregable 8)	*8.7.1 Gestión de la disponibilidad del servicio*
Plan de contingencia, BCP y DRP (1.8 y 1.9)	*8.7.2 Gestión de la continuidad del servicio*
Seguridad del servicio y de los datos (1.4)	*8.7.3 Gestión de la seguridad de la información*
Optimización de la herramienta durante la garantía	*10 Mejora continua*

4. ***Los ANS exigidos requieren procesos formales.*** *Atender un caso crítico en 30 minutos y resolverlo en 1 hora 30 minutos en esquema 7x24, y garantizar 99,6 % de disponibilidad (un máximo aproximado de 35 horas de indisponibilidad en el año), no se logra con atención ad hoc: requiere turnos de disponibilidad, herramienta de registro con medición de tiempos, matrices de escalamiento y revisión periódica de indicadores. Estos son precisamente los elementos que verifica el ente certificador en las auditorías de la norma.*
5. ***Coherencia con el modelo de servicio de la propia Entidad.*** *La SDA opera su mesa de servicios bajo ITIL v4 sobre la misma herramienta Aranda ASMS. Resulta consistente que el proveedor que soporta esa mesa de servicios opere bajo un sistema de gestión equivalente y certificado, de modo que los indicadores y la terminología de ambas partes sean compatibles.*

Fundamento jurídico

El requisito es proporcional (artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015) porque se refiere exclusivamente a la capacidad de prestar el servicio que constituye el objeto del contrato durante el período de garantía; es objetivo y verificable con la copia del certificado, y no otorga puntaje (artículo 5 de la Ley 1150 de 2007). Por tratarse de un requisito habilitante, es subsanable conforme al parágrafo 1 del artículo 5 de la Ley 1150 de 2007, modificado por el artículo 5 de la Ley 1882 de 2018, siempre que la certificación exista antes del cierre. Su inclusión materializa el deber de planeación y mitiga el riesgo de incumplimiento de los ANS, complementando el amparo de calidad del servicio previsto en el numeral 7 de los Estudios Previos.

Solicitud concreta

Incorporar el texto propuesto en el numeral 5.2.5 de los Estudios Previos y en el pliego de condiciones definitivo, precisando que el certificado debe estar vigente al cierre del proceso, que su alcance debe cubrir la prestación de servicios de mesa de servicios y/o soporte de TI, y que debe ser expedido por un organismo de certificación acreditado (ONAC o miembro del acuerdo de reconocimiento multilateral IAF). Para proponentes plurales, se sugiere que al menos uno de sus integrantes lo acredite.

Respuesta Observación 2:

Revisada la observación, la Entidad no la acoge, por las siguientes razones: La Entidad considera que exigir la certificación ISO/IEC 20000-1 como requisito habilitante no es necesario ni proporcional al objeto del proceso, que consiste en la renovación de la suscripción SaaS de una plataforma existente y la prestación de soporte y mantenimiento sobre ella. Conforme al artículo 5, numeral 1, de la Ley 1150 de 2007 y al artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015, los requisitos habilitantes deben ser adecuados y proporcionales a la naturaleza y al valor del contrato, y el Manual para determinar y verificar los requisitos habilitantes de Colombia Compra Eficiente orienta a no exigir condiciones innecesarias para verificar la aptitud del proponente. Su exigencia limitaría la concurrencia de oferentes autorizados por el fabricante, sin ser indispensable para garantizar la ejecución.

Si bien los procesos que la norma audita guardan relación con las obligaciones del proceso, éstas se exigen y verifican como obligaciones de ejecución, mediante instrumentos que la Entidad ya prevé: niveles de prioridad y tiempos de atención y solución por prioridad (Tablas 1 y 2), escalamiento al fabricante con seguimiento hasta el cierre (Nivel 3), garantía de disponibilidad del 99,6 % con informe de indicadores y tiempos de caída, reporte de solicitudes escaladas, plan de contingencia, soporte certificado por el fabricante, supervisión del contrato y las garantías de cumplimiento y de calidad del servicio. Adicionalmente, aunque la infraestructura SaaS sea administrada por el

fabricante, el contratista responde ante la Entidad por la continuidad, disponibilidad, seguridad y soporte del servicio contratado en su integridad, sin que la ejecución de parte de estas actividades por el fabricante lo exima de dicha responsabilidad, la cual se exige y verifica mediante los instrumentos señalados. Por su parte, el marco ITIL v4 que la Entidad cita en el numeral 1.7 se refiere a los procesos funcionales de la herramienta, no a la organización del contratista.

Observación No. 3

Certificación en seguridad para servicios en la nube

Numerales objeto de la observación

Numerales 1.1 (canal seguro SSL), 1.3 (hosting del fabricante), 1.4 (seguridad del servicio y de los datos), 2.4 (respaldo según ISO/IEC 27001), 2.5 (arquitectura de la solución), 2.7 (propiedad y entrega de la información); Entregable No. 5 (credenciales de base de datos de solo lectura); Condiciones Técnicas (integración con Directorio Activo y APIs); apartado «Normatividad que rige las condiciones técnicas» de la Ficha Técnica.

