ESTUDIO PREVIO

Generalidades del Proceso de Contratación	
Dependencia	Área de sistemas
Objeto	Prestación de servicios para la provisión, administración y soporte integral de la infraestructura tecnológica institucional, incluyendo servicios en la nube, mecanismos de continuidad del negocio, licenciamiento y suministro de componentes tecnológicos, así como soporte especializado.
Presupuesto Oficial	OCHOCIENTOS SESENTA Y SIETE MILLONES SETECIENTOS NOVENTA Y CUATRO MIL CUATROCIENTOS TREINTA Y SIETE PESOS M/CTE (867.794.437) INCLUIDOS TODOS LOS IMPUESTOS A QUE HUBIERE LUGAR.
Modalidad de Selección	Licitación publica
Clase de Contrato	Prestación de servicios
Fecha de Elaboración	Diciembre de 2025

Conforme lo establecido en los numerales 7 y 12 del artículo 25 de la Ley 80 de 1993, en armonía con los apartados pertinentes de la Ley 1150 de 2007, y en aplicación del artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, se procede a suscribir el estudio previo necesario para el impuso de un proceso de selección.

Numeral 1 del Artículo 2.2.1.1.2.1.1: *"Descripción de la necesidad que la Entidad pretende satisfacer con el Proceso".*

INFICALDAS es una entidad descentralizada del orden departamental que, mediante la administración de sus inversiones y la prestación de servicios financieros a los entes territoriales y a las personas jurídicas de derecho público y privado, que estén destinadas a la prestación de un servicio público, o tiendan a satisfacer una necesidad básica de la comunidad, contribuye al financiamiento, promoción y desarrollo del Departamento de Caldas.

Para el cumplimiento de su objetivo misional INFICALDAS ofrece un portafolio de servicios compuesto por:

1. Servicios financieros: A través de estos servicios se ofrecen soluciones de crédito a Municipios y entidades para el desarrollo de proyectos estratégicos, en beneficio de la comunidad, así como en la administración eficiente de excedentes de liquidez, garantizando seguridad, rentabilidad y respaldo a las finanzas territoriales
2. Banca de Desarrollo: A través de la banca de desarrollo, INFICALDAS colabora en proyectos de alto impacto que fomentan el crecimiento, la infraestructura, el turismo, la sostenibilidad y el crecimiento económico del territorio.
3. Inversiones patrimoniales: Inficaldas cuenta con una participación en entidades estratégicas que le aportan valor a la región, en la que adelantan acciones orientadas a generar rentabilidad inmediata, preservación de capital y sostenibilidad en tiempo.

INFICALDAS dentro de su Plan estratégico y buscando el fortalecimiento institucional tiene como uno de sus objetivos *"consolidar una gestión organizacional enmarcada en el Modelo Integrado de Planeación y Gestión y el Gobierno Corporativo"* esto con el propósito de continuidad con los requerimientos para la vigilancia especial planteada por la Superfinanciera y de esta forma poder fortalecer sus servicios ampliando su portafolio con nuevos productos y mejorando los actuales para satisfacer las necesidades de sus clientes.

En desarrollo de estas funciones misionales y del propósito institucional de fortalecer la gestión organizacional bajo los lineamientos del Modelo Integrado de Planeación y Gestión, el Gobierno Corporativo y las exigencias de la Superintendencia Financiera, INFICALDAS requiere contar con una infraestructura tecnológica que soporte de manera segura, estable y eficiente sus procesos estratégicos, misionales y de apoyo. La actividad financiera y de desarrollo que adelanta el Instituto depende cada vez más de plataformas digitales, servicios en la nube, sistemas de información y esquemas de seguridad que garanticen la disponibilidad, integridad y confiabilidad de la información. Por esta razón, se hace necesario estructurar un conjunto de componentes tecnológicos que permitan asegurar la operación institucional, atender el crecimiento técnico y reforzar los mecanismos de continuidad del negocio.

A continuación, se describen los elementos que conforman esta necesidad tecnológica:

1. INFRAESTRUCTURA COMO SERVICIO (IAAS)

El instituto no cuenta con una infraestructura tecnológica propia, sin embargo, mediante la figura de renta ha logrado mantener la operación y proyectar acompañamiento, crecimiento y ejecución frente al desarrollo de los proyectos estratégicos del Departamento de Caldas.

En Colombia se reconoce el arrendamiento de tecnología y sus beneficios; no obstante, aún existe poco conocimiento sobre las razones específicas que justifican su adopción. A continuación, se presentan las principales consideraciones para su implementación:

ESTUDIO PREVIO

Obsolescencia Tecnológica (CTP: Costo total de la propiedad): Al no ser un equipo propio la obsolescencia tecnológica y el soporte técnico es responsabilidad del proveedor por ser el propietario de los equipos en su condición de ARRENDADOR, de esta manera la empresa arrendadora, se encarga de que sus equipos estén actualizados y a punto, para soportar el trabajo diario que requiere la entidad en calidad de beneficiario de la renta.

Garantía: Los equipos contaran con tiempos de garantías vigentes, con el fin de asegurar su correcto funcionamiento.

Características Técnicas: Los avances tecnológicos se están renovando constantemente, es por ello por lo que es importante renovar constantemente los equipos de cómputo y hardware requerido en la operación a últimas versiones, con el fin de mejorar las cualidades técnicas de los mismos y mantener la vanguardia de los cambios tecnológicos frecuentes que oferta el mercado.

Adicionalmente, dentro de los beneficios del alquiler de bienes y servicios, encontramos los siguientes:

1. Las empresas que prestan el servicio incluyen los costos de personal especializado.
2. Se cuenta con repuestos e insumos disponibles de forma inmediata en la Entidad, garantizando de esta forma la prestación ininterrumpida del servicio.
3. Se cuenta con un stock de equipos de respaldo, para reemplazar en forma inmediata los equipos que presenten fallas técnicas.
4. Al tratarse de la contratación de un servicio de alquiler de equipos de escritorios, portátiles y servidores, firewall y demás unidades de hardware, se garantiza la correcta operación de todos los equipos suministrados a través de los mantenimientos preventivos. correctivos, y la instalación de nuevos equipos conforme la Entidad lo requiera.
5. El proveedor garantiza el desplazamiento del personal técnico y los traslados de los dispositivos que se requieran para atender a las necesidades en las sedes de la Entidad y mantiene backup de los mismos en caso de incidentes asociados a su operación sin afectar la entidad.

En la Entidad se presentan necesidades en infraestructura tecnológica que se deben satisfacer proporcionando los elementos que permitan llevar a cabo el desarrollo de las actividades de los funcionarios, así como el fortalecimiento e implementación de la infraestructura. Por lo anterior, se requiere contratar el servicio de alquiler de los elementos que se detallan a continuación, con el fin de asegurar la prestación de los servicios basados en tecnología, de punta, que estén siempre disponibles para atender las necesidades tecnológicas de las diferentes dependencias.

Resulta importante resaltar el principio de economía en la actividad contractual, el cual señala, entre otras tantas condiciones, que el objetivo de la Administración Pública en los procesos de contratación es lograr la austeridad en el gasto, la selección objetiva del contratista. y evitar el desgaste procesal en la elaboración de diferentes procesos contractuales.

Este principio está consagrado en el artículo 209 de la Constitución Política en concordancia con el artículo 25, numerales 7 y 12 de la Ley 80 de 1993, y garantiza que, en la actuación contractual se observen rigurosamente los principios de celeridad y eficacia eliminando trámites innecesarios, reclamando la adopción de mecanismos y procedimientos ágiles, exigiendo la existencia de partidas y disponibilidades presupuestales y la apropiación de reservas y compromisos. Así las cosas, teniendo en cuenta el objeto a contratar y sus especificaciones técnicas es viable adelantar el proceso de conformidad con lo establecido en el literal a numeral 2 del artículo 2 de la Ley 1 150 de 2007. reglamentado en el Decreto 1082 de 2015.

Para tal fin, se determina el servicio especializado requerido para mantener y garantizar el correcto funcionamiento de la plataforma tecnológica de la entidad durante el año 2026, el cual se describe a continuación:

INFICALDAS ha venido incorporando una infraestructura tecnológica destinada a soportar las principales plataformas y aplicaciones institucionales, entre ellas el software ERP, el sistema de gestión documental, el directorio activo para la administración de usuarios de red, los servidores de archivos y demás servicios informáticos necesarios para garantizar la operación del Instituto.

INFICALDAS ha venido incorporando una infraestructura tecnológica destinada a soportar las principales plataformas y aplicaciones institucionales, entre ellas el software ERP, el sistema de gestión documental, el directorio activo para la administración de usuarios de red, los servidores de archivos y demás servicios informáticos necesarios para garantizar la operación del Instituto.

El Instituto ha fortalecido su infraestructura tecnológica mediante el arrendamiento de soluciones de hardware que garantizan la operación continua, independientemente de los requerimientos de procesamiento, almacenamiento o proyección de crecimiento de los diferentes sistemas de información. En esta línea, INFICALDAS ha contratado servicios de renta en infraestructura física que han asegurado el adecuado desarrollo de la misionalidad institucional.

ESTUDIO PREVIO

La arquitectura tecnológica con que actualmente cuenta el Instituto es 100% bajo la modalidad de alquiler, situación que obliga a mantener servicios disponibles, y activos en cuanto a procesamiento y almacenamiento de información. De igual forma es importante resaltar que las fallas que se presenten en las soluciones actuales son corregidas por el contratista, evento que evita e impide que algún servicio de la entidad se pueda ver comprometido y afecte la operación; este contrato de alquiler garantiza la continuidad y contingencia del negocio en un porcentaje superior al 99%.

En el mismo sentido, INFICALDAS ha venido evaluando la necesidad de modernizar su arquitectura tecnológica, considerando la migración hacia entornos en la nube como una alternativa estratégica para fortalecer la operación institucional. Si bien el modelo actual basado en soluciones físicas bajo modalidad de alquiler ha permitido la prestación continua de los servicios misionales, también ha evidenciado limitaciones significativas en materia de continuidad del negocio, escalabilidad, integración de nuevas herramientas y eficiencia operativa. La naturaleza misma de la infraestructura física impone restricciones en capacidad de crecimiento, soporte, disponibilidad y actualización tecnológica.

En este sentido, la migración hacia una infraestructura en la nube surge como una respuesta necesaria y coherente con los procesos de transformación digital de la entidad, ya que permite gestionar de manera centralizada, escalable y segura los recursos de cómputo, almacenamiento y redes. Este enfoque garantiza un entorno moderno, confiable y alineado con los objetivos institucionales de INFICALDAS, facilitando además la adopción de nuevas tecnologías y el fortalecimiento de la operación a largo plazo.

Entre los principales beneficios de adoptar un modelo de infraestructura en la nube se destacan:

1. Escalabilidad y flexibilidad: Ajuste dinámico de recursos según la demanda, evitando inversiones innecesarias en hardware físico.
2. Continuidad del negocio y resiliencia: Alto nivel de disponibilidad y recuperación ante desastres, garantizando que los servicios críticos permanezcan operativos.
3. Reducción de costos operativos: Modelo de pago por consumo (OPEX) que optimiza los recursos financieros de la entidad.
4. Actualización tecnológica constante: Acceso a las últimas versiones de software, hardware virtual y servicios gestionados sin interrupciones en la operación.
5. Gestión centralizada y automatizada: Administración simplificada de la infraestructura mediante plataformas de gestión en la nube y herramientas de automatización como Infrastructure as Code (IaC).
6. Innovación y agilidad: Facilita la incorporación de tecnologías avanzadas, como análisis de datos, inteligencia artificial y servicios gestionados, acelerando la transformación digital de la entidad.

La arquitectura propuesta estará basada en servicios gestionados en la nube, garantizando la integración de todos los componentes tecnológicos en una plataforma unificada, segura y altamente disponible. Esta estrategia permitirá que INFICALDAS evolucione hacia un entorno digital moderno, alineado con los objetivos misionales y estratégicos, fortaleciendo su capacidad para ofrecer servicios eficientes y de calidad a la comunidad del Departamento de Caldas.

Justificación Técnica de la Migración a Nube Privada:

1. Seguridad y control:
    - La nube privada ofrece un entorno dedicado exclusivamente a INFICALDAS, garantizando mayor control sobre la información sensible y cumpliendo con las normativas de protección de datos.
    - Permite implementar políticas de acceso, firewall virtual, VPN, cifrado y monitoreo continuo, asegurando la integridad y confidencialidad de los datos.
2. Escalabilidad y flexibilidad:
    - La infraestructura en nube permite ajustar dinámicamente recursos de cómputo, memoria y almacenamiento según la demanda.
    - Se eliminan las limitaciones físicas de los servidores tradicionales y la necesidad de inversiones adicionales en hardware.
3. Continuidad del negocio y resiliencia:
    - La nube privada garantiza alta disponibilidad, redundancia de servicios y respaldo con múltiples puntos de retención inmutables, asegurando que los servicios críticos permanezcan operativos ante cualquier eventualidad.
    - La gestión de desastres (DRP) se optimiza, permitiendo una recuperación rápida y minimizando impactos financieros, operativos y de reputación.

4. Optimización de costos y recursos:
    - Se pasa de un modelo CAPEX (compra de hardware) a OPEX (pago por consumo), evitando gastos en infraestructura física y mantenimiento.
    - Se reduce el tiempo de gestión interna, dado que el proveedor administra servidores, almacenamiento, redes y licenciamiento incluido.
5. Actualización y soporte continuo:
    - La nube privada permite disponer de la última versión de software y hardware virtual, con mantenimiento y soporte permanente.
    - Se garantiza la atención de incidentes, monitoreo proactivo y migración de servicios sin interrupción de las operaciones.
6. Integración y modernización tecnológica:
    - Facilita la adopción de nuevas tecnologías y servicios avanzados, como análisis de datos, inteligencia artificial y herramientas de colaboración.
    - Mejora la eficiencia operativa, permite automatizar tareas administrativas y soporta la transformación digital de la entidad.

La migración hacia una nube privada representa la solución más adecuada para INFICALDAS, garantizando un entorno seguro, flexible, escalable y altamente disponible. Esta estrategia permite que la entidad mantenga la continuidad de sus operaciones, optimice costos y recursos, y se alinee con las mejores prácticas de transformación digital y gestión moderna de TI. Por tanto, se recomienda contratar la solución de Infraestructura como Servicio (IaaS) en nube privada, junto con los servicios de soporte y monitoreo, para asegurar el correcto funcionamiento y evolución de la plataforma tecnológica durante el año 2026 y los periodos siguientes.

La adopción de una infraestructura en nube privada por parte de INFICALDAS se enmarca en el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) 2025–2030, documento que orienta cómo la entidad debe utilizar las TIC para alcanzar sus objetivos estratégicos. Este plan busca asegurar que las soluciones tecnológicas se encuentren alineadas con las necesidades del negocio, impulsen la eficiencia institucional, fortalezcan los procesos de transformación digital y optimicen la prestación de servicios a la comunidad del Departamento de Caldas.