Texto que se solicita incorporar

> *El oferente deberá garantizar que sus servicios basados en infraestructura en la nube cuenten con procedimientos formalmente establecidos, documentados y operativos para la gestión segura de la información en entornos cloud. Para ello, el oferente deberá contar con certificación vigente en una norma internacional que establezca buenas prácticas de seguridad aplicables a servicios en la nube, incluyendo aspectos como la protección de datos, la responsabilidad compartida entre proveedor y cliente, el control de accesos, la segregación lógica de entornos y el monitoreo de recursos virtualizados.*
>
> *Esta certificación respaldará el cumplimiento de estándares internacionales en la gestión de servicios en la nube, conforme a las políticas de seguridad de la entidad y en armonía con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.*

Fundamento técnico

1. ***Hoy la seguridad en la nube se exige, pero no se verifica.*** *El numeral 1.4 obliga al contratista a garantizar integridad, confidencialidad, cifrado, trazabilidad, protección contra uso fraudulento y una plataforma protegida por firewall, antivirus e IDS. Sin un requisito habilitante asociado, el cumplimiento de estas condiciones queda reducido a la firma de la*

carta de compromiso del numeral 5.2.4, una declaración que no permite a la Entidad comprobar nada antes de adjudicar.

2. ***El oferente forma parte de la cadena de suministro de la nube.*** *Aunque la infraestructura es hospedada por el fabricante (numeral 1.3), el partner administra el entorno: configura y parametriza la solución, ejecuta respaldos (2.4), documenta la arquitectura (2.5), entrega credenciales de acceso a la base de datos (Entregable 5) y gestiona la devolución de la información al terminar el contrato (2.7). Por ello no basta con las certificaciones del hosting; el propio oferente debe demostrar que maneja de forma segura la información en entornos cloud.*
3. ***La integración híbrida amplía la superficie de ataque.*** *La solución se sincroniza con el Directorio Activo de la Entidad, permite a los usuarios restablecer sus contraseñas de red, despliega agentes con capacidad de control remoto en 1.200 equipos y se integra con el chatbot institucional mediante APIs. Un compromiso del entorno SaaS o de las credenciales administrativas del contratista podría servir de punto de entrada a la red interna de la SDA. Esto exige controles específicos de nube sobre accesos privilegiados, segregación de entornos y monitoreo.*
4. ***Información sensible y de valor institucional.*** *El repositorio de más de 200.000 incidentes y requerimientos, la CMDB y el inventario de activos contienen datos personales de servidores y contratistas, configuraciones de la infraestructura y antecedentes de incidentes de seguridad. Su exposición tendría impacto legal y operativo.*
5. ***Referente: ISO/IEC 27017:2015.*** *La norma ISO/IEC 27001, que la Entidad ya cita en el numeral 2.4, no aborda de manera específica las responsabilidades compartidas en la nube. La ISO/IEC 27017 complementa la ISO/IEC 27002 con guías para servicios cloud y añade controles propios que corresponden uno a uno con los aspectos enumerados en el texto propuesto:*

Aspecto del texto propuesto	*Control de ISO/IEC 27017:2015 y relación con el proceso*
Responsabilidad compartida entre proveedor y cliente	*CLD.6.3.1 Roles y responsabilidades compartidas: delimita qué controla el fabricante (hosting), el partner y la SDA.*
Protección de datos	*CLD.8.1.5 Remoción de activos del cliente: soporta la devolución y eliminación segura de la información al terminar el contrato (numeral 2.7).*

Aspecto del texto propuesto	*Control de ISO/IEC 27017:2015 y relación con el proceso*
Segregación lógica de entornos	*CLD.9.5.1 Segregación en entornos de cómputo virtual: aísla el tenant de la SDA de otros clientes del servicio.*
Control de accesos	*CLD.12.1.5 Seguridad operacional del administrador: controla los accesos privilegiados del contratista, la integración con el Directorio Activo y las credenciales del Entregable 5.*
Monitoreo de recursos virtualizados	*CLD.12.4.5 Monitoreo de servicios en la nube: soporta la verificación de disponibilidad (1.2), las pruebas de desempeño (1.1) y el informe de downtime (Entregable 8).*
Seguridad de la red y endurecimiento	*CLD.9.5.2 Endurecimiento de máquinas virtuales y CLD.13.1.4 Alineación de la seguridad de redes físicas y virtuales: respaldan la exigencia de firewall, antivirus e IDS (1.4).*

Fundamento normativo y jurídico

El requisito es coherente con el marco normativo que la misma Entidad incorporó en la Ficha Técnica: el Modelo de Seguridad y Privacidad de la Información (MSPI) adoptado por la Resolución 500 de 2021 y la Resolución 746 de 2022 de MinTIC, que según la propia Ficha exige la gestión de riesgos de seguridad digital en la cadena de suministro; el Decreto 338 de 2022 y la Directiva Presidencial 07 de 2022 sobre gobernanza de la seguridad digital; y la Ley 1581 de 2012, según la cual el responsable del tratamiento debe exigir al encargado condiciones de seguridad que impidan la pérdida, consulta, uso o acceso no autorizado de los datos personales. La certificación solicitada es la forma objetiva de verificar esas condiciones en el proveedor.

Igual que en las observaciones anteriores, se trata de un requisito habilitante, proporcional al objeto (artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015), verificable con la copia del certificado, que no otorga puntaje (artículo 5 de la Ley 1150 de 2007) y que es subsanable en los términos del parágrafo 1 del mismo artículo.

Solicitud concreta

Incorporar el texto propuesto en el numeral 5.2.5 de los Estudios Previos, en el pliego de condiciones definitivo y en el numeral 1.4 de la Ficha Técnica, indicando como referente la norma ISO/IEC 27017

en su versión vigente, con certificado vigente al cierre y expedido por organismo acreditado. Para proponentes plurales, se sugiere que al menos uno de sus integrantes lo acredite.

Respuesta Observación 3:

Revisada la observación, la Entidad no la acoge, por las razones que se precisan a continuación:

1. La seguridad del servicio y de los datos sí se exige y se verifica durante la ejecución: integridad, confidencialidad, cifrado, trazabilidad y disponibilidad de los datos, y protección con firewall, antivirus y detección de intrusos (numeral 1.4); respaldos conforme a ISO/IEC 27001, el Decreto 1080 de 2015 y la Ley 1581 de 2012 (numeral 2.4); propiedad de la información de la Entidad y acceso a ella al terminar el contrato (numeral 2.7); y la suscripción de acuerdos de confidencialidad y formatos de seguridad de la información (obligación 11). La alineación con el Modelo de Seguridad y Privacidad de la Información se materializa mediante estas obligaciones contractuales, supervisadas por la Entidad, y no mediante un requisito habilitante adicional.

2. La infraestructura está alojada en el hosting del fabricante (numeral 1.3), por lo que los controles de nube sobre segregación de entornos, monitoreo de recursos virtualizados y seguridad de red corresponden al fabricante. Para ellos se aceptarán las políticas, certificaciones e informes oficiales vigentes del fabricante, junto con la delimitación de responsabilidades entre fabricante, contratista y Entidad.

3. La conexión de la plataforma con el Directorio Activo se limita a la comunicación con éste (autenticación de usuarios y agentes, sincronización de usuarios y autogestión de contraseñas), sin otros servicios, integraciones ni autenticaciones alternas, y la integración con el chatbot institucional se limita a asesoría sobre el uso de APIs, de modo que la superficie descrita no se amplía por el alcance contractual.

4. El texto propuesto exige una "norma internacional que establezca buenas prácticas de seguridad aplicables a servicios en la nube" sin identificar una certificación concreta; ISO/IEC 27017 es una guía de controles y no una norma certificable por sí misma. Un requisito habilitante debe ser claro y verificable de forma objetiva, y exigirlo en estos términos restringiría la concurrencia sin ser necesario para garantizar la ejecución (artículo 5, numeral 1, de la Ley 1150 de 2007 y artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015).

OBSERVANTE 4 : HEIMCORE S.A.S.

Observación No. 1

Unificación del emisor de la certificación requerida para el pago. se solicita unificar en todos los documentos quién expide la certificación de activación, su contenido mínimo y si requiere informe del contratista.

Observación 1 — Unificación del emisor de la certificación requerida para el pago

Referencias:

- Ficha Técnica Aranda, página 19, apartado "Forma de pago".
- Estudio Previo Aranda, página 20, apartado de forma de pago.
- Proyecto de Pliego de Condiciones, página 56, numeral 10.6.
- Clausulado del Contrato, página 4, cláusula sexta.

La ficha técnica establece que la certificación de activación de la suscripción y disponibilidad de los servicios será expedida por el contratista y validada por el supervisor. Por su parte, el estudio previo, el proyecto de pliego y el clausulado contractual señalan que dicha certificación será expedida por el fabricante.

Solicitamos unificar esta condición en todos los documentos del proceso e indicar expresamente quién debe expedir la certificación, cuál es su contenido mínimo y si se requiere una certificación del fabricante acompañada de un informe del contratista.

Lo anterior permitirá identificar de manera inequívoca los documentos exigibles para **acreditar el cumplimiento y tramitar el pago.**

Respuesta Observación 1:

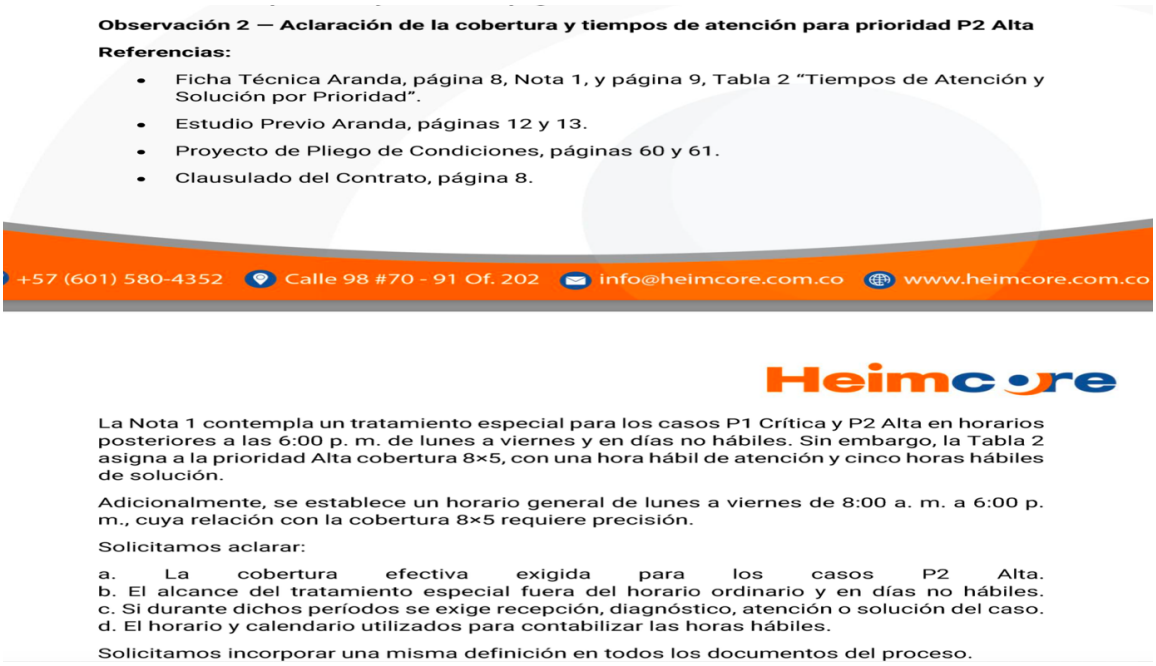
Revisada la observación, la misma es aceptada. La Entidad identifica una diferencia de redacción en la Ficha Técnica, apartado "Forma de pago", donde se indica que la certificación de activación de la suscripción y de disponibilidad de los servicios sería expedida por el contratista. Se aclara que el emisor es el fabricante Aranda Software, tal como lo establecen el Estudio Previo (numeral 3.3), el Proyecto de Pliego de Condiciones (numeral 10.6), el Clausulado del Contrato (cláusula sexta) y el Entregable 1 de la propia Ficha Técnica.