Las entidades estatales en Colombia, incluyendo INFICALDAS, están obligadas a contar con Planes Estratégicos de TIC mediante normativas como la Ley 87 de 1993, el Decreto 1499 de 2014, el Decreto 1078 de 2015 y el Decreto 767 de 2022. Estas disposiciones buscan garantizar la alineación de las tecnologías de la información con los objetivos institucionales, promoviendo la eficiencia, la transparencia y la modernización de la administración pública.

La adopción de una infraestructura en nube privada por parte de INFICALDAS se encuentra alineada con el Plan Estratégico de Tecnologías de la Información y las Comunicaciones –PETI 2025–2030, instrumento que define la manera en que la entidad debe utilizar las TIC para alcanzar sus objetivos estratégicos. Este plan establece directrices orientadas a asegurar que las soluciones tecnológicas respondan a las necesidades del negocio, impulsen la eficiencia institucional, fortalezcan los procesos de transformación digital y optimicen la prestación de servicios a la comunidad del Departamento de Caldas.

En Colombia, las entidades estatales incluida INFICALDAS están obligadas a formular y mantener actualizado su Plan Estratégico de TIC, conforme a lo dispuesto en la Ley 87 de 1993, el Decreto 1499 de 2014, el Decreto 1078 de 2015 y el Decreto 767 de 2022. Estas normas buscan garantizar que la gestión tecnológica esté alineada con los objetivos institucionales y que se promuevan principios de eficiencia, transparencia y modernización en la administración pública.

El PETI de 2024 de INFICALDAS no contaba con los lineamientos necesarios para impulsar la transformación digital a través de un portafolio de proyectos alineado con los objetivos institucionales, lo que dificultaba el cumplimiento de las metas estratégicas a corto, mediano y largo plazo. Asimismo, no fortalecía de manera suficiente las capacidades del Área de Sistemas para respaldar la estrategia y el modelo operativo de la entidad.

Del mismo modo, dicho plan no facilitaba la identificación de herramientas que permitieran disponer de información oportuna para la toma de decisiones, ni promovía el desarrollo y mejoramiento continuo de la gestión institucional. Tampoco incorporaba prácticas adecuadas de gestión y gobierno de TI, lo que limitaba la adopción de tecnologías emergentes o disruptivas necesarias para apoyar de manera efectiva la operación misional de INFICALDAS.

Como consecuencia de estas limitaciones y con el fin de subsanar las brechas identificadas, en mayo de 2025 INFICALDAS, mediante concurso de méritos, suscribió el contrato INFI251084 con la empresa SOFTWITZ S.A.S., cuyo objeto fue la “Revisión

y actualización del Plan Estratégico de Tecnologías de la Información, con base en el marco de trabajo del Ministerio de Tecnologías de la Información, las buenas prácticas establecidas para este tipo de planes y la normatividad aplicable.

En sesión del Comité de Gerencia del 18 de septiembre de 2025 (Acta No. 14) se presentó y aprobó oficialmente el PETI, consolidando la planeación institucional con la normativa vigente y la Política de Gobierno Digital. En este contexto, la migración hacia una infraestructura en nube privada se convierte en una estrategia clave del PETI, garantizando que la entidad:

- Evolucione hacia un entorno digital moderno, seguro y altamente disponible.
- Mantenga la continuidad del negocio, la resiliencia y la escalabilidad de sus servicios tecnológicos.
- Optimice costos operativos mediante un modelo de consumo eficiente (OPEX).
- Facilite la adopción de nuevas tecnologías y la innovación en la prestación de servicios.
- Administre de manera centralizada y automatizada los recursos de cómputo, almacenamiento y red.

A continuación, se presenta la información definida en el PETI 2025-2030 para cada uno de los componentes de la infraestructura tecnológica, con el fin de orientar su renovación y adecuación conforme a las necesidades institucionales.

"Infraestructura de TI

"…El modelo de negocio de INFICALDAS se adapta con facilidad a las nuevas tendencias en evolución de las tecnologías de la información. Sin embargo, aunque la infraestructura tecnológica actual es funcional, no garantiza de manera eficaz la implementación de un plan de continuidad del negocio. Además, la incorporación de nuevas tecnologías no se integra de forma óptima con el objetivo de mitigar disrupciones en el servicio, lo cual podría impactar directamente al negocio en aspectos financieros, de imagen, reputación, nivel de servicio, entre otros.
El análisis evidenció que el área de Tecnologías de la Información no posee un valor estratégico claramente definido dentro de la organización. Esta situación denota una falta de alineación con los objetivos corporativos en materia de transformación digital, lo cual limita significativamente su capacidad para evolucionar y posicionarse a la vanguardia tecnológica. En consecuencia, se desaprovechan oportunidades para optimizar procesos clave y mejorar el desempeño en ámbitos críticos como auditoría, seguridad de la información y productividad organizacional."

"Uso y apropiación de TI

En el Instituto de Financiamiento, Promoción y Desarrollo de Caldas (INFICALDAS), el uso y apropiación de Tecnologías de la Información (TI) se refiere a la forma en que se implementan y adaptan las herramientas tecnológicas para alcanzar los objetivos de la organización. El "uso" de las TI implica la aplicación efectiva de las herramientas y recursos digitales disponibles en las operaciones diarias. Es decir, cómo se utilizan estas tecnologías en el día a día para llevar a cabo las tareas. Por otro lado, la "apropiación" va más allá del simple uso. Se trata de integrar estas tecnologías en la cultura de INFICALDAS, asegurando que todos los miembros no solo las utilicen, sino que también las comprendan y las adapten a sus propias tareas y procesos. Esto significa que la tecnología se convierte en una parte intrínseca de cómo trabajan y evolucionan. INFICALDAS en la actualidad no cuenta con planes de uso y apropiación definidos y mantenidos en el tiempo, que puedan llevar a los colaboradores a una capacitación y adopción constante de las tecnologías implementadas y por implementar en el instituto."

"Estrategia de uso y apropiación de TI
La estrategia de uso y apropiación de Tecnologías de la Información (TI) en el Instituto de Financiamiento, Promoción y Desarrollo de Caldas – INFICALDAS, comprende un conjunto articulado de acciones y enfoques orientados a garantizar que las tecnologías implementadas no solo sean utilizadas, sino verdaderamente integradas, comprendidas y adoptadas por todos los grupos de valor. INFICALDAS reconoce que el verdadero valor de las TI no radica únicamente en su instalación o disponibilidad, sino en su capacidad para transformar positivamente los procesos institucionales, fortalecer la cultura organizacional y facilitar una toma de decisiones más ágil, informada y estratégica. Para ello, se promueve un entorno donde los empleados y demás partes interesadas se sientan acompañados, capacitados y motivados a incorporar estas herramientas en su quehacer diario, generando así una cultura digital sólida, sostenible y alineada con los objetivos misionales de la entidad."

Tabla 36. Servicios de TI de INFICALDAS y sus oportunidades de Mejora

ID	Nombre	Descripción funcional	Hallazgos u oportunidades de mejora/acciones
SER-TI-011	Servidores Físicos y Virtuales	El Instituto tiene bajo el esquema de renting de infraestructura una plataforma de servidores físicos y virtuales, sobre los cuales tiene instalados los sistemas de información.	Se da la oportunidad de mejora de cambiar los servidores on-premise a la nube, esto con el fin de aumentar la flexibilidad y escalabilidad de la infraestructura tecnológica, reduciendo costos de mantenimiento y mejorando la disponibilidad y recuperación ante desastres, además de facilitar el acceso remoto seguro a los recursos empresariales, optimizando así la eficiencia operativa y permitiendo a la empresa adaptarse rápidamente a cambios en la demanda y crecimiento del negocio.

"Gobierno de TI
El gobierno de Tecnologías de la Información (TI) es crucial para asegurar que las inversiones tecnológicas estén alineadas con los objetivos estratégicos de INFICALDAS, optimizando el uso de los recursos y garantizando su eficiencia. El gobierno de TI facilita la gestión de riesgos, asegurando la continuidad del negocio y el cumplimiento normativo, especialmente en áreas clave como ciberseguridad y protección de datos. Además, promueve la innovación continua al permitir la adopción de nuevas tecnologías, mejora la toma de decisiones mediante el acceso a información precisa y favorece la transparencia y la rendición de cuentas en la gestión tecnológica."
"Políticas generales para la gestión de TI.
Las políticas generales de gestión de Tecnologías de la Información (TI) en INFICALDAS son cruciales para garantizar que las decisiones tecnológicas estén alineadas con los objetivos estratégicos y para mejorar la eficiencia operativa en un entorno cada vez más dependiente de la tecnología. Estas políticas establecen un marco robusto que orienta la toma de decisiones en el ámbito tecnológico, optimiza el aprovechamiento de los recursos disponibles y asegura la seguridad y la continuidad de las operaciones del instituto.

Tabla 42. *Políticas generales del dominio de Infraestructura*

Políticas generales del dominio de Infraestructura	
Política de Infraestructura Escalable:	Asegurar que la infraestructura tecnológica (servidores, redes, almacenamiento, etc.) sea escalable, flexible y capaz de soportar el crecimiento y las necesidades cambiantes de INFICALDAS.
Política de Redundancia y Continuidad Operativa:	Establecer sistemas de respaldo y redundancia para garantizar la continuidad de las operaciones tecnológicas en caso de fallos o desastres naturales, protegiendo la cadena de suministro y distribución.
Política de Uso Eficiente de los Recursos:	Fomentar el uso eficiente de los recursos tecnológicos, incluyendo la energía, equipos y redes, para reducir costos operativos y la huella de carbono de la infraestructura de TI.

"Infraestructura de TI
Hoy en día, en el ámbito empresarial, la tecnología no es simplemente un conjunto de sistemas y herramientas, sino el eje central que impulsa las operaciones diarias, fomenta la innovación y garantiza la competitividad. Contar con una

infraestructura tecnológica avanzada, flexible y resistente no solo permite que la entidad funcione con eficacia, sino que también le brinda la capacidad de adaptarse ágilmente a los cambios del mercado y a las exigencias del negocio.
En un escenario dominado por la transformación digital, donde la velocidad y la adaptabilidad son fundamentales, disponer de una infraestructura de TI moderna y bien planificada representa una ventaja estratégica. Aquellas empresas que incorporan tecnologías de última generación como la computación en la nube, el Internet de las Cosas (IoT), la inteligencia artificial y el análisis de datos, no solo mejoran su eficiencia operativa, sino que también pueden ofrecer a sus clientes servicios más dinámicos, personalizados y de alta calidad."

"Planteamiento de la infraestructura necesaria para la renovación de la plataforma tecnológica de INFICALDAS

La finalidad de esta propuesta es definir y suministrar la infraestructura requerida para llevar a cabo la renovación de la plataforma de la entidad. Este diseño se ha elaborado a partir del análisis de la situación actual y de los requerimientos futuros identificados en el estudio de gestión de capacidad.

Tabla 59. *Infraestructura tecnológica actual de INFICALDAS*

Equipo	Problemática	Justificación problema
Servidor físico HPE MS1050	Tecnología obsoleta, equipos sin garantía optima, no cuentan con la eficiencia óptima para la demanda del negocio, falta de innovación, vulnerabilidades de seguridad	Los equipos actualmente utilizados para el desarrollo del negocio no cumplen con los requerimientos de ciclo de vida apropiados, considerados en grado de obsolescencia.
Servidor Fileserver	El uso de un file server tradicional limita el acceso remoto, la colaboración en tiempo real y la escalabilidad del almacenamiento.	El uso continuado de un file server tradicional como principal medio de almacenamiento y gestión de archivos presenta limitaciones significativas en el contexto actual de transformación digital. Estos sistemas, aunque funcionales en su momento, ya no responden adecuadamente a las demandas de colaboración ágil, trabajo remoto y escalabilidad que exigen las organizaciones modernas.
Licenciamiento server	Licenciamiento en versión obsoleta, vulnerabilidades de seguridad, compatibilidad limitada, problemas de rendimiento, características limitadas, falta de soporte técnico, falta de innovación	Tener versiones obsoletas de software no solo pone en riesgo la seguridad, sino que también puede afectar el rendimiento, la compatibilidad, y el cumplimiento normativo.
Servidor físico HPE DL 380 – Hipervisor	El uso de servidores on-premise mplica altos costos de adquisición, mantenimiento y actualización de hardware, además de una menor escalabilidad y flexibilidad. Limita el acceso remoto seguro, dificulta la continuidad operativa ante desastres y requiere una gestión interna compleja. A diferencia de las soluciones en la nube, no permite	Esta modalidad dificulta el acceso remoto seguro, reduce la capacidad de recuperación ante desastres y puede afectar la continuidad operativa. En contraste, las soluciones en la nube ofrecen mayor flexibilidad, escalabilidad, seguridad gestionada y facilitan la adaptación rápida a cambios del negocio, aspectos esenciales para mantener la competitividad.

Equipo	Problemática	Justificación problema
	una rápida adaptación a las necesidades cambiantes del negocio ni una colaboración eficiente en entornos híbridos o distribuidos.	

”

“Principales beneficios de la infraestructura tecnológica planteada.
La migración a la nube ofrece mayor escalabilidad, flexibilidad y reducción de costos operativos. Facilita el acceso remoto seguro, mejora la continuidad del negocio mediante respaldo y recuperación rápida, y permite una gestión simplificada de recursos. Además, favorece la innovación al facilitar la integración con tecnologías avanzadas y acelerar la implementación de nuevos servicios.”

“Bases de la Arquitectura de la infraestructura tecnológica planteada.
La propuesta se fundamenta en una arquitectura completamente basada en servicios gestionados en Cloud, donde todos los componentes y funcionalidades están integrados y soportados de forma unificada a través de la plataforma global de gestión Cloud.
Cloud ofrece una infraestructura escalable y flexible que permite diseñar entornos altamente disponibles y seguros, ideales para cargas de trabajo VMware y otras aplicaciones críticas. La infraestructura en la nube permite desplegar recursos de cómputo, almacenamiento y redes de forma dinámica, ajustándose fácilmente a las necesidades de la entidad sin limitaciones físicas.
Con Cloud, es posible gestionar múltiples entornos y clústeres desde una consola centralizada como Cloud Management Console o mediante APIs, facilitando la administración y expansión de la infraestructura según la demanda. La arquitectura permite combinar diferentes tipos de instancias y configuraciones para optimizar costos y rendimiento, y definir distintos niveles de protección y redundancia a través de múltiples servicios ofrecidos por Cloud.
Los recursos en Cloud colaboran de manera integrada, compartiendo capacidades de cómputo, almacenamiento y redes distribuidas globalmente, lo que garantiza una escalabilidad transparente y una alta disponibilidad para el entorno de la entidad, permitiendo crecer con agilidad sin interrupciones ni necesidad de inversión en hardware físico.”

“Gestión Simple y completa del ciclo de vida de la plataforma.
Otra gran ventaja de las plataformas Cloud es su modelo de administración altamente automatizado y centralizado.
Cloud ofrece una gestión integral del ciclo de vida de la infraestructura y servicios a través de herramientas como Cloud Systems Manager y CloudFormation, que facilitan la automatización y simplificación de tareas que normalmente requieren intervención manual.