En cuanto al contenido mínimo, la certificación será expedida por el fabricante y validada por el supervisor del contrato, y acreditará únicamente aquello que el fabricante puede certificar: (i) que la Entidad cuenta con acceso a la plataforma SaaS y (ii) que las licencias objeto de renovación se encuentran habilitadas por el período de doce (12) meses. Dado que el soporte técnico, los niveles de servicio y la disponibilidad son obligaciones del contratista y no del fabricante, el compromiso de soporte técnico durante la garantía se acreditará con el documento firmado por el contratista (Entregable 8), validado por el supervisor del contrato. No se requiere un informe adicional del contratista como condición de pago; la validación del supervisor del contrato es el mecanismo de verificación previsto.

En consecuencia, se ajustan la Forma de pago de la Ficha Técnica y el numeral 3.3 del Estudio Previo, y la misma redacción se incorporará en el Proyecto de Pliego de Condiciones (numeral 10.6) y en el Clausulado del Contrato (cláusula sexta).

Observación No. 2

Se solicita aclarar la cobertura efectiva de P2 Alta, el alcance del tratamiento especial fuera del horario y en días no hábiles, y el calendario de las horas hábiles



Observación 2 — Aclaración de la cobertura y tiempos de atención para prioridad P2 Alta

Referencias:

- Ficha Técnica Aranda, página 8, Nota 1, y página 9, Tabla 2 "Tiempos de Atención y Solución por Prioridad".
- Estudio Previo Aranda, páginas 12 y 13.
- Proyecto de Pliego de Condiciones, páginas 60 y 61.
- Clausulado del Contrato, página 8.

+57 (601) 580-4352 Calle 98 #70 - 91 Of. 202 info@heimcore.com.co www.heimcore.com.co

Heimcore

La Nota 1 contempla un tratamiento especial para los casos P1 Crítica y P2 Alta en horarios posteriores a las 6:00 p. m. de lunes a viernes y en días no hábiles. Sin embargo, la Tabla 2 asigna a la prioridad Alta cobertura 8×5, con una hora hábil de atención y cinco horas hábiles de solución.

Adicionalmente, se establece un horario general de lunes a viernes de 8:00 a. m. a 6:00 p. m., cuya relación con la cobertura 8×5 requiere precisión.

Solicitamos aclarar:

a. La cobertura efectiva exigida para los casos P2 Alta.
b. El alcance del tratamiento especial fuera del horario ordinario y en días no hábiles.
c. Si durante dichos períodos se exige recepción, diagnóstico, atención o solución del caso.
d. El horario y calendario utilizados para contabilizar las horas hábiles.

Solicitamos incorporar una misma definición en todos los documentos del proceso.

Respuesta Observación 2:

Una vez revisada la observación es aceptada parcialmente, en ese sentido se precisa el alcance de la Nota 1 sin modificar los tiempos de la Tabla 2.

a) La cobertura de los casos P2 Alta es 8x5: los tiempos de atención (1 hora hábil) y solución (5 horas hábiles) se contabilizan dentro del horario de soporte de lunes a viernes, de 8:00 a.m. a 6:00 p.m.

b) y c) Fuera de ese horario y en días no hábiles, el tratamiento especial de la Nota 1 para los casos P1 y P2 consiste en garantizar la recepción del caso y la atención inicial (primer contacto y diagnóstico preliminar). Para los casos P2 Alta no se exige la solución definitiva fuera del

horario ordinario, la cual se gestiona dentro de la cobertura 8x5; para los casos P1 Crítica se mantiene la cobertura 7x24 de la Tabla 2, tanto para la atención como para la solución.

d) Las horas hábiles se contabilizan de lunes a viernes dentro del horario de soporte (8:00 a.m. a 6:00 p.m.), descontando el intervalo de 12:00 m. a 2:00 p.m., para un total de ocho (8) horas hábiles diarias, que corresponde a la cobertura 8x5. Se excluyen sábados, domingos y festivos del calendario colombiano.

Esta precisión se incorporará de manera concordante en los documentos precontractuales.

Observación No. 3

Delimitación de las actividades de configuración, parametrización e integración - Se solicita confirmar que las obligaciones se limitan a conservar y validar la configuración existente y los ajustes derivados de actualizaciones, o identificar las nuevas actividades.