Entre las capacidades clave se incluyen:

- *El despliegue y configuración inicial de entornos y clústeres de cómputo, almacenamiento y redes mediante plantillas de infraestructura como código (IaC).*

- *La expansión automática de recursos, como la incorporación de nuevas instancias, volúmenes de almacenamiento o nodos a clústeres administrados, que Cloud detecta y configura sin interrupciones.*

- *Actualizaciones continuas y no disruptivas tanto del software gestionado por Cloud (sistemas operativos, servicios, parches de seguridad) como del firmware asociado a instancias, a través de procesos automatizados y prevalidaciones que garantizan la compatibilidad y estabilidad. Esto elimina la necesidad de que los administradores verifiquen manualmente matrices de compatibilidad y reduce el riesgo de errores.*

Además, con Cloud es posible monitorear el rendimiento de instancias y servicios en todo el entorno, visualizando métricas como uso de CPU, almacenamiento y memoria, tanto a nivel global como por recurso individual, facilitando una supervisión proactiva y eficiente.”

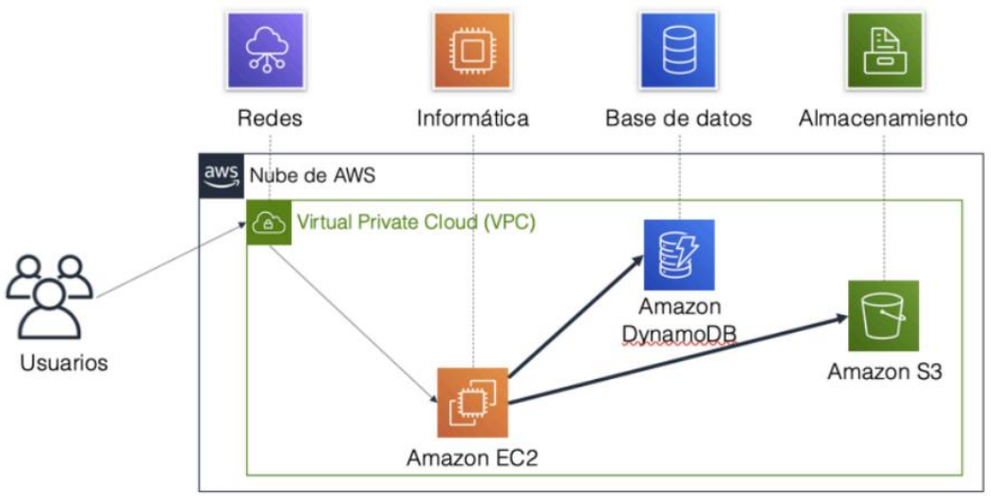
“Descripción de la infraestructura tecnológica planteada para INFICALDAS.
Una arquitectura en Cloud ofrece una solución integral y moderna que, al igual que un sistema de virtualización Onpremise, unifica recursos de cómputo, almacenamiento y red en una plataforma altamente automatizada, escalable y gestionada

centralmente. A diferencia de las infraestructuras tradicionales que dependen de hardware físico específico y separado, Cloud permite virtualizar y aprovisionar estos componentes como servicios bajo demanda, eliminando la necesidad de equipos dedicados y reduciendo significativamente la complejidad operativa.
En lugar de depender de servidores físicos agrupados como nodos de virtualización Onpremise, una plataforma Cloud como AWS ofrece instancias EC2 para cómputo, volúmenes EBS y S3 para almacenamiento, y servicios como VPC para redes, todo administrado desde una consola unificada. La infraestructura puede escalarse automáticamente según las necesidades del negocio y mantenerse mediante servicios como AWS Auto Scaling, sin requerir intervención manual para configuraciones individuales.
La propuesta equivalente en AWS considera el dimensionamiento adecuado de recursos (CPU, memoria y almacenamiento) utilizando instancias EC2 optimizadas y servicios de almacenamiento elástico, con alta disponibilidad y posibilidad de crecimiento inmediato, cumpliendo los requerimientos de capacidad definidos para la entidad."

"Arquitectura de infraestructura tecnológica
A continuación, se presenta el diseño y la organización de los componentes tecnológicos esenciales que soportan los servicios y sistemas de INFICALDAS, reestructurados bajo un modelo en la nube utilizando como ejemplo Amazon Web Services (AWS). Este diseño incluye la planificación y disposición de servicios de cómputo (instancias EC2), almacenamiento (Amazon S3, EBS, EFS), redes (Amazon VPC, Direct Connect), y plataformas (sistemas operativos, bases de datos, aplicaciones y servicios gestionados), así como su interconexión, gestión y monitoreo centralizado.
El objetivo es construir una infraestructura moderna, escalable, segura y altamente disponible que permita a la entidad operar de manera eficiente, con capacidad de adaptarse rápidamente a las necesidades futuras del negocio.
Componentes clave de la arquitectura en AWS:
- *ISP Proveedor de internet de interconexión a la nube*
- *Firewall Componente de interconexión ISP - Nube*
- *Nube pública (AWS) como entorno principal de operación.*
- *Instancias EC2 para servicios de cómputo.*
- *Amazon S3, EBS y EFS como servicios de almacenamiento escalable.*
- *Amazon VPC para redes virtuales privadas, y AWS Direct Connect o VPN para comunicación segura con redes on-premise o usuarios remotos.*

La siguiente figura proporciona una vista conceptual de la arquitectura tecnológica basada en AWS. En lugar de un enfoque tradicional de infraestructura de virtualización onpremise, esta arquitectura en la nube integra los recursos de computación, almacenamiento y red de forma virtualizada y gestionada desde una única plataforma. Esto simplifica la administración, mejora la escalabilidad y proporciona mayor resiliencia a los servicios de TI de INFICALDAS, sin la necesidad de mantener hardware físico local en el centro de datos.

Ilustración 11. *Arquitectura tecnológica basada en AWS*



"

"Administración de la capacidad de la infraestructura tecnológica
En contextos tecnológicos cada vez más complejos, donde las organizaciones requieren infraestructuras flexibles y escalables, la gestión de la capacidad adquiere un rol crítico para garantizar que los sistemas puedan responder

adecuadamente a las necesidades de los usuarios, evitando interrupciones o caídas en los servicios. Este proceso requiere una evaluación constante y una planificación anticipada que permita prever el crecimiento de la demanda y realizar los ajustes pertinentes en la infraestructura, ya sea ubicada en centros de datos físicos o como se propone para INFICALDAS, en entornos de nube."

"Áreas clave para una correcta administración de la capacidad de la infraestructura tecnológica.

La correcta administración de la capacidad de la infraestructura tecnológica es esencial para garantizar que los recursos tecnológicos sean eficientes, escalables y estén alineados con las necesidades del negocio. Esto implica gestionar de manera efectiva diversos componentes y procesos, asegurando que la infraestructura esté siempre disponible, optimizada y preparada para afrontar las demandas actuales y futuras. A continuación, se detallan las áreas clave que deben ser gestionadas para lograr una administración exitosa de la capacidad de la infraestructura tecnológica:

- *Gestión de recursos físicos, virtuales y cloud: Optimización del uso de servidores, almacenamiento y servicios en la nube, garantizando flexibilidad y escalabilidad.*
- *Administración de hardware de conectividad: Mantenimiento y configuración adecuados de los componentes de red, como switches y routers, para asegurar un rendimiento máximo.*
- *Administración de software: Actualización y gestión de aplicaciones y sistemas operativos, asegurando su integración con la infraestructura tecnológica.*
- *Gestión de LAN/WAN/WIFI: Planificación y mantenimiento de redes locales, de área amplia y redes inalámbricas, asegurando conectividad estable y segura.*
- *Monitoreo de servicios: Supervisión constante de los servicios críticos para detectar y resolver fallos rápidamente, manteniendo la disponibilidad.*
- *Planificación de capacidad: Garantizar que la infraestructura tecnológica pueda escalar de manera adecuada ante el crecimiento y aumento de la demanda.*
- *Evaluación de costos: Control de los costos asociados con la infraestructura tecnológica, asegurando que los recursos sean rentables y eficientes.*
- *Plan de continuidad, disponibilidad y DRP: Implementación de un plan para garantizar la resiliencia de la infraestructura y su recuperación ante eventos inesperados.*
- *Gestión de SLA y ANS: Aseguramiento de que los proveedores y equipos internos cumplan con los niveles de servicio acordados, optimizando la calidad y eficiencia operativa."*

descripción detallada de los proyectos que conforman la Hoja de Ruta TIC de INFICALDAS para el periodo 2025–2030.

ESTUDIO PREVIO

Campo	Detalle
ID	Serv TI 1
Nombre del Proyecto	Trasladar los servicios a la nube
Descripción Resumida	Cierra brechas de infraestructura y escalabilidad, alineando el proyecto al MGGTI y al PETI MinTIC, con enfoque en eficiencia operativa, resiliencia tecnológica, seguridad digital y optimización de costos mediante gestión de servicios en la nube.
Objetivo Estratégico (OETI / Institucional)	Objetivo 1. Maximizar la generación de valor a través de soluciones financieras innovadoras / OETI02: Transformar la experiencia del cliente mediante tecnología / OETI04: Fomentar la innovación digital Objetivo Transversal. Consolidar una gestión organizacional enmarcada en el Modelo Integrado de Planeación y Gestión y Gobierno Corporativo Maximizar generación de valor mediante soluciones financieras innovadoras / OETI06: Mejorar la eficiencia operativa mediante la automatización
Linea de tiempo:	2026 (4 meses)
Costo Estimado	$ 210.210.000
Impacto Esperado	Optimización de costos y escalabilidad inmediata de los servicios; agilidad en despliegue de soluciones, disponibilidad 24/7 y flexibilidad en la operación

”

El Plan Estratégico de Tecnologías de la Información y las Comunicaciones –PETI 2025–2030 de INFICALDAS constituye un insumo fundamental y parte integral del proceso precontractual que sustenta la presente licitación. Su contenido orienta la planeación, priorización y ejecución de las iniciativas tecnológicas de la entidad, garantizando que los requerimientos definidos se encuentren alineados con los objetivos estratégicos institucionales, la transformación digital y las necesidades operativas que soportan la misión de INFICALDAS.

De esta manera, la transición a la nube privada no solo responde a necesidades técnicas, sino que se alinea con los objetivos estratégicos institucionales definidos en el PETI, fortaleciendo la gestión tecnológica, la eficiencia operativa y la capacidad de INFICALDAS para ofrecer servicios de calidad a la comunidad del Departamento de Caldas.

Dado el portafolio de servicios que INFICALDAS desarrolla servicios financieros, banca de desarrollo e inversiones patrimoniales la operación institucional depende de sistemas de información seguros, disponibles y escalables, capaces de soportar la gestión financiera, la toma de decisiones estratégicas y la ejecución de proyectos de impacto territorial. Por estas razones, la migración hacia una infraestructura en la nube se convierte en un componente esencial para garantizar la continuidad y fortalecimiento de las funciones misionales.

En primer lugar, los servicios financieros y de crédito requieren plataformas con alta disponibilidad, integridad de datos y tiempos de respuesta confiables, especialmente para la administración de excedentes de liquidez y el análisis de riesgo

financiero. Una infraestructura en la nube permite garantizar estos niveles de servicio con mayores estándares de seguridad, redundancia y continuidad del negocio que las soluciones físicas tradicionales.

De igual manera, la banca de desarrollo, orientada al acompañamiento de proyectos estratégicos para el crecimiento económico, la infraestructura, el turismo y la sostenibilidad del territorio, exige herramientas tecnológicas que faciliten el análisis de información, el seguimiento de proyectos y la articulación con diversas entidades. La nube ofrece escalabilidad inmediata y la posibilidad de integrar nuevas soluciones analíticas, plataformas colaborativas y herramientas de monitoreo sin las restricciones propias de los equipos físicos.

Por su parte, la gestión de inversiones patrimoniales demanda entornos tecnológicos seguros, que permitan la administración de información sensible, proyecciones financieras y operaciones estratégicas con niveles altos de disponibilidad y protección. La nube proporciona mecanismos avanzados de seguridad, control de acceso y respaldo, minimizando riesgos operativos y fortaleciendo la confianza sobre la información institucional.

La migración a la nube contribuye al cumplimiento de los lineamientos del PETI actualizado, al permitir que las TIC se integren plenamente con la misión y los objetivos estratégicos de INFICALDAS, promoviendo la eficiencia operativa, la innovación y la incorporación de tecnologías disruptivas que impulsan la transformación digital.

Para garantizar la adecuada transición de la plataforma tecnológica de INFICALDAS desde el entorno On Premise hacia la infraestructura en la nube, el contratista deberá contar con un equipo profesional especializado encargado de la planificación, ejecución y aseguramiento de la migración, incluyendo las actividades que requieran presencia en sitio.

Considerando que el contrato actual de infraestructura finaliza el 31 de diciembre de 2025, y con el fin de asegurar la continuidad del servicio y la disponibilidad operativa de los equipos, el contratista deberá coordinar con el contratista saliente las actividades técnicas indispensables para la entrega, migración y puesta en funcionamiento de la infraestructura tecnológica, tales como cronogramas, inventarios, acceso a información y procedimientos de transición.

Esta coordinación tendrá un carácter estrictamente técnico y operativo, sin que en ningún caso implique transferencias económicas, pagos, reconocimientos de valor o subordinación contractual entre los contratistas.

El contratista deberá disponer de un equipo profesional especializado con experiencia comprobable en migraciones de infraestructura tecnológica desde entornos On-Premise hacia la nube. El equipo deberá contar con competencias en:

- Planeación y gestión de la migración, incluyendo coordinación con contratistas salientes y definición de cronogramas de trabajo.
- Administración y operación de infraestructura tecnológica, tanto en entornos locales como en la nube, asegurando disponibilidad, rendimiento y seguridad de los sistemas.
- Seguridad y cumplimiento normativo, garantizando la protección de la información y el cumplimiento de estándares aplicables durante la transición.
- Pruebas, validación y aseguramiento de la continuidad operativa, asegurando que la infraestructura y las aplicaciones funcionen correctamente después de la migración.

El equipo deberá estar en capacidad de realizar actividades tanto de manera remota como presencial, según sea necesario para la correcta ejecución de la migración.

2. DRaaS EN NUBE

El Instituto cuenta actualmente con una solución tecnológica que soporta de manera adecuada sus procesos misionales, incluyendo un sistema ERP (Enterprise Resource Planning) que atiende las necesidades operativas y financieras de la entidad. Esta infraestructura debe complementarse con un servicio especializado de respaldo y continuidad del negocio que permita preservar de forma segura las copias de seguridad de los sistemas de información y asegurar la disponibilidad de los recursos necesarios para restablecer la operación en el menor tiempo posible ante cualquier eventualidad.

En este sentido, se requiere una solución que garantice la disponibilidad continua y el funcionamiento estable de los servidores que conforman la infraestructura tecnológica institucional, entre ellos el Directorio Activo, encargado de la autenticación y gestión de usuarios; el sistema financiero ERP; el servidor de archivos; y el sistema de gestión documental, considerados todos como servicios críticos para la operación diaria del Instituto.

En consecuencia, la solución debe permitir la recuperación y puesta en operación de estos servicios en el menor tiempo posible, asegurando la continuidad del respaldo y la disponibilidad inmediata de la información para los usuarios de INFICALDAS en caso de una contingencia que impida el funcionamiento normal de los sistemas de información en la sede principal.