Observación 3 — Delimitación de las actividades de configuración parametrización e integración

Referencias:

- Ficha Técnica Aranda, página 7, obligación específica 5, y páginas 11 y 12, numeral 1.7.
- Estudio Previo Aranda, página 11, numeral 2.6, obligación 5, y páginas 15 y 16, numeral 1.7.
- Proyecto de Pliego de Condiciones, página 59, numeral 10.8.2, obligación 5, y páginas 62 y 63, numeral 1.7.
- Clausulado del Contrato, página 7, cláusula octava, obligación 5, y página 10, numeral 1.7.

Los documentos identifican la contratación como renovación, actualización y soporte de una plataforma existente. No obstante, se exige ejecutar actividades de configuración, parametrización, integración y puesta en funcionamiento, y que los módulos queden completamente configurados, parametrizados y operativos.

Solicitamos confirmar si estas obligaciones se limitan a conservar y validar la configuración existente y a realizar los ajustes necesarios derivados de las actualizaciones del fabricante.

En caso de requerirse nuevas configuraciones, integraciones, despliegues o modificaciones funcionales, solicitamos identificar los módulos involucrados, las actividades, cantidades, interfaces, entregables y criterios de aceptación.

Esta precisión permitirá dimensionar las actividades incluidas y valorar sus costos bajo condiciones comparables para los oferentes.

Respuesta Observación 3:

Una vez revisada la observación, la Entidad confirma lo solicitado y aclara que la obligación específica 5 y el numeral 1.7 se limitan a conservar y validar la configuración actualmente operativa de los módulos, y a realizar los ajustes, pruebas y estabilización que se deriven de las actualizaciones (versiones estables y mejoras) liberadas por el fabricante durante la garantía, conforme a la obligación específica 4 (“si ello fuera necesario por actualizaciones”). La expresión “completamente configurados, parametrizados y operativos” del numeral 1.7 describe el estado en que deben permanecer los módulos ya adquiridos por la Entidad, no una nueva implementación.

La Entidad no exige nuevos despliegues, módulos ni desarrollos funcionales. Las únicas actividades adicionales a la conservación de la configuración son las expresamente enumeradas en la Ficha

Técnica: (i) la elaboración de seis (6) reportes en el módulo AQM (numeral 1.11); (ii) la asesoría de integración para la interoperabilidad del chatbot institucional mediante APIs; (iii) la asesoría en elaboración de reportes; y (iv) la transferencia de conocimiento (numeral 1.5). La sincronización con el Directorio Activo no es una actividad adicional: hace parte de la configuración existente que se conserva. Con ello, los oferentes cuentan con la información necesaria para valorar sus costos en condiciones comparables.

Observación No. 4

Se solicita confirmar si el acceso está disponible en la suscripción SaaS, precisar bases, vistas y mecanismo, y aceptar alternativas (API, vistas, exportaciones).

Observación 4 — Viabilidad y alcance del acceso de solo lectura a la base de datos

Referencias:

- Ficha Técnica Aranda, página 14, entregable 5.
- Estudio Previo Aranda, página 19, numeral 2.11, informe 5.
- Proyecto de Pliego de Condiciones, página 65, entregable 5.
- Clausulado del Contrato, página 12, entregable 5.

Se exige suministrar credenciales de acceso a la base de datos con perfil de solo lectura, habilitado para consultas y extracción de información.

Considerando que la solución opera bajo modalidad SaaS sobre infraestructura del fabricante, solicitamos confirmar que dicho acceso está permitido y disponible dentro de la suscripción objeto de renovación.

Asimismo, solicitamos precisar las bases de datos o vistas a las que se requiere acceso, el mecanismo de conexión, los perfiles y las restricciones de seguridad aplicables.

Si el fabricante no permite acceso directo a la base de datos, solicitamos confirmar si la obligación podrá cumplirse mediante mecanismos autorizados de consulta y extracción, como API, vistas o exportaciones, e indicar las condiciones mínimas de aceptación.

Respuesta Observación 4:

Revisada la observación, la Entidad la acoge parcialmente y aclara que el requerimiento de fondo es contar con un mecanismo autorizado y permanente para consultar y extraer la información de la plataforma, que es de propiedad de la Entidad (numeral 2.7 de la Ficha Técnica).

Si el fabricante habilita acceso directo de solo lectura a la base de datos en el servicio SaaS, el contratista deberá entregar las credenciales con perfil Read-Only. Si el modelo SaaS no lo permite, la obligación se tendrá por cumplida mediante mecanismos autorizados de consulta y extracción: API de la plataforma, vistas de datos, el módulo de reportes AQM o exportaciones, en concordancia con la “Asesoría en integración” y la “Asesoría en elaboración de reportes” de las Condiciones Técnicas, que ya contemplan el uso de APIs y la extracción de datos desde el almacenamiento de la plataforma.

Condiciones mínimas de aceptación: (i) acceso de solo lectura, sin capacidad de modificar datos; (ii) cobertura de la información de los módulos contratados (casos, activos y CI, usuarios y catálogo de servicios, entre otros); (iii) mecanismo disponible durante toda la garantía, sin costo adicional; (iv) documentación de uso (endpoints, vistas o procedimiento, perfiles y restricciones de seguridad); y (v) validación del supervisor. Las bases de datos o vistas específicas y el mecanismo de conexión se

definirán con el supervisor durante la ejecución, según lo que el fabricante disponga para el servicio SaaS.