Por ello, se plantea la implementación de un esquema de copias de seguridad continuo en un centro de datos externo, que permita contar con la totalidad de la solución ERP financiero y sus datos replicados en un sitio alterno provisto por el proveedor. Este centro de datos debe contar con el espacio de almacenamiento suficiente para conservar y respaldar los servidores definidos por INFICALDAS, así como para soportar la operación temporal en contingencia cuando sea necesario activar el sitio alterno.

La circular básica jurídica de la Superintendencia Financiera en la Parte I, Titulo IV, Capitulo V, menciona los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad. Así mismo en su artículo 4 menciona lo siguiente: *"Las entidades deben desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la gestión de la ciberseguridad. La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad. En esta etapa, las entidades cuando menos:*

> *4.1.2 Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos de información.*
> *4.1.3 Gestionar y documentar la seguridad de la plataforma tecnológica*
> *4.1.4 La unidad de la que se trata el subnumeral 3.2 de este capitulo debe contar con los recursos necesarios para realizar una adecuada gestión de la seguridad de la información y la ciberseguridad.*
> *4.1.5 Identificar, y en la medida de lo posible, medir, los riegos cibernéticos emergentes que puedan llegar a afectar a la entidad y establecer controles para su mitigación.*
> *4.1.6 Considerar dentro del plan de continuidad del negocio la respuesta, reanudación de la operación en contingencia y restauración ante la materialización de ataques de cibernéticos.*
> *4.1.8 Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, tal como un SIEM.*

Es necesario que se cumpla una serie de parámetros que plantea la Superintendencia Financiera circular 034 de 2013 y que el numeral 2.1.3.3 define los aspectos a ser evaluados por este ente de control y vigilancia en su funcionamiento y calidad, que se encuentran definidos a continuación:

> *Numeral 2.1.3.2, literal b: "Descripción de la plataforma tecnológica sobre la cual operan las actividades supervisadas, considerando tales como*
>
> - *Equipos Centrales*
> - *Sistemas Operativos*
> - *Sistema de administración de bases de datos*
> - *Red de comunicaciones*
> - *Canales mediante los cuales se prestan los servicios indicando si son propios o se tiene contrato con un tercero*
> - *Centro de cómputo principal y de contingencia indicando los controles de seguridad física y de ambiente*
> - *Controles de seguridad lógica a nivel de sistema operativo y bases de datos."*

De igual manera, en la misma circular, en el numeral 2.9 Requerimientos tecnológicos y operativos, el documento reza lo siguiente:

> *Para la realización de las actividades objeto de supervisión INFICALDAS deberá contar:*
>
> - *Una plataforma tecnológica para su operación, la cual deberá estar acorde con el tamaño de la entidad.*
> - *La implementación de los requerimientos mínimos de seguridad y calidad que le aplican en el manejo de información de las actividades supervisadas.*
> - *Un plan de conservación, custodia y seguridad de la información, tanto documental como electrónica.*
> - *Un Plan de Contingencia y continuidad del negocio que tenga como finalidad primordial prevenir y solucionar los problemas, fallas e incidentes que se puedan presentar en cualquiera de los sistemas de información que se tengan dispuestos en la operación de las actividades supervisadas, de tal manera que se garantice la realización de las actividades objeto de supervisión.*

- *La descripción de los procesos para cada una de las actividades objeto de supervisión, con sus respectivos procedimientos y soporte tecnológico.*
- *Mecanismos para la administración del riesgo operativo a que se expone las actividades objeto de supervisión, con el fin de gestionarlos y minimizar la probabilidad o impacto en los casos que se materialicen.*
- *La información de aquellas actividades objeto de supervisión que pretendan ser contratadas con terceros, indicando el objeto de la respectiva contratación los requisitos a exigir a la firma a contratar, el detalle de las funciones que se contratarán externamente, los controles y áreas encargadas de seguimiento a dichos contratos. Esta información debe ser remitida a la Superintendencia con quince (15) días de antelación al inicio de dicho contrato.*

Así las cosas y en armonía con los requerimientos de la Superintendencia Financiera, INFICALDAS requiere contratar con personas naturales o jurídicas que se encuentre en las condiciones de ejecutar el objeto requerido, con experiencia, con personal capacitado en la labor y que cuente con los elementos necesarios para satisfacer la necesidad del Instituto y en las condiciones que la misma establezca.

Para la vigencia 2025, el Instituto contó con un servicio centrado en la realización de copias de respaldo y en la replicación básica de información. Esta solución se limitaba a programar tareas de backup, almacenar los datos en repositorios definidos y establecer un mecanismo de conexión segura mediante VPN para su administración.

Si bien este modelo permitía conservar la información institucional y realizar restauraciones puntuales, desde el punto de vista técnico no ofrecía capacidades de continuidad operativa, ya que no disponía de infraestructura alterna, procesamiento en la nube, ni mecanismos para activar los servicios críticos en caso de falla del centro de datos principal. En términos de ingeniería, el contrato anterior operaba únicamente en la capa de protección de datos, pero no en la capa de disponibilidad y recuperación.

La necesidad de una solución más robusta surge debido al aumento en la criticidad de los sistemas corporativos del Instituto, especialmente el ERP financiero, el servidor de archivos, el sistema de gestión documental y el directorio activo, los cuales deben mantenerse operativos bajo un esquema de alta disponibilidad. Asimismo, los riesgos operativos y tecnológicos relacionados con ciberataques, fallas de hardware, interrupciones eléctricas, corrupción de datos y eventos ambientales exigen adoptar un modelo de continuidad del negocio basado en parámetros claros de RTO (Recovery Time Objective) y RPO (Recovery Point Objective), los cuales el esquema anterior no podía garantizar. Adicionalmente, los lineamientos actuales de seguridad y ciberresiliencia requieren infraestructura capaz de escalar, aislar cargas de trabajo y ejecutar procesos de recuperación sin depender del entorno físico principal.

Por estas razones, se requiere migrar hacia una solución de Recuperación ante Desastres como Servicio (DRaaS) soportada en infraestructura en la nube. Este modelo incorpora elementos técnicos que representan una mejora sustancial frente al esquema previo, entre ellos:

- Réplica continua de máquinas virtuales a un data center en la nube, con sincronización en tiempo casi real.
- Aprovisionamiento de recursos computacionales dedicados (vCPU, memoria, almacenamiento e IP pública) para activar los servidores críticos en caso de contingencia.
- Pruebas controladas de failover y failback, que permiten validar periódicamente los planes de recuperación sin afectar la operación productiva.
- Capas de seguridad avanzadas, tales como cifrado en tránsito y en reposo, autenticación reforzada, segregación de redes y monitoreo de integridad.
- Almacenamiento de larga duración en AWS Glacier, adecuado para bases de datos y respaldos históricos del ERP, con durabilidad superior al 99,999999999%.
- Soporte especializado y monitoreo proactivo, que permite detectar fallas antes de que impacten los servicios institucionales.

A diferencia de la solución anterior, que únicamente resguardaba datos, el modelo basado en DRaaS garantiza la recuperación funcional del entorno tecnológico completo, permitiendo levantar los servicios institucionales en un sitio alterno en cuestión de minutos u horas, dependiendo de los RTO establecidos. Esto se traduce en continuidad del negocio, operación resiliente y una respuesta rápida ante eventos disruptivos.

En conclusión, la implementación de una arquitectura de continuidad del negocio basada en la nube constituye una necesidad técnica prioritaria para asegurar la estabilidad, integridad y disponibilidad de los sistemas de información del

Instituto. Esta solución supera ampliamente las capacidades del contrato anterior y se articula con las mejores prácticas de ingeniería, seguridad y recuperación ante desastres.

En concordancia con lo anterior, es importante señalar que la transición institucional hacia una infraestructura tecnológica en la nube es un componente esencial del fortalecimiento del Plan de Continuidad del Negocio de INFICALDAS. Este proceso requiere que las actividades de respaldo, réplica, recuperación y disponibilidad de los servicios críticos se adapten a la nueva arquitectura tecnológica, garantizando que la operación pueda mantenerse o restablecerse de manera oportuna ante cualquier contingencia.

En este sentido, el Plan de Continuidad deberá incorporar los lineamientos, procedimientos y capacidades técnicas asociadas a la migración a la nube, asegurando que dicha transición se ejecute de manera ordenada, segura y en coherencia con los requerimientos de la Superintendencia Financiera, así como con las metas establecidas en el PETI 2025–2030.

3. Licenciamiento, suministros tecnológicos y soporte integral de infraestructura

Además de los requerimientos de infraestructura tecnológica y de las capacidades necesarias para el Plan de Continuidad del Negocio, INFICALDAS requiere garantizar la operación, seguridad, sostenibilidad y disponibilidad de todos los servicios digitales que soportan su misión institucional. Esto implica no solo fortalecer la arquitectura tecnológica, sino asegurar la renovación, actualización y continuidad de los licenciamientos y servicios que permiten que dicha infraestructura funcione de manera segura, estable y conforme a los lineamientos de la Superintendencia Financiera, la Política de Gobierno Digital y el PETI 2025–2030.

En este sentido, la infraestructura tecnológica del Instituto no puede concebirse únicamente desde la perspectiva de los recursos físicos o computacionales; también depende de los servicios de software, las plataformas de ofimática y productividad, las herramientas de seguridad, los mecanismos de autenticación, las soluciones de respaldo y recuperación, así como de los servicios especializados de soporte y atención que garantizan la operación diaria del Instituto.

Cada uno de estos componentes forma parte integral del ecosistema tecnológico institucional y resulta indispensable para prevenir fallas, mitigar riesgos, asegurar el cumplimiento normativo y garantizar que los procesos internos puedan desarrollarse de manera eficiente y estable. En conjunto, estos elementos permiten que la operación del Instituto funcione adecuadamente en el día a día, preservando la seguridad de la información y la disponibilidad de los servicios que soportan la gestión administrativa, financiera y operativa de INFICALDAS.

1. Licenciamiento de Correo Electrónico, Ofimática y Power BI

El Instituto adoptó Microsoft Office 365 como plataforma institucional para correo, ofimática y productividad, reemplazando la infraestructura heredada de Google sin soporte técnico y con capacidades limitadas. Tras su implementación y consolidación en el año 2023, la plataforma se convirtió en un componente crítico para las comunicaciones institucionales, la gestión documental, la colaboración interna y el soporte operativo de todas las áreas.

La renovación del servicio para la vigencia 2026 es indispensable para garantizar:

- Disponibilidad continua del correo institucional.
- Acceso seguro a herramientas de productividad.
- Cumplimiento de estándares de seguridad y retención de datos.
- Integración con Power BI, herramienta clave para analítica, informes gerenciales y toma de decisiones basadas en datos.

Dado que Office 365 es un servicio basado en la nube, su renovación resulta indispensable para mantener la operación de la plataforma, la cual depende de licenciamientos vigentes y de la continuidad de los servicios provistos por el fabricante.

2. Bolsa de Suministro para Elementos de Informática

La operación tecnológica del Instituto requiere insumos permanentes para estaciones de trabajo, servidores y periféricos. Las necesidades son variables según área, función y nivel de criticidad del equipo. La modalidad de bolsa permite una provisión flexible, eficiente y oportuna frente a daños, reemplazos, expansiones o actualizaciones, asegurando:

- Continuidad operativa del personal.
- Sostenibilidad de la infraestructura de usuario final.
- Atención inmediata de requerimientos técnicos que impactan la productividad.

Sin esta disponibilidad, la operación institucional se enfrenta a interrupciones que afectan la prestación del servicio público.

3. Renovación Cisco Umbrella – Protección de Navegación para Usuarios Remotos

En un modelo moderno de continuidad del negocio, la seguridad ya no se limita al perímetro físico. Los usuarios acceden desde redes externas, hogares o ubicaciones remotas, lo que genera riesgos de navegación, malware, phishing y sitios maliciosos.

Cisco Umbrella proporciona:

- Protección basada en DNS para todos los usuarios remotos.
- Visibilidad y control centralizado del tráfico fuera de las instalaciones.
- Mitigación de ataques provenientes de navegación insegura.

Su renovación para 2026 es indispensable para seguir protegiendo la entidad en escenarios híbridos de trabajo, alineado con los lineamientos de seguridad digital.

La selección de Cisco Umbrella obedece a criterios técnicos asociados a la solución que actualmente soporta los procesos de seguridad institucional y que se encuentra plenamente integrada al ecosistema tecnológico de INFICALDAS.

En la vigencia 2021 la Entidad adoptó esta solución como mecanismo de protección para usuarios remotos, configurándola, ajustándola y vinculándola a los lineamientos de seguridad digital, monitoreo y control de navegación definidos por el área de TI. A partir de dicha implementación se han construido políticas, reglas de seguridad, perfiles de usuario y reportes técnicos que hoy permiten:

- Disponer de visibilidad centralizada sobre el tráfico DNS interno y externo.
- Aplicar políticas de seguridad consistentes para usuarios internos y remotos.
- Mantener un registro histórico continuo de eventos, alertas y actividades sospechosas.
- Integrar la protección con otros componentes del ambiente Cisco ya configurados en INFICALDAS.
- Garantizar la continuidad del servicio, al ser la plataforma probada, estabilizada y operativa en la Entidad.

Implementar un producto diferente implicaría:

- Reconfigurar completamente las políticas de navegación para más de 50 usuarios.
- Interrumpir el esquema de monitoreo y telemetría que se ha consolidado desde 2021.
- Generar inconsistencias en la protección de usuarios remotos, afectando las medidas actuales de seguridad.
- Asumir costos adicionales de despliegue, migración, capacitación y ajuste.
- Incrementar los riesgos operativos durante la transición tecnológica.

Adicionalmente, Cisco Umbrella cumple con los criterios funcionales exigidos para entidades vigiladas por la Superintendencia Financiera, al ofrecer:

- Protección DNS avanzada.
- Prevención de malware, phishing y dominios maliciosos.
- Control de navegación y categorización web.
- Reportes y auditorías exhaustivas para gestión del riesgo tecnológico.

Por lo anterior, la renovación del licenciamiento Cisco Umbrella constituye la alternativa técnica más adecuada para INFICALDAS, al garantizar continuidad operativa, mantenimiento de las políticas institucionales de seguridad, integración con el ecosistema existente y mitigación de riesgos asociados a la navegación y trabajo remoto.

4. Licenciamiento Cisco DUO – Autenticación Multifactor (MFA)

ESTUDIO PREVIO

La autenticación de doble factor constituye un mecanismo de seguridad obligatorio para las entidades vigiladas por la Superintendencia Financiera, en cumplimiento de los lineamientos establecidos en las Circulares Externas 007 y 008 de 2019, que exigen la adopción de controles robustos de autenticación para mitigar riesgos de acceso no autorizado, suplantación de identidad y vulnerabilidades previsibles.

Adicionalmente, la póliza de seguro Cyber adquirida por INFICALDAS establece como condición de asegurabilidad la implementación de mecanismos avanzados de autenticación para los usuarios remotos, con el fin de reducir la exposición a incidentes de ciberseguridad y garantizar la aplicabilidad plena de las coberturas contratadas.