Observación No. 5

Alcance de los entregables de arquitectura y documentación: Se solicita aceptar documentos oficiales del fabricante, precisar el nivel de detalle, las condiciones de actualización y desde cuándo corren los veinte días



Observación 5 — Alcance de los entregables de arquitectura y documentación

Referencias:

- Ficha Técnica Aranda, páginas 13 y 14, numerales 2.5 y 2.6, y página 14, entregables 2 y 3.
- Estudio Previo Aranda, página 17, numerales 2.5 y 2.6, y página 19, numeral 2.11, informes 2 y 3.
- Proyecto de Pliego de Condiciones, páginas 64 y 65.
- Clausulado del Contrato, página 11, numerales 2.5 y 2.6, y página 12, entregables 2 y 3.

Se exige entregar documentación de arquitectura que incluya procesamiento, almacenamiento, velocidad de red, sistemas operativos, motor de base de datos y servidor de aplicaciones, así como diagramas y manuales de la herramienta.

Solicitamos confirmar que podrán presentarse documentos oficiales vigentes del fabricante, correspondientes al servicio SaaS contratado, y precisar el nivel de detalle exigido respecto de infraestructura administrada por aquel.

Heimcore

Igualmente, solicitamos aclarar si las actualizaciones documentales se exigirán únicamente cuando existan cambios que afecten el servicio contratado y desde qué fecha se contabilizan los primeros veinte días señalados en los numerales 2.5 y 2.6.

Si existe información de infraestructura que el fabricante no suministra a sus canales o clientes, solicitamos indicar qué soporte equivalente será aceptado.

Respuesta Observación 5:

Revisada la observación, la Entidad aclara lo siguiente: Para la infraestructura de hosting administrada por el fabricante (procesamiento, almacenamiento, red, sistemas operativos, motor de base de datos y servidor de aplicaciones), se aceptarán documentos oficiales vigentes del fabricante correspondientes al servicio SaaS contratado. El contratista deberá complementarlos con la información propia de la implementación de la Entidad: módulos habilitados, integración con el Directorio Activo, certificado SSL de conexión y diagrama de la herramienta desplegada.

Respecto de los documentos que no hayan cambiado frente a la arquitectura desplegada, se acepta la presentación de la versión vigente sin reelaboración, indicando expresamente que no han tenido modificaciones. La actualización documental se exigirá únicamente cuando se presenten cambios que afecten el servicio contratado.

En cuanto al plazo, la documentación debe entregarse dentro del plazo de ejecución del contrato (un (1) mes). Los primeros veinte (20) días calendario de los numerales 2.5 y 2.6 se cuentan desde la suscripción del acta de inicio y, por tanto, se cumplen dentro de dicho plazo. Si existe información

de infraestructura que el fabricante no suministra a sus canales o clientes, se aceptará la comunicación oficial del fabricante que así lo indique, junto con la información equivalente disponible.

Observación No. 6

Confirmación de la cobertura de Aranda Local Connector Service

Síntesis de la observación: Se solicita confirmar si la arquitectura requiere el componente y, de ser así, si está incluido en la suscripción o debe ofertarse.

Observación 6 — Confirmación de la cobertura de Aranda Local Connector Service

Referencias:

- Ficha Técnica Aranda, página 2, relación de licencias, y páginas 16 y 17, condiciones técnicas e ítem 1.1.
- Clausulado del Contrato, página 3, relación de ítems.
- Observación 2 presentada anteriormente al evento EC-0532026.

En las relaciones de productos y cantidades se identifican las licencias ASMS Usuario Concurrente, ASMS Usuario Nombrado y Aranda Device Management, sin una identificación expresa del componente Aranda Local Connector Service.

Solicitamos confirmar si la arquitectura y las integraciones actualmente utilizadas por la entidad requieren dicho componente.

En caso afirmativo, solicitamos indicar si se encuentra incluido en la suscripción objeto de renovación, cubierto mediante otro servicio vigente o si debe ser suministrado o renovado dentro de esta contratación. En este último supuesto, solicitamos precisar cantidad, modalidad, vigencia y ubicación del costo en la oferta económica.

En caso de no requerirse, solicitamos confirmar expresamente esta condición.

Respuesta de la Entidad:

Revisada la observación, la Entidad aclara lo siguiente: La Entidad confirma que su arquitectura actual utiliza un servicio de conexión entre la plataforma en la nube y su Directorio Activo: en la parametrización base del servicio vigente, la autenticación de Aranda con el Directorio Activo se realiza mediante una conexión VPN. Esta conexión hace parte de la configuración operativa de la plataforma desde su migración a SaaS y es indispensable para la autenticación de los usuarios y la sincronización con el Directorio Activo (Condiciones Técnicas: “Sincronización de la herramienta provista con el Directorio Activo (Ldap) de la Entidad”, y módulo de Autogestión de Contraseñas).