La adopción de un sistema MFA permite:

• Fortalecer el acceso seguro a los sistemas institucionales al requerir un segundo factor de verificación.
• Reducir el riesgo de intrusiones, accesos indebidos y ataques de fuerza bruta asociados a credenciales comprometidas.
• Dar cumplimiento a los requisitos regulatorios y de gestión del riesgo tecnológico definidos para entidades vigiladas.

Por lo anterior, la adquisición de una solución de autenticación multifactor no constituye un elemento opcional, sino un requisito técnico, normativo y asegurador indispensable para la operación segura de la infraestructura tecnológica de INFICALDAS.

La selección de Cisco Duo como solución de autenticación multifactor (MFA) responde a criterios técnicos, operativos y de continuidad institucional, derivados del ecosistema tecnológico ya implementado en INFICALDAS y de los requisitos normativos de la Superintendencia Financiera.
No se trata de una preferencia por la marca, sino de la necesidad de garantizar compatibilidad, integración, continuidad operativa y cumplimiento regulatorio, aspectos que no pueden ser asegurados por cualquier solución MFA genérica.

A. Integración directa con las plataformas tecnológicas actuales

Cisco Duo se integra de forma nativa con:

- La infraestructura de seguridad basada en Cisco (Umbrella, Meraki/Fortinet, control de acceso).
- Los servicios corporativos como Active Directory, infraestructura híbrida y VPN SSL.
- Plataformas Microsoft, incluido Office 365, que es el servicio de correo institucional.

Seleccionar un producto distinto implicaría realizar integraciones adicionales, más complejas o no garantizadas.

B. Continuidad técnica con los mecanismos de seguridad ya implementados

INFICALDAS ya opera bajo un modelo de seguridad que incorpora componentes Cisco. Duo extiende estas capacidades al controlar:

- Accesos remotos,
- Sesiones VPN,
- Servicios en la nube,
- Recursos corporativos internos,
- Dispositivos no administrados.

Cambiar la solución interrumpiría la arquitectura de seguridad consolidada desde 2021.

C. Garantiza cumplimiento con los requisitos de la Superfinanciera

La Superintendencia exige (Circulares 007 y 008 de 2019):

- MFA robusto, verificable y auditable.
- Control sobre accesos remotos.
- Registro detallado de autenticaciones.

Cisco Duo tiene módulos de auditoría, telemetría, reportes normativos y trazabilidad que permiten cumplir estos requisitos sin desarrollos adicionales.

D. Requisito de la póliza Cyber del Instituto

La aseguradora exige:

- MFA robusto,
- Capacidad de validación del dispositivo,
- Control en accesos remotos,
- Registros verificables de autenticación.

Cisco Duo ya está reconocido por aseguradoras como solución que cumple estas características sin necesidad de validaciones adicionales.

E. Menor riesgo operativo y costo de transición

Implementar un MFA distinto generaría:

- Reconfiguración de VPN, AD, servicios en nube y accesos internos.
- Interrupciones en el acceso de hasta 60 usuarios remotos.
- Necesidad de capacitación adicional.
- Riesgos de bloqueo de servicios críticos durante la transición.
- Costos de migración y reimplementación.
-

Con Cisco Duo no existe curva de implementación porque su arquitectura es compatible con todo lo ya configurado.

F. Tecnología probada, estable y adoptada en el sector financiero

Cisco Duo es ampliamente utilizado por entidades:

- financieras,
- aseguradoras,
- públicas y privadas de alto nivel de riesgo.

Esto garantiza confiabilidad, soporte especializado y continuidad en actualizaciones de seguridad.

La necesidad de Cisco Duo se justifica porque es la única alternativa que se integra plenamente con la arquitectura actual, cumple los requisitos normativos y de asegurabilidad, reduce riesgos operativos y garantiza que el mecanismo MFA funcione sin interrupciones, sin desarrollos adicionales y sin comprometer la operación.

5. FortiGate 100F y FortiMail Cloud

La seguridad perimetral y el filtrado avanzado de correo son componentes esenciales del DRP y de la arquitectura de continuidad del negocio. El Firewall FortiGate 100F soporta la carga operativa de hasta 100 usuarios, con IA para detección de amenazas, soporte IPv6 y visibilidad avanzada.
FortiMail Cloud permite:

- Protección integral sobre Microsoft 365.
- Prevención de spam, malware y ataques dirigidos por correo.
- Reforzar la seguridad de la capa de mensajería, un vector de ataque crítico.

Ambos servicios garantizan estabilidad, disponibilidad y seguridad institucional.

La continuidad de la solución Fortinet responde a criterios estrictamente técnicos y operativos derivados de las necesidades de seguridad, estabilidad y crecimiento de la infraestructura tecnológica de INFICALDAS. Durante la vigencia 2023, tras las limitaciones de rendimiento y caídas de red presentadas con el firewall anterior, el Instituto adoptó un dispositivo FortiGate que permitió estabilizar la operación, soportar una mayor cantidad de usuarios simultáneos y mejorar la capacidad de inspección de tráfico sin afectar la disponibilidad de los servicios. Esta solución se configuró de manera integral con la arquitectura existente, las VPN institucionales, los servicios de autenticación, el direccionamiento IPv4/IPv6 y la infraestructura híbrida implementada por el Instituto, convirtiéndose en un componente crítico para el funcionamiento seguro y continuo de la red.

Asimismo, la incorporación de FortiMail Cloud – Gateway Premium resulta necesaria debido a que esta plataforma se integra directamente con el firewall FortiGate y con el ecosistema Microsoft 365 utilizado por INFICALDAS, permitiendo reforzar la protección del correo electrónico —uno de los principales vectores de ataque— mediante filtrado avanzado, análisis de amenazas, sandboxing, validación de remitentes y políticas de protección contra phishing y malware. Esta integración nativa garantiza coherencia en las políticas de seguridad, facilita la administración centralizada y evita la necesidad de soluciones adicionales que podrían generar incompatibilidades o requerir configuraciones más complejas.

Optar por una plataforma distinta implicaría reconstruir desde cero las políticas de seguridad, reconfigurar VPN, rehacer la segmentación de red, ajustar la integración con el correo institucional y asumir riesgos operativos durante la transición, además de incurrir en mayores costos de implementación y soporte. Por el contrario, la continuidad de Fortinet y FortiMail asegura consistencia, compatibilidad plena con los servicios actuales, estabilidad en el desempeño, una protección avanzada adaptada al crecimiento institucional y una administración unificada que reduce la complejidad operativa.

En este sentido, Fortinet y FortiMail no se seleccionan por ser una marca específica, sino porque constituyen la alternativa técnica que mejor responde a la infraestructura ya implementada, a los requerimientos de seguridad digital del Instituto y a la necesidad de garantizar un funcionamiento robusto, eficiente y alineado con la arquitectura tecnológica de INFICALDAS.

6. Licenciamiento Veeam Backup – Respaldo y Recuperación

La continuidad del negocio depende de la capacidad de recuperar información en caso de fallas, incidentes o desastres. La plataforma Veeam garantiza:

- Backups en nube y en cinta.
- Virtualización eficiente para recuperación rápida.
- Protección integral de datos y buzones.

La renovación para 2026 es esencial para asegurar recuperación ante desastres y cumplimiento del DRP.

El uso de Veeam Backup se justifica técnicamente porque es la solución que actualmente se encuentra implementada, configurada y operativa en la infraestructura del Instituto, integrándose de manera nativa con los entornos virtualizados, los servicios en nube y el ecosistema de Microsoft 365 utilizado por INFICALDAS. Cambiar a una herramienta distinta implicaría rehacer toda la arquitectura de respaldo, redefinir políticas de retención, volver a integrar servidores y máquinas virtuales, capacitar nuevamente al personal técnico y asumir riesgos operativos durante la migración, afectando la disponibilidad de la información y los tiempos de recuperación ante incidentes. Veeam garantiza continuidad, estabilidad y compatibilidad plena con los servicios actuales, además de ofrecer tiempos de restauración más rápidos, gestión centralizada, escalabilidad y trazabilidad completa de los respaldos, características que resultan indispensables para el cumplimiento del Plan de Continuidad del Negocio y de los lineamientos de seguridad de la información. Por ello, mantener esta solución constituye la alternativa técnica más adecuada para proteger los datos críticos del Instituto y asegurar la operatividad de los procesos institucionales.

7. Antivirus Avanzado Basado en la Nube

La evolución de las ciberamenazas en especial el ransomware, ataques de día cero y malware avanzado— exige una solución de seguridad que supere las capacidades de los antivirus tradicionales basados únicamente en firmas. En este sentido, la implementación de una plataforma de protección de endpoints basada en la nube permite una defensa más robusta, inteligente y adaptable a los riesgos actuales.

La solución propuesta incorpora componentes especializados que fortalecen de manera integral la seguridad de estaciones de trabajo, servidores y dispositivos móviles:

- Consola de administración en la nube: Centraliza la gestión, monitoreo y aplicación de políticas de seguridad sin depender de infraestructura propia. Esta característica permite actualizaciones inmediatas, reducción de cargas administrativas y visibilidad completa del estado de protección de la entidad.
- Protección avanzada para endpoints (NGAV/EDR): Utiliza análisis de comportamiento, inteligencia artificial y detección basada en heurísticas para identificar y bloquear amenazas conocidas y desconocidas, reduciendo significativamente el riesgo de infecciones por ransomware o malware polimórfico.
- Sandboxing en la nube: Archivos y comportamientos sospechosos se ejecutan en un entorno seguro aislado, permitiendo detectar amenazas complejas que no serían identificadas por herramientas tradicionales. Esta capacidad complementa el análisis local y fortalece la prevención de ataques dirigidos.

- Cifrado de disco completo: Garantiza la protección de la información almacenada en los equipos institucionales ante pérdida, robo o acceso no autorizado, cumpliendo con buenas prácticas de protección de datos y asegurando la confidencialidad de la información pública.
- Seguridad para servidores y móviles: Amplía la cobertura de protección a toda la infraestructura, minimizando brechas y puntos de vulnerabilidad entre diferentes plataformas.
- Defensa contra amenazas avanzadas (APT): La correlación de eventos y análisis en tiempo real desde la nube permite identificar patrones maliciosos sofisticados, fortaleciendo la capacidad de respuesta frente a ataques de gran complejidad.

En comparación con un antivirus tradicional instalado localmente, el modelo cloud-based ofrece:

- Actualizaciones inmediatas desde la nube.
- Menor dependencia de hardware propio.
- Mayor capacidad de análisis gracias a procesamiento en infraestructura de nube.
- Respuesta más rápida ante amenazas emergentes.
- Reducción del riesgo operacional y mejora del control institucional.

En síntesis, la adopción de una solución de seguridad avanzada basada en la nube no solo fortalece la protección de los endpoints, sino que garantiza una postura de ciberseguridad alineada con estándares modernos, disminuye la exposición de la entidad a ataques y optimiza la administración del sistema de defensa.

Numeral 2 del Artículo 2.2.1.1.2.1.1: *"El objeto a contratar, con sus especificaciones, las autorizaciones, permisos y licencias requeridos para su ejecución"*.

Objeto. Prestación de servicios para la provisión, administración y soporte integral de la infraestructura tecnológica institucional, incluyendo servicios en la nube, mecanismos de continuidad del negocio, licenciamiento y suministro de componentes tecnológicos, así como soporte especializado.

2.1. CLASIFICACIÓN UNSPSC: En atención a la Clasificación de Bienes y Servicios de las Naciones Unidad (Versión 14 del UNSPSC) dispuesto por Colombia Compra Eficiente, el código del servicio requerido se identifica de manera precisa hasta el tercer o cuarto nivel de la clasificación UNSPSC, así:

CODIGO UNSPSC	CONCEPTO
81111800	Servicios de sistemas y administración de componentes de sistemas
81112200	Mantenimiento y soporte de software
81111809	Servicio de instalación de sistemas
43230000	Software
43233700	Software de administración de sistemas
81112206	Mantenimiento de Software o búsqueda o recuperación de la información
81112208	Mantenimiento de Software de protección y seguridad
43211600	Accesorios de computador
81112501	Servicio de licencias del software del computador

2.2. CONDICIONES TECNICAS:

De acuerdo con la Clasificación de Bienes y Servicios de las Naciones Unidad (Versión 14 del UNSPSC) dispuesto por Colombia Compra Eficiente, el código del servicio requerido se identifica de manera precisa hasta el tercer o cuarto nivel de la clasificación UNSPSC, así:

CODIGO UNSPSC	CONCEPTO
81111800	Servicios de sistemas y administración de componentes de sistemas
81112200	Mantenimiento y soporte de software
81111809	Servicio de instalación de sistemas
43230000	Software
43233700	Software de administración de sistemas
81112206	Mantenimiento de Software o búsqueda o recuperación de la información
81112208	Mantenimiento de Software de protección y seguridad
43211600	Accesorios de computador
81112501	Servicio de licencias del software del computador

ESTUDIO PREVIO

Siendo las especificaciones mínimas las que se ilustran a continuación**:**

1. Infraestructura como Servicio (IaaS)

Alquiler de infraestructura como servicio (IaaS) en nube privada, que incluye los recursos de cómputo, almacenamiento y red necesarios para la operación de la entidad, junto con los servicios de instalación, configuración, migración y puesta en marcha de la solución, de acuerdo con las siguientes especificaciones técnicas:

DESCRIPCIÓN	CANT
Infraestructure as a Service (IaaS), incluye: • 71 vCPU • 183 GB RAM • 14393 GB DISCO • 1 Public IP • Hipervisor VMware • Licenciamiento Windows Server - Linux (Incluido • Bundle IaaS) • Backup para 7 VMs con 7 puntos de retención • inmutables • Firewall virtual standard protection • VPN IPsec • Canales de Internet Redundantes	1
Servicio de soporte y monitoreo Se debe realizar servicio de migración de la solución actual a la ofertada Atención de incidentes durante la duración del contrato Entrega mensual de estado de la plataforma y de incidentes presentados	1

La infraestructura en nube para 7 máquinas virtuales, con recursos optimizados para soportar las aplicaciones críticas del cliente:

- 183 GB de memoria RAM
- 71 vCPU
- 14.393 GB de almacenamiento en nube
- 1 dirección IP pública
- Licenciamiento incluido:
- Windows Server y Linux (Bundle IaaS)
- Veeam Backup & Replication para 7 VMs, con 7 puntos de retención inmutables

Seguridad y conectividad:

- Firewall Sophos virtual con protección estándar
- VPN IPsec para acceso seguro
- Canales de Internet redundantes para alta disponibilidad

Servicios adicionales:

- Instalación y configuración completa de la solución IaaS
- Ancho de banda sin limitaciones
- Transferencia de conocimiento al equipo del cliente

Las máquinas en la nube deberán operar con sistemas operativos soportados y debidamente licenciados, alineados con la infraestructura tecnológica actual de Inficaldas, priorizando:

- Microsoft Windows Server 2022 (64 bits) para servicios institucionales, dominio, archivos, aplicaciones corporativas y gestión documental.
- Distribuciones Linux soportadas (Debian GNU/Linux 12 u Oracle Linux) para servicios específicos como monitoreo, aplicaciones especializadas o bases de datos, según corresponda.

La selección de los sistemas operativos garantizará compatibilidad con la infraestructura existente, seguridad, soporte del fabricante y cumplimiento de las políticas de TI de la entidad.

Dimensionamiento de Máquinas Virtuales

La infraestructura en la nube privada requerida para la operación de los sistemas institucionales se encuentra dimensionada con un total de 71 vCPU y 183 GB de memoria RAM, distribuidos en siete (7) máquinas virtuales, conforme a las necesidades específicas de cada servicio, de la siguiente manera:

- Servidor de Dominio 2022 INFICALDAS: 4 vCPU, 12 GB de memoria RAM y 200 GB de almacenamiento.
- File Server Nuevo: 4 vCPU, 12 GB de memoria RAM y 1.150 GB de almacenamiento.
- FS-INFICALDAS: 8 vCPU, 32 GB de memoria RAM y 7.300 GB de almacenamiento.
- Gestión Documental: 12 vCPU, 24 GB de memoria RAM y 4.500 GB de almacenamiento.
- Power BI: 20 vCPU, 60 GB de memoria RAM y 500 GB de almacenamiento.
- Servidor de Antivirus: 4 vCPU, 12 GB de memoria RAM y 800 GB de almacenamiento.
- Zabbix Proxy: 4 vCPU, 8 GB de memoria RAM y 160 GB de almacenamiento.

El dimensionamiento definido permite asignar los recursos de manera diferenciada según la carga de trabajo de cada sistema, evitando la sobreasignación de CPU (*overprovisioning*), optimizando el uso de licencias que se facturan por núcleo y garantizando el desempeño, la estabilidad y la escalabilidad de la infraestructura en la nube privada.

Los servidores en la nube alojarán principalmente los siguientes servicios y aplicaciones:

Servicios de infraestructura:

- Active Directory, DNS, DHCP
- File Server institucional
- Servicios de respaldo y recuperación (Veeam)

Aplicaciones institucionales:

- Gestión Documental
- Power BI
- Servicios de monitoreo (Zabbix)
- Antivirus y seguridad centralizada

Servicios de seguridad:

- Antivirus corporativo
- Monitoreo, registro y control de accesos

La configuración de estos servicios garantizará la continuidad operativa, la seguridad de la información y la correcta ejecución de los procesos institucionales.

Los servidores en la nube utilizan principalmente:

- Bases de datos relacionales incluidas en las aplicaciones institucionales, según la arquitectura definida por cada proveedor.
- Bases de datos de monitoreo y gestión, como Zabbix sobre Linux.

-

Las versiones de las bases de datos se mantendrán soportadas por el fabricante y alineadas con las políticas de actualización, seguridad y gestión de la información de la entidad.

En el mismo sentido, se requiere contar con un ambiente productivo 100% VMware, así como la migración al modelo *Infrastructure as a Service* (IaaS) y la implementación del Tenant. Lo anterior incluye el traslado de datos, la configuración correspondiente y la puesta en funcionamiento, garantizando la continuidad operativa y evitando cualquier pérdida de información.

La Entidad dispone actualmente de un canal de internet dedicado, para la interconexión de los servidores, con un ancho de banda mínimo de 60 Mbps, el cual garantiza:

- Acceso seguro entre la infraestructura local y los servicios en la nube.
- Replicación de respaldos y sincronización de datos.
- Acceso y operación de los sistemas institucionales alojados en servidores.
- Continuidad operativa de la infraestructura tecnológica.

Este canal no está destinado al tráfico de usuarios finales, sino a la comunicación servidor–nube. El ancho de banda podrá escalarse conforme al crecimiento de los servicios, la carga operativa y las necesidades de contingencia, asegurando la disponibilidad, estabilidad y eficiencia de la infraestructura en la nube.

La información inicial necesaria para establecer la conexión con la nueva infraestructura en la nube será suministrada por INFICALDAS. El oferente será responsable de la configuración técnica inicial de la conectividad y del firewall virtual, en el marco de la provisión de la infraestructura en la nube, con el fin de garantizar una comunicación segura, eficiente y confiable hacia dicha infraestructura.

La administración avanzada de seguridad, el monitoreo activo 24/7, la gestión de incidentes de seguridad, así como las funciones de detección y respuesta ante intrusiones (IDS/IPS) y la gestión de vulnerabilidades, serán realizadas a través del servicio de Monitoreo de Seguridad SOC, contratado directamente por INFICALDAS.

ALCANCE SERVICIO:

- Plataforma VMware vCloud director para las máquinas virtuales en el sitio del proveedor de nube.
- Certification Broadcom VMware VCSP Premier Partner
- Implementación de la solución sin cobro para el cliente.
- El proveedor no debe de generar cobros adicionales a los pactados por el servicio por carga o descarga de información, ni por transacción ni limitar el ancho de banda de acceso del cliente a la nube.
- El proveedor debe de entregar una bóveda segura de contraseñas al cliente como valor agregado
- El canal de comunicación entre el cliente y el proveedor debe establecer una sesión TLS, con un cifrado simétrico no inferior a AES-256, para proteger los datos en tránsito.

  La ventana de retención se establece en 7 días diarios, aplicable a todos los puntos de retención inmutable. La inmutabilidad de los datos debe garantizarse tanto en el sitio principal de la nube privada como en el sitio de recuperación ante desastres (DRP) de la nube privada, asegurando la replicación georredundante para el respaldo y restauración de la información institucional ante cualquier eventualidad o incidente.
- El proveedor debe de entregar al cliente un acceso a mesa de ayuda con al menos 3 canales de comunicación.

Para garantizar la adecuada transición de la plataforma tecnológica de INFICALDAS desde el entorno On Premise hacia la infraestructura en la nube, el contratista deberá disponer del equipo profesional especializado necesario para la planeación, ejecución y aseguramiento de la migración, incluyendo las actividades que requieran presencia en sitio, sin que ello implique recomendar o exigir una sede física determinada en la ciudad.

Teniendo en cuenta que el contrato actual de infraestructura finaliza el 31 de diciembre de 2025, y con el fin de asegurar la continuidad del servicio y la disponibilidad operativa de los equipos, el contratista deberá coordinar con el contratista saliente las actividades técnicas indispensables para la entrega, migración y puesta en funcionamiento de la infraestructura tecnológica, tales como cronogramas, inventarios, acceso a información y procedimientos de transición.

De igual manera, dado que el proceso de migración desde la infraestructura on-premise hacia la plataforma IaaS requiere un periodo técnico estimado de veinticinco (25) días, durante el cual deben ejecutarse actividades de replicación,

aprovisionamiento, validación de cargas de trabajo, pruebas de interoperabilidad y estabilización del entorno virtualizado, se hace indispensable garantizar la continuidad de los servicios institucionales mediante la operación ininterrumpida de la infraestructura física vigente. En este sentido, INFICALDAS deberá continuar utilizando, durante todo el proceso de transición, la plataforma instalada en 2025, compuesta por:

DESCRIPCIÓN	CANT
Especificaciones Técnicas del Servidor • Almacenamiento: 2 discos duros SAS de 300 GB a 10K. • Procesador: CPU con 10 núcleos, frecuencia base de 2.20 GHz. • Memoria RAM: 288 GB. • Tarjeta de almacenamiento: Tarjeta PCI para almacenamiento con 2 puertos FC y 2 transceptores de 16 Gbps. • Tarjetas de red: o 1 tarjeta de red PCI con 1 puerto de 1 Gbps. o 1 tarjeta de red integrada con 1 puerto de 1 Gbps. • Fuentes de poder: 2 unidades de 800 W. • Accesorios: Rieles para montaje en rack.	
Especificaciones Técnicas del Servidor • Almacenamiento: 2 discos duros SAS de 300 GB a 10K. • Procesador: CPU con 10 núcleos y una frecuencia base de 2.20 GHz. • Memoria RAM: 288 GB. • Tarjeta de almacenamiento: Tarjeta PCI con 2 puertos FC y 2 transeiver de 16 Gbps. • Tarjetas de red: o 1 tarjeta PCI con un puerto de red de 1 Gbps. o 1 puerto de red integrado de 1 Gbps. • Fuentes de poder: 2 unidades de 800 W. • Accesorios: Rieles para montaje en rack.	1
Especificaciones Técnicas del Sistema de Almacenamiento • Capacidad de almacenamiento: 20 TB efectivos. • Unidades de disco: Discos SAS de 2.4 TB, 12 Gbps, 10K, SFF con tecnología 512e compatible MSA 2040 8GB Fiber Channel SW FC SFP+tarjetas HBA fiberchannel storage 8gb (dual port) • Conectividad de almacenamiento: o Adaptadores de canal de fibra de 8 Gbps para conexión al almacenamiento. o Tarjetas HBA de canal de fibra de 8 Gbps con puertos duales para servidores.	
NAS Backup hasta 80 TB usables. Incluye Windows Storage	
Monitoreo 7X24	
Servicios de instalación, configuración e integración a la infraestructura tecnológica y de comunicaciones del Instituto, así como la configuración de la plataforma en ALTA DISPONIBILIDAD.	
Se debe garantizar la interconexión entre los dispositivos ofertados.	

La infraestructura deberá mantenerse operativa bajo estas especificaciones hasta que la migración sea completada en su totalidad, validada y puesta en producción, garantizando la integridad de la información, la continuidad transaccional y la disponibilidad de los servicios críticos durante la transición tecnológica.

El contratista entrante deberá asegurar la continuidad del servicio y la disponibilidad operativa de los equipos durante la transición. Para ello, coordinará con el contratista saliente las actividades técnicas indispensables para la entrega, migración y puesta en funcionamiento de la infraestructura tecnológica, tales como cronogramas, inventarios, acceso a información y procedimientos de transición.

Sin embargo, el contratista entrante deberá garantizar la continuidad de los servicios utilizando su propia infraestructura, sin depender del hardware del contratista saliente.

Esta coordinación será exclusivamente de carácter técnico y operativo, sin que implique transferencias económicas, pagos, reconocimientos de valor o subordinación contractual entre los contratistas. Cada parte responderá directamente ante la Entidad dentro del ámbito de sus obligaciones contractuales.

Es importante tener en cuenta que la administración del sistema operativo es de exclusiva responsabilidad de INFICALDAS, gestionándolo mediante licenciamiento dentro del esquema provisto por el proveedor de servicios en la nube, de acuerdo con el modelo IaaS. En este contexto, los terceros contratados únicamente se limitan a entregar la aplicación correspondiente o a proporcionar soporte funcional sobre un sistema operativo previamente definido y administrado por el Instituto.

Estado de los Aplicativos y Coordinación para Migración a IaaS

- El aplicativo WorkManager se encuentra alojado bajo un modelo On-Premise, mientras que los aplicativos ERP IAS y SIICO operan en nube.
- La transición hacia el modelo de Infrastructure as a Service (IaaS) se refiere únicamente a la migración del ambiente productivo de la Entidad. La coordinación con los proveedores de terceros se limita a actividades técnicas necesarias para garantizar la compatibilidad, ajustar conexiones y planificar ventanas de mantenimiento, sin que ello implique que el contratista gestione o modifique las aplicaciones de terceros.
- Los proveedores actuales de los aplicativos ERP IAS, SIICO y WorkManager, responsables del mantenimiento y operación de sus respectivas aplicaciones, garantizarán la continuidad de los servicios, la integridad de los datos corporativos y la disponibilidad de los módulos transaccionales durante la migración. Estas actividades se coordinarán con el contratista encargado de la infraestructura IaaS, quien realizará únicamente las tareas relacionadas con la migración del ambiente productivo de la Entidad, sin intervenir en la operación o gestión de las aplicaciones de terceros.

Este esquema asegura que la migración se realice de manera controlada, preservando la integridad, disponibilidad y continuidad de los sistemas de la Entidad, sin afectar las operaciones de los aplicativos provistos por terceros. INFICALDAS cuenta con SLA vigentes con los proveedores de ERP IAS, SIICO y WorkManager. La coordinación técnica para la transición hacia IaaS se realizará con mediación de INFICALDAS, garantizando la continuidad operativa, aunque el cumplimiento del cronograma dependerá de la disponibilidad de estos terceros, fuera del control directo del contratista.

Infraestructura en la Nube – Almacenamiento Complementario (S3 Glacier) y Seguridad

- El almacenamiento tipo S3 Glacier (14,3 TB) se realizará dentro de la nube privada gestionada por el proveedor, integrado en la misma consola de administración, asegurando seguridad, control y trazabilidad de los datos, en cumplimiento de las políticas institucionales.
- Para cumplir con las políticas de seguridad de la información institucional y las mejores prácticas internacionales, se requiere cifrado en reposo (Encryption at Rest) para todo el almacenamiento, además del cifrado en tránsito (TLS con AES-256) exigido en el pliego.
- El cifrado en reposo protege los datos frente a accesos no autorizados, incidentes internos o físicos, y debe implementarse con algoritmos robustos (preferiblemente AES-256), gestionando adecuadamente las claves de cifrado bajo estrictos controles de acceso y auditoría, ya sea por INFICALDAS o por el contratista.

Requisitos de Conectividad y Desempeño para Aplicaciones en la Nube

Para garantizar una adecuada experiencia de usuario en las aplicaciones críticas (ERP, SIICO) alojadas en la nube privada, se establecen como parámetros de referencia los siguientes:

- Ancho de banda mínimo requerido: 50 Mbps simétricos.
- Latencia máxima aceptable: entre 30 y 50 ms entre la red local de INFICALDAS y el punto de acceso a la nube privada.

Estos parámetros permiten asegurar un rendimiento óptimo, disponibilidad y continuidad operativa, garantizando que las aplicaciones críticas funcionen sin degradación perceptible para los usuarios finales.

Por último, es importante tener en cuenta que la infraestructura objeto del presente proceso corresponde en su totalidad a ambientes productivos, que soportan los sistemas institucionales críticos de la Entidad. El proceso no incluye ambientes de desarrollo, pruebas o contingencia distintos a los productivos, ni su evaluación o migración, por lo cual el dimensionamiento de la solución en la nube se ha realizado considerando exclusivamente la operación productiva.

Durante la vigencia 2025, INFICALDAS operó bajo un esquema de arrendamiento de infraestructura física en sitio, compuesto por servidores, almacenamiento SAN/NAS y demás equipos instalados directamente en el datacenter de la entidad. Este modelo implicaba la administración, soporte y mantenimiento local de todo el hardware, así como la gestión de los recursos de procesamiento, memoria y almacenamiento desde la infraestructura física provista por el contratista.

Para el año 2026, la entidad realiza una transición tecnológica hacia un modelo de Infraestructura como Servicio (IaaS) en nube privada, en el cual los recursos tecnológicos vCPU, memoria RAM, almacenamiento, firewall virtual, backups y licenciamiento ya no se encuentran alojados físicamente dentro de INFICALDAS, sino provisionados, gestionados y operados directamente desde la plataforma cloud del proveedor. Esto permite contar con una infraestructura más flexible, escalable, segura y con menores dependencias operativas frente al hardware local.