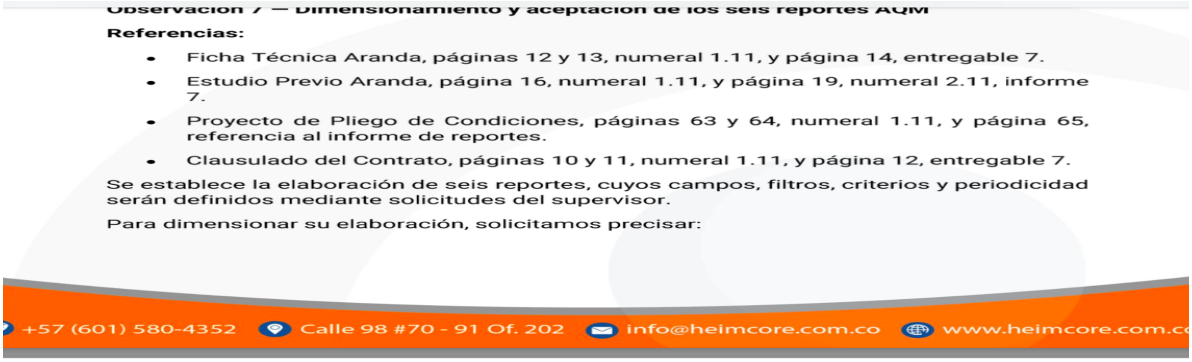
Dado que la renovación tiene por propósito conservar la configuración actualmente operativa (obligaciones específicas 4 y 5 y numeral 1.7), dicho servicio de conexión se considera incluido dentro de la parametrización propia de la renovación y de la garantía de continuidad y disponibilidad de la plataforma (numerales 1.2 y 1.3). En consecuencia, no constituye un ítem adicional, no requiere cantidad, modalidad ni vigencia propias, y no tiene un valor separado en la oferta

económica: su costo se entiende incorporado en el valor de los ítems de renovación ofertados. Para mayor claridad, esta precisión se incorpora en las Condiciones Técnicas de la Ficha Técnica, que hace parte integral del Estudio Previo (numeral 2.2).

La red y el Directorio Activo de la Entidad permanecen bajo su administración. Al contratista, directamente o a través del fabricante, le corresponde mantener, validar y, de ser necesario, reconfigurar la conexión del lado de la plataforma en la nube, de modo que la autenticación y la sincronización se conserven tal como operan actualmente.

Observación No. 7

Dimensionamiento y aceptación de los seis reportes AQ: Se solicita precisar módulo, fuentes de información, complejidad, ajustes, plazos, criterios de aceptación y tratamiento de solicitudes incompletas o cambios de alcance.


Observación 7 — Dimensionamiento y aceptación de los seis reportes AQM

Referencias:

- Ficha Técnica Aranda, páginas 12 y 13, numeral 1.11, y página 14, entregable 7.
- Estudio Previo Aranda, página 16, numeral 1.11, y página 19, numeral 2.11, informe 7.
- Proyecto de Pliego de Condiciones, páginas 63 y 64, numeral 1.11, y página 65, referencia al informe de reportes.
- Clausulado del Contrato, páginas 10 y 11, numeral 1.11, y página 12, entregable 7.

Se establece la elaboración de seis reportes, cuyos campos, filtros, criterios y periodicidad serán definidos mediante solicitudes del supervisor.

Para dimensionar su elaboración, solicitamos precisar:

+57 (601) 580-4352 Calle 98 #70 - 91 Of. 202 info@heimcore.com.co www.heimcore.com.c

Heimcore

a. El módulo y versión de reportería disponibles y su cobertura dentro del licenciamiento renovado.
b. Las fuentes de información y si se requieren integraciones con sistemas externos.
c. Los límites de complejidad y las funcionalidades esperadas.
d. El número de revisiones o ajustes incluidos por reporte.
e. El plazo de entrega contado desde la recepción de cada solicitud completa.
f. Los criterios de aceptación y el procedimiento de aprobación.

Asimismo, solicitamos definir el tratamiento de solicitudes incompletas o de cambios de alcance posteriores a su aprobación, y la fecha máxima para recibir solicitudes que permitan entregar los reportes dentro de la cobertura prevista.

Respuesta de la Entidad:

Revisada la observación, la Entidad la acoge parcialmente y precisa lo siguiente:

a) y b) Los reportes se elaboran en el módulo de reportes AQM de la herramienta Aranda, disponible en el licenciamiento ASMS renovado. Se construirán únicamente con datos propios de Aranda (casos, CMDB y activos, entre otros) y su visualización; no requieren integración con sistemas externos.

c) Los límites de complejidad corresponden a la gestión y visualización de datos propios de la herramienta, conforme a los campos, filtros, criterios y periodicidad que la Entidad indique en la solicitud escrita.

d) a f) Los reportes serán solicitados por la Entidad, a través del supervisor, cuando los requiera y dentro del plazo de ejecución, mediante comunicación escrita (numeral 1.11); esa es la fecha máxima para recibir solicitudes. Durante el primer mes (plazo de ejecución) el contratista deberá entregar el avance que se tenga de los reportes solicitados, conforme al Entregable 7 (estado de avance y fecha comprometida de entrega).

El plazo de entrega de cada reporte será de máximo un (1) mes, contado desde la recepción de la solicitud completa, sin perjuicio de que se convenga por escrito con el supervisor un plazo menor según su complejidad y, en todo caso, dentro del período de garantía. Las solicitudes incompletas se devolverán al solicitante, y el plazo solo se contará desde que se complete la información requerida.

Revisiones o ajustes: cada reporte incluye hasta dos (2) rondas de ajuste, sin costo adicional, sobre lo originalmente solicitado, cada una atendida en el plazo que se convenga con el supervisor. Los cambios de alcance posteriores a la aprobación de la solicitud (nuevos campos, filtros, fuentes o criterios distintos de los solicitados) se tratarán como una solicitud nueva y tendrán su propio plazo.

La aceptación se formaliza con el acta de recibo a satisfacción suscrita por el supervisor, previa verificación de que el reporte está publicado y funcionando en el ambiente productivo conforme a lo solicitado.