En este nuevo escenario, es importante precisar que para la vigencia 2026 no debe incluirse ningún componente de infraestructura física en sitio. Es decir, no se requieren servidores, cabinas de almacenamiento, equipos SAN/NAS ni dispositivos instalados en el datacenter de INFICALDAS, como sí ocurrió en 2025. De igual manera, no se contemplan actividades asociadas a instalación, montaje, soporte o mantenimiento de hardware local. Toda la capacidad tecnológica requerida debe ser suministrada exclusivamente desde la nube del proveedor, mediante un servicio virtualizado, centralizado y administrado bajo el esquema IaaS.

En síntesis, mientras 2025 correspondió a un modelo de infraestructura física instalada dentro de la entidad, la vigencia 2026 adopta completamente una infraestructura alojada en la nube, eliminando la necesidad de equipos en sitio y fortaleciendo la continuidad y disponibilidad de los servicios institucionales.

1. DRAAS EN NUBE.

Conforme al análisis previo realizado, el objeto del contrato se ejecutará atendiendo las siguientes especificaciones técnicas y operativas, orientadas a garantizar la continuidad del negocio, la disponibilidad de los sistemas de información y la recuperación ante desastres mediante infraestructura en la nube:

2.1. Infraestructura de Nube para DRaaS (Disaster Recovery as a Service)

El proveedor deberá suministrar una plataforma de recuperación ante desastres en la nube (DRaaS), con capacidad dedicada para alojar y ejecutar los servicios críticos del Instituto en caso de contingencia, con las siguientes características mínimas:

- 56 vCPU de procesamiento garantizado.
- 148 GB de memoria RAM.
- 14.110 GB de almacenamiento en disco.
- 1 dirección IP pública.
- Instalación y configuración completa de la solución DRaaS
- Ancho de banda sin limitaciones para transferencia de datos
- Transferencia de conocimiento al equipo del cliente para la correcta operación y
- gestión del servicio.

2.2. Servidores críticos para replicar en la nube

Adicionalmente, deberá existir una máquina en la nube operando de manera permanente como controlador de dominio adicional, para garantizar autenticación, federación y continuidad de políticas de seguridad.

2.3. Replicación, respaldo y almacenamiento en la nube

El proveedor deberá implementar y administrar un esquema de replicación continua (near real-time), sincronización y restauración basado en Veeam Cloud Connect o tecnología equivalente.

El servicio incluirá:

- Almacenamiento en nube para réplicas y ejecutables.
- Repositorios de respaldo en AWS S3 Glacier Instant Retrieval para bases de datos del ERP IAS, SIICO y WorkManager.
- Pruebas ilimitadas de failover y failback sin afectar la operación productiva.
- Restauración granular y por máquina virtual, según se requiera.

2.4. Sitio alterno físico para continuidad operativa

El proveedor deberá garantizar un centro alterno de operación (sala de crisis) ubicado a más de 150 km del datacenter principal, con:

- Hasta 10 puestos de trabajo con equipos portátiles y software licenciado.
- Conectividad redundante y acceso seguro a los sistemas activados en la nube.
- Un (1) despacho de gerencia y una sala de juntas.
- Cinco (5) parqueaderos.
- Disponibilidad del espacio por 15 días hábiles en caso de contingencia.

2.5. Servicios profesionales incluidos

El proveedor deberá suministrar como mínimo:

- Diseño de la arquitectura de recuperación ante desastres.
- Implementación completa del entorno DRaaS en la nube.
- Configuración de replicación, políticas de retención y recuperación.
- Puesta en marcha de las máquinas virtuales en el entorno alterno.
- Administración, monitoreo y soporte 7x24.
- Mesa de servicio basada en mejores prácticas ITIL y ubicada en cuadrante Gartner.
- Entrega mensual de informes de incidentes, actividades de respaldo y estado de réplicas.
- Ejercicios de simulación de contingencia para los funcionarios del Instituto.
- Elaboración de instructivos y cartillas de operación ante incidentes.
- Bolsa de 50 horas de ingeniería para requerimientos adicionales de soporte específicamente para actividades relacionadas con la puesta en marcha del plan de continuidad del Instituto.
- 720 horas disponibles al año para encendido de VMs, en caso de pruebas y ejecución de failover.
- Pruebas de Failover

2.6. Certificaciones y capacidad técnica del proveedor

El proveedor deberá contar con personal certificado y acreditado en:

- Veeam Backup & Replication y/o Veeam Data Platform
- VMware
- Microsoft Windows Server
- Infraestructura HPE (ProLiant, SimpliVity, almacenamiento)
- Certificación como Veeam Cloud Service Provider (VCSP)
- Acreditación como HPE Partner Silver
- Certificación de seguridad y calidad del Datacenter (Tier IV o equivalente)
- VCSP Silver
- VASP (Veeam Accredited Service Partner)
- Certificaciones VMCE y VMCA

La infraestructura tecnológica de INFICALDAS está siendo proyectada hacia un modelo operativo basado en la nube, el cual soportará los servicios críticos institucionales. Sin embargo, en cumplimiento de las buenas prácticas de continuidad del negocio y de las exigencias de la Superintendencia Financiera, la infraestructura destinada para la operación diaria no puede ser la misma que se utilice como sitio de recuperación ante desastres (DRP).

Por tal razón, se requiere contar con una infraestructura secundaria en la nube, independiente y técnicamente diferenciada de la plataforma principal**,** que permita replicar los servicios esenciales y garantizar su disponibilidad en caso de fallas, interrupciones del proveedor, incidentes de seguridad, indisponibilidad regional o cualquier evento de contingencia que afecte la operación normal del Instituto, esta condición será verificada de manera permanente por parte del supervisor del contrato.

Esta separación arquitectónica es indispensable para asegurar que, aun cuando la infraestructura principal se vea comprometida, INFICALDAS pueda activar su entorno de recuperación y restablecer los servicios críticos de manera oportuna, minimizando el impacto operativo y cumpliendo con los lineamientos del Plan de Continuidad del Negocio, el DRP institucional y las directrices de gestión del riesgo tecnológico.

El licenciamiento requerido para la operación diaria de los sistemas críticos será administrado por la Entidad.

En el escenario de DRaaS, la replicación de los servicios críticos se realizará en una infraestructura secundaria en la nube, independiente de la plataforma principal, gestionada por el proveedor de DRaaS.

El proveedor será responsable de garantizar que todos los servicios críticos cuenten con las licencias necesarias para su funcionamiento en el entorno de recuperación ante desastres, asegurando la continuidad operativa, la disponibilidad de los sistemas y el cumplimiento de las normas y políticas aplicables, mientras que la Entidad supervisará y verificará permanentemente el correcto funcionamiento del DRaaS.

3. Licenciamiento, suministros tecnológicos y soporte integral de infraestructura.

3.1. Renovación correo electrónico y ofimática Microsoft Office 365, servicio de soporte y Licencias de Power Bi Microsoft

Renovación de los servicios de correo electrónico de solo buzón y de las cuentas de correo electrónico con ofimática Microsoft Office 365 para los equipos de propiedad del Instituto, así como la contratación de los servicios de configuración, capacitación y definición de políticas de seguridad, y la adquisición de licencias Microsoft Power BI Pro. El licenciamiento deberá contar con las siguientes características:

ITEM	DESCRIPCIÓN	CANT
1	Microsoft 365 Business Basic - Solo buzón de correo – Suscripción 1 año	63
2	Licencias Microsoft 365 Business Standard Incluye: Aplicaciones de Office: Word, Excel, PowerPoint, Publisher, Outlook Servicios: Exchange, Sharepoint, Teams, 1 Tera OneDrive]CSP- Cloud Solution Provider Suscripción 1 año	60
3	Licencias de Power Bi Microsoft	5
4	Power Automate Premium (NCE COM ANN)	1
5	Project Plan 3 (NCE COM ANN)	1
6	MICROSOFT COPILOT FOR MICROSOFT 365 (NCE COM ANN)	10
7	Licencia de Power Apps Premium (NCE COM ANN	1
8	Licenciamiento Fabric, F2, 2 unidades de capacidad x 730 Horas, Almacenamiento de OneLake **3 GB**	1
9	Servicios de configuración capacitación políticas de seguridad **Microsoft Exchange Online:** - Configuración de Alias (usuarios) - Sincronización de calendarios Outlook – Exchange Online. - Delegación de buzones, reenvío y administración. - Configuración de otros dominios sobre la plataforma Office365.	1

	Microsoft Outlook: - Capacitación y uso de la herramienta. - Reglas y políticas de uso de carpetas en Outlook.	
10	Azure Aplicación Pachito Suscripción Anual y Azure Services Suscripción Anual	1
11	ArcGIS Online Credits; Block of 1,000	2
12	ArcGIS Online Professional (formerly Standard) User Type Annual Subscription	1
13	ArcGIS Online Viewer User Type Annual Subscription	1

El Instituto responsable de la administración y gestión del licenciamiento de los sistemas y aplicaciones contratadas, adquiriendo las licencias a través de los proveedores autorizados según corresponda:

- Microsoft (Windows Server, Microsoft 365, Power BI, Copilot, Power Apps, etc.) mediante CSP – Cloud Solution Provider.
- VMware, Veeam, Fortinet, ESET, Cisco, a través de contratos y suscripciones vigentes.
- Servicios en la nube bajo modalidad Pay As You Go, cuando aplique.

Bajo este esquema, la Entidad mantiene la administración, configuración y uso de las licencias, garantizando así la legalidad, continuidad operativa y soporte técnico de los sistemas y servicios implementados, mientras que los proveedores suministran las licencias y servicios contratados.

3.2. Bolsa de suministro de elementos de informática

Los elementos de informática que se relacionan a continuación se toman como referencia, pero no son taxativos ni limitantes, en caso de la entidad requerir elementos similares a los descritos, estos elementos se estiman como frecuentes y solo se descuente el valor máximo permitido para el uso de esta:

ITEM	DESCRIPCION	CAN
1	MONITOR DE 21" CON PUERTO HDMI RESOLUCIÓN FULL HD (1920 X 1080) FRECUENCIA DE ACTUALIZACIÓN DE AL MENOS 75 Hz	1 Un
2	SOPORTE GENIUS PORTATIL ALIMINIO GStand M250	1 Un
3	DISCO SÓLIDO SSD PARA PORTÁTIL (512 GB) - DISCO SÓLIDO M.2 NVMe PCIe 3.0 512 GB	1 Un
4	ADAPTADOR WI-FI USB	1 Un
5	COMBO TECLADO Y MOUSE INALAMBRICO	1 Un n
6	KIT DE HERRAMIENTAS PARA MANTENIMIENTO Y REPARACION DE COMPUTADORES	1 Un
7	PAD MOUSE PLANO	1 Un
8	PAD TECLADO ERGONOMICO	1 Un
9	MEMORIA RAM DDR5 – MEMORIA DDR5 SO-DIMM 5200MHz 16GB/32GB	1 Un
10	JABRA SPEAKER	1 Un
11	DIADEMAS CON MICROFONO BLUETOOTH O USB	1 Un
12	CABLE HDMI 1.5 MTS Cable HDMI 1.5M MACHO A 1.8M MACHO A HDMI MACHO 14+1 28AWG	1 Un
13	CABLE HDMI 5 MTS	1 Un

14	CABLE PATCHCORD CATEGORIA 6 3 MTS Cable Patchcord UTP Cat6 1Mts 26AWG 8X8 PVC Blanca	1 Un
15	SWITCH HDMI	1 Un
16	CABLE PATCHCORD CATEGORIA 6 5 MTS Cable Patchcord UTP Cat6 5Mts 26AWG 8X8 PVC Blanca	1 Un
17	CONVERTIDOR HDMI A VGA	1 Un
18	DISCO DURO EXTERNO 4TB – DISCO DURO EXTERNO USB 3.0 3.5" 4TB	1 Un
19	BRAZO PARA MONITOR/PANTALLA	1 Un
20	MEMORIA USB 16GB	1 Un
21	MEMORIA USB 32GB	1 Un
22	MEMORIA USB 64GB	1 Un
23	ADAPTADOR USB-C Digital AV Multiport Adapter (USB-C HDMI USB)	**1**
24	HUB DE RED 8 PUERTOS	**1**
25	KIT DE LIMPIEZA PC - CLEAN ESPUMOSO, LIMPIADOR ELECTRONICO	**3.2.1.1**

Nota: Se aclara que el ítem 3.2 se establece como monto agotable dentro del futuro contrato a suscribirse, por un valor de VEINTIDÓS MILLONES SEISCIENTOS DIEZ MIL PESOS M/CTE ($22.610.000), suma que incluye la totalidad de los impuestos, tasas, contribuciones y demás gravámenes a que haya lugar.

3.3. Renovación licenciamiento Cisco Umbrella protección para teletrabajadores (usuarios remotos)

El Instituto requiere renovar el siguiente licenciamiento:

ITEM	DESCRIPCIÓN	CANT
1	Cisco Umbrella DNS Security Essentials	54
2	Enhanced Support for Umbrella	1
3	Servicios configuración portal Umbrella	1

3.4. Adquisición de licenciamiento Cisco Duo-Sistema de autenticación de múltiple factor

Las licencias para adquirir deben tener las siguientes características:

DESCRIPCIÓN	CANT
DUO-MFA - Standard Cisco Duo MFA edition 1Y debe incluir / DUO-SUB - Cisco Duo subscription y SVS-DUO-SUP-B - Cisco Duo Basic Support	60
Servicios de configuración de licenciamiento	1

3.5. Renovación Firewall Fortinet

Las características requeridas son las siguientes:

ITEM	DESCRIPCIÓN	CANT
1	Licencia FEVMCLM000236846 (Coterm End Date:2025-12-04)(Last Expiry Date:2025-04-18) - FG100FTK23014870 (Coterm End Date:2025-12-04)(Last Expiry Date:2024-12-04) - (Quote ID 5639125-1)	1
2	FortiMail Cloud - Gateway Premium with Office365 1 Year FortiMail Cloud - Gateway Premium w. Cloud Email API support for Microsoft 365 or Google (25-100 mailboxes)	50
	Servicios de configuración e instalación en 50 dispositivos de cómputo en FortiMail Cloud, parametrización, puesta en marcha, capacitación y documentación	

3		1

El licenciamiento deberá renovarse por un período de un (1) año, cubriendo todos los servicios asociados descritos en las características técnicas, tales como soporte, actualizaciones y mantenimiento, según las condiciones establecidas en el contrato.

3.6. Adquisición licenciamiento VEEM BACKUP.

Se requiere continuar con el servicio de cobertura para garantizar la virtualización de las soluciones y plataformas institucionales; de igual forma es necesario realizar el proceso de renovación de estas licencias, las cuales debe cumplir con las siguientes características:

DESCRIPCIÓN	CANT
Renovación de licenciamiento de VEEAM BACKUP & Replication Universal Editio features. 10 Instance pack – 1 year	1
Veeam Backup for Microsoft 365. 1 Year Subscription Upfront Billing & Production (24/7) Support	60
Servicios de configuración y soporte Veeam Backup	1

3.7. Renovación Antivirus

Con el propósito de asegurar la protección integral de los equipos de cómputo, servidores y dispositivos corporativos frente a amenazas informáticas, se requiere la renovación del licenciamiento de la solución antivirus empresarial. Esta renovación permite mantener operativas las funcionalidades de prevención, detección y respuesta ante incidentes, así como garantizar la correcta ejecución de las actividades de configuración, actualización, monitoreo y afinamiento necesarias para preservar la seguridad, disponibilidad y rendimiento de la infraestructura tecnológica institucional.