Observación No. 8

Distribución de responsabilidades sobre seguridad, respaldos y continuidad del servicio SaaS

Síntesis de la observación: Se solicita definir qué ejecuta el fabricante, el contratista y la Entidad, y precisar respaldos, recuperación, planes de continuidad, medición de la disponibilidad del 99,6 % y mantenimientos.

Observación 8 — Distribución de responsabilidades sobre seguridad respaldos y continuidad del servicio SaaS

Referencias:

- Ficha Técnica Aranda, página 10, numerales 1.2, 1.3 y 1.4; página 12, numerales 1.8 y 1.9; página 13, numerales 2.1 y 2.4.
- Estudio Previo Aranda, páginas 14, 16 y 17.
- Proyecto de Pliego de Condiciones, páginas 62, 63 y 64.
- Clausulado del Contrato, páginas 10 y 11.

Los documentos señalan que la plataforma se encuentra alojada en infraestructura del fabricante y, simultáneamente, asignan al contratista obligaciones de disponibilidad, seguridad, actualización, respaldo y recuperación.

Solicitamos definir las actividades que ejecutará el fabricante, las que deberá realizar o gestionar el contratista y aquellas que corresponden a la entidad, así como los soportes aceptados para acreditar su cumplimiento.

En particular, solicitamos precisar:

a. Frecuencia, retención y alcance de los respaldos.
b. Procedimiento de restauración y tiempos objetivos de recuperación.
c. Alcance de los planes de contingencia, continuidad y recuperación ante desastres, y si se aceptarán los documentos y evidencias del fabricante aplicables al servicio.
d. Período, fórmula y fuente de medición de la disponibilidad del 99,6 %.
e. Tratamiento de mantenimientos programados y eventos externos a la plataforma.

Estas precisiones permitirán establecer obligaciones verificables y coherentes con la operación del servicio SaaS.

+57 (601) 580-4352 Calle 98 #70 - 91 Of. 202 info@heimcore.com.co www.heimcore.com.co

Heimcore

Agradecemos que las aclaraciones y ajustes que se adopten se incorporen de manera concordante en la ficha técnica, el estudio previo, el pliego de condiciones y el clausulado contractual.

Respuesta de la Entidad:

Revisada la observación, la Entidad la acoge parcialmente mediante las siguientes precisiones:

Distribución de responsabilidades. El fabricante Aranda Software aloja y opera la infraestructura del servicio SaaS (hosting, respaldos de plataforma, parches de infraestructura y seguridad perimetral). El contratista responde ante la Entidad por la continuidad, disponibilidad, seguridad y soporte del servicio contratado en su integridad (numerales 1.2, 1.3, 1.4, 2.1 y 2.4), sin que la ejecución de parte de estas actividades por el fabricante lo exima de dicha responsabilidad; le corresponde gestionar ante el fabricante lo que sea necesario y acreditarlo. La Entidad es responsable de su propia red, su Directorio Activo, su conectividad y de la gestión de los usuarios y datos que registra. Para acreditar el cumplimiento se aceptarán certificaciones, políticas e informes oficiales vigentes del fabricante aplicables al servicio SaaS, acompañados del informe del contratista.

a) y b) Respaldos y restauración: Los respaldos de la plataforma son ejecutados por el fabricante sobre la infraestructura del servicio SaaS, y el contratista garantizará ante la Entidad que se realicen, conforme al numeral 2.4. Se aceptan la frecuencia, retención y alcance de la política vigente del fabricante para el servicio SaaS, que el contratista deberá certificar y presentar al supervisor dentro del plazo de ejecución del contrato; esta precisión se incorporará en el numeral 2.4 de la Ficha Técnica y del Estudio Previo. Cuando la Entidad requiera una restauración, el contratista la gestionará conforme a los tiempos de la Tabla 2 según la prioridad del caso; en caso de que este

trámite dependa directamente de los tiempos de respuesta del fabricante, se tramitará conforme a lo estipulado en la Nota 2.

c) Los planes de contingencia, continuidad (BCP) y recuperación ante desastres (DRP) se limitan al servicio de la Mesa de Servicio contratado. Se aceptarán los documentos y evidencias del fabricante aplicables al servicio, que el contratista entregará dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio (numeral 1.8) y socializará con la Entidad.

d) La disponibilidad del 99,6 % se mide sobre todo el período de garantía (doce meses contados desde la activación de la suscripción), con base en el reporte de disponibilidad del fabricante para el servicio contratado, y se consolida en el informe final de indicadores y tiempos de caída (Entregable 9). Se calcula como el tiempo total del período menos el tiempo de indisponibilidad, dividido entre el tiempo total.

e) No se computan como indisponibilidad los mantenimientos programados notificados con anticipación y acordados con el supervisor, ni los eventos ajenos a la plataforma (red o conectividad de la Entidad, internet, Directorio Activo de la Entidad) ni los de fuerza mayor o caso fortuito, en concordancia con la Tabla 1, que limita las prioridades P1 y P2 a fallas atribuibles exclusivamente al software provisto por el contratista

Lo anterior se verá reflejado en los documentos precontractuales.

JOHN JAIRO ARDILA ROMERO

GERENTE DE PROYECTO

Proyectó: Carlos Andres Perdomo -Contratista OTIC

Proyectó: Juan Carlos Rueda -Contratista OTIC

Proyectó: Leonardo Cárdenas-Contratista OTIC

Proyectó: Andrés Mauricio Villegas Navarro– Contratista OTIC