La solución contempla, entre otros, los siguientes componentes:

- Consola centralizada de administración
- Protección avanzada para endpoints
- Seguridad para servidores y cargas críticas
- Defensa ante amenazas en dispositivos móviles
- Protección contra amenazas avanzadas y de día cero
- Cifrado de disco completo para dispositivos corporativos

ITEM	DESCRIPCIÓN	CANT
1	Renovación Antivirus ESET Protect Advanced Suscripcion 1 año - Edxcluido de IVA	80
4	Servicios Profesionales Incluye: Actualizacion de Antivirus Configuracion y despliegue Afinamiento de consola Actividades remotas	1

Condiciones de Ciberseguridad

A continuación, se enfatiza la necesidad de garantizar la seguridad, integridad y confidencialidad de la información institucional, en cumplimiento de los lineamientos de la Superintendencia Financiera y la normativa vigente. Se destacan los siguientes puntos:

Migración a la nube privada: Se justifica como una estrategia para fortalecer el control sobre la información sensible, permitiendo la implementación de políticas de acceso, firewall virtual, VPN, cifrado y monitoreo continuo.

Gestión de desastres y continuidad del negocio: Se requiere una infraestructura que garantice alta disponibilidad, redundancia y respaldo, con múltiples puntos de retención inmutables y recuperación rápida ante incidentes.

Cumplimiento normativo: Se mencionan controles exigidos por la Superintendencia Financiera, como la adopción de políticas y mecanismos para evitar la fuga de datos, gestión de la seguridad de la plataforma tecnológica, identificación y mitigación de riesgos cibernéticos, y la incorporación de herramientas como SIEM para la correlación de eventos de seguridad.

Seguridad en la Infraestructura y Servicios

La arquitectura tecnológica propuesta incluye medidas específicas para proteger los sistemas y servicios críticos:

Firewall virtual y protección perimetral: Se exige la renovación y configuración de soluciones como FortiGate 100F y FortiMail Cloud, que soportan la carga operativa, ofrecen detección avanzada de amenazas y refuerzan la seguridad del correo electrónico, un vector crítico de ataque.

Autenticación multifactor (MFA): La adquisición y renovación de licencias Cisco Duo responde a la obligatoriedad de implementar controles robustos de autenticación, exigidos por la Superintendencia Financiera y las pólizas de seguro Cyber, para mitigar riesgos de acceso no autorizado y suplantación de identidad.

Protección para usuarios remotos: La renovación de Cisco Umbrella garantiza la protección basada en DNS para usuarios fuera de las instalaciones, visibilidad y control centralizado del tráfico, y mitigación de ataques de navegación insegura.

Respaldo, Recuperación y Continuidad Operativa

DRaaS (Disaster Recovery as a Service): Se requiere una solución robusta que permita la réplica continua de máquinas virtuales, aprovisionamiento de recursos dedicados, pruebas de failover/failback y almacenamiento seguro en AWS Glacier, asegurando la recuperación funcional del entorno tecnológico completo en caso de contingencia.

Veeam Backup: La renovación de esta plataforma es esencial para garantizar backups en nube y cinta, recuperación rápida, protección integral de datos y cumplimiento del DRP institucional.

Políticas y Gobierno de TI

Políticas generales: Se establecen políticas de infraestructura escalable, redundancia y continuidad operativa, y uso eficiente de los recursos, orientadas a asegurar la seguridad y disponibilidad de los servicios tecnológicos.

Gestión y monitoreo: Se exige monitoreo activo 24/7, administración avanzada de seguridad, gestión de incidentes y cumplimiento de niveles de servicio (SLA/ANS).

Seguridad en Endpoints y Dispositivos

Antivirus avanzado basado en la nube: Se requiere una solución que incorpore protección avanzada para endpoints, servidores y dispositivos móviles, cifrado de disco completo, defensa contra amenazas de día cero y sandboxing en la nube.

Obligaciones del Contratista en Seguridad

El contratista debe implementar y mantener todas las medidas de seguridad descritas, garantizar la continuidad operativa, administrar licencias y respaldos, y cumplir con los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) de INFICALDAS y la Superintendencia Financiera.

ESTUDIO PREVIO

OBLIGACIONES DEL CONTRATISTA:

Conforme las especificaciones anteriores el contratista se obliga a:

1. Implementar la infraestructura tecnológica principal en la nube, asegurando su disponibilidad, estabilidad y capacidad conforme a los requerimientos institucionales.
2. Implementar la plataforma de Recuperación ante Desastres (DRaaS) como infraestructura independiente y secundaria, destinada a la continuidad operativa.
3. Configurar los recursos en la nube (v CPU, RAM, almacenamiento, redes, IP pública y demás componentes) conforme a lo ofertado y a las necesidades del Instituto.
4. Integrar la infraestructura local del Instituto con la infraestructura en la nube mediante esquemas seguros de comunicación (VPN SSL o equivalentes).
5. Configurar y mantener mecanismos de replicación continua, políticas de retención, respaldo y sincronización, garantizando compatibilidad con Veeam Backup.
6. Administrar, monitorear y mantener operativa la plataforma DRaaS durante toda la vigencia contractual.
7. Realizar monitoreo permanente 7x24 de réplicas, respaldos, conectividad, uso de recursos, alertas e incidentes que afecten la infraestructura.
8. El proveedor deberá gestionar las plataformas de almacenamiento de largo plazo (como AWS S3 Glacier), garantizando la integridad, disponibilidad y trazabilidad de la información de los sistemas ERP, SIICO, WorkManager y demás sistemas institucionales.

   La administración de la infraestructura tecnológica, incluyendo backup, restauración, DRP y licencias correspondientes, será responsabilidad del proveedor.

   Sin embargo, la administración de los sistemas de información y de las bases de datos continuará siendo responsabilidad de INFICALDAS, quien garantizará acceso directo y oportuno, disponibilidad y control de la información para la validación periódica de la integridad de los datos en un ambiente de pruebas.

9. Mantener disponible la infraestructura para pruebas y activación (failover) por hasta 720 horas anuales.
10. Ejecutar pruebas de failover y failback conforme el cronograma aprobado por el Instituto, sin afectar la operación productiva.
11. Realizar pruebas de restauración total o parcial de información con periodicidad trimestral o según requerimientos institucionales.
12. Brindar soporte técnico especializado para la activación del sitio alterno cuando se requiera.
13. Garantizar la disponibilidad operativa del controlador de dominio alterno alojado en la nube.
14. Garantizar la continuidad, estabilidad y desempeño de todos los servicios, plataformas y componentes alojados en la nube.
29. Suministrar, activar, administrar y mantener vigentes las licencias necesarias para la operación institucional.
30. Garantizar la integración técnica de todas las licencias con la infraestructura institucional.
30. Mantener todas las plataformas licenciadas funcionando de manera continua, estable y actualizada durante toda la vigencia contractual.
31. Realizar seguimiento a fechas de expiración, renovaciones y continuidad operativa de los servicios licenciados.
32. Suministrar, mediante la modalidad de bolsa, los repuestos, partes, componentes y elementos tecnológicos requeridos para garantizar el funcionamiento de los equipos institucionales.
33. Realizar la instalación, configuración y puesta en marcha de los elementos suministrados, asegurando su pleno funcionamiento.
34. Garantizar disponibilidad permanente de partes críticas o de alto impacto para la operación institucional.
35. Una vez suscrito el contrato, el contratista deberá designar un responsable técnico principal con formación profesional en Ingeniería de Sistemas o carreras afines**,** y con experiencia acreditada en administración de infraestructura tecnológica, servicios en la nube y/o recuperación ante desastres**.**

Este profesional será el encargado de liderar la ejecución técnica del contrato y coordinar las actividades del equipo interdisciplinario asignado por el contratista.

El contratista deberá garantizar la disponibilidad del responsable técnico principal para la atención y coordinación de las actividades técnicas requeridas para la ejecución del contrato, incluyendo presencia en las instalaciones de INFICALDAS cuando las necesidades del servicio así lo requieran**,** dentro del horario institucional, sin que ello implique dedicación exclusiva, permanencia continua ni vínculo laboral alguno con la Entidad**.**

36. Contar con un equipo interdisciplinario con capacidades en:

- Administración de servidores y servicios corporativos (AD, DNS, DHCP).
- Redes, seguridad perimetral y comunicaciones.
- Virtualización y almacenamiento.
- Respaldo, recuperación y servicios en la nube.
- Análisis forense, respuesta y contención de incidentes.

38. Brindar soporte técnico especializado 7x24 para incidentes críticos que afecten la disponibilidad, integridad o confidencialidad de la información institucional.
39. Atender incidentes, alertas y fallas dentro de los niveles de servicio establecidos por INFICALDAS.
40. Utilizar una mesa de servicio alineada con prácticas ITIL y ubicada en cuadrante Gartner, presentando reportes mensuales de atención.
41. Entregar informes periódicos que incluyan, como mínimo:

- Estado de réplicas
- Estado de respaldos
- Actividades de soporte
- Incidentes atendidos
- Pruebas de failover/failback
- Estado del almacenamiento en la nube

43. Garantizar la disponibilidad del sitio alterno físico conforme a las condiciones ofertadas, incluyendo puestos de trabajo, conectividad y equipos mínimos requeridos.
44. Facilitar el acceso y operación del personal del Instituto en escenarios de contingencia.
45. Mantener vigentes las certificaciones del datacenter utilizado (Tier IV o equivalente).
46. Garantizar la seguridad física y lógica de todos los componentes, plataformas y servicios entregados.
47. Adoptar controles, protocolos y medidas que aseguren el cumplimiento normativo aplicable a seguridad digital, protección de datos y continuidad del negocio.
48. El contratista deberá contar con un equipo profesional con experiencia comprobable en migraciones de infraestructura tecnológica desde entornos On-Premise hacia la nube, con competencias en planificación, operación, seguridad y aseguramiento de la continuidad operativa.
49. El contratista deberá planificar y coordinar la migración de la infraestructura tecnológica con el contratista saliente, incluyendo cronogramas, inventarios, procedimientos de transición y acceso a la información necesaria, garantizando que la entrega de la infraestructura se realice de manera ordenada y sin afectar la disponibilidad de los servicios.
50. El contratista será responsable de la ejecución de todas las actividades técnicas necesarias para la migración, incluyendo pruebas, validación de sistemas y puesta en funcionamiento de la infraestructura tecnológica en la nube.
51. El contratista deberá garantizar que la migración cumpla con los estándares de seguridad, protección de la información y normativas aplicables, implementando las medidas necesarias para mitigar riesgos durante el proceso.
52. El equipo destinado para la labor de migración de la infraestructura deberá estar en capacidad de realizar actividades presenciales en sitio cuando sea necesario para la correcta ejecución de la migración.

53. El contratista deberá llevar a cabo todas las acciones de coordinación técnica necesarias con el contratista saliente y demás actores involucrados, que permitan garantizar la correcta migración y funcionamiento de la infraestructura tecnológica.

OBLIGACIONES GENERALES:

1. Cumplir el objeto contractual en los términos, condiciones y especificaciones definidas por INFICALDAS.
2. Presentar los informes requeridos para pagos, seguimiento y control contractual, así como aquellos que solicite el supervisor.
3. Mantener, durante toda la ejecución, la organización técnica y administrativa ofrecida, garantizando altos niveles de calidad, eficiencia técnica y profesional.
4. Ejecutar las actividades previstas en el objeto contractual y en la propuesta presentada, la cual hace parte integral del contrato.
5. Contar con la capacidad y disponibilidad necesarias para atender oportunamente incidentes y requerimientos surgidos durante la ejecución del contrato.
6. Disponer permanentemente de los recursos humanos, técnicos, logísticos y financieros necesarios para la correcta ejecución del contrato.
7. Asumir los pagos de salarios, prestaciones sociales, aportes e indemnizaciones del personal asignado, sin generar vínculo laboral alguno con INFICALDAS.
8. Pagar los impuestos, tasas y contribuciones derivados del contrato.
9. Constituir y mantener vigente la garantía única de cumplimiento conforme a los términos definidos por el Instituto.
10. Guardar estricta confidencialidad y reserva sobre la información institucional.
11. Suministrar al supervisor toda documentación e información necesaria para el ejercicio de sus funciones.
12. Suscribir las actas de inicio, suspensión, reinicio y liquidación, cuando aplique.
13. Acatar las instrucciones impartidas por el supervisor del contrato.
14. Cumplir todas las demás obligaciones relacionadas con el objeto contractual y las que determine INFICALDAS para garantizar su adecuada ejecución profesional.
15. Cumplir con los lineamientos, políticas, procedimientos y controles del Sistema de Gestión de Seguridad de la Información SGSI de INFICALDAS, así como con las disposiciones de la Superintendencia Financiera de Colombia, garantizando la protección, integridad, disponibilidad y confidencialidad de la información institucional y del tratamiento de datos personales durante toda la ejecución del contrato.

PLAZO DE EJECUCIÓN DEL CONTRATO:

Desde el cumplimiento de los requisitos de perfeccionamiento y ejecución contractual y hasta el 31 de diciembre de 2026 mediando suscripción de la correspondiente acta de inicio.

Numeral 3 del Artículo 2.2.1.1.2.1.1: *"La modalidad de selección del contratista y su justificación, incluyendo los fundamentos jurídicos"*.

En lo que respecta a la licitación pública, modalidad que constituye la regla general para la selección de contratistas, el artículo 30 de la Ley 80 de 1993 establece sus etapas. De esta disposición se distinguen dos momentos:

i) La fase de planeación o etapa preparatoria, en la cual la entidad debe elaborar los estudios previos que justifican técnica y jurídicamente la contratación, conforme a lo señalado en el numeral 12 del artículo 25 de la Ley 80 de 1993 y en el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015; y
ii) El inicio formal del proceso de licitación pública, mediante el acto de apertura.
Adicionalmente, el numeral 2 del artículo 30 de la Ley 80 de 1993 impone la obligación de elaborar el pliego de condiciones, en los términos previstos en el numeral 5 del artículo 24 de la misma ley y en el artículo 2.2.1.1.2.1.3 del Decreto 1082 de 2015.

La licitación pública es la modalidad que mejores garantías ofrece respecto de los principios de la función administrativa, tales como imparcialidad, selección objetiva, transparencia y participación. No obstante, la doctrina y la jurisprudencia han señalado que este procedimiento no está exento de críticas, pues su etapa procedimental puede ser extensa, lo que en ocasiones afecta el interés público o la obtención de ofertas oportunas para la Administración.

ESTUDIO PREVIO

Por su parte, el artículo 2 de la Ley 1150 de 2007, numeral 1, reafirma que la licitación pública es la modalidad general de selección, salvo las excepciones previstas en los numerales 2, 3, 4 y 5 del mismo artículo. El parágrafo del artículo 30 de la Ley 80 de 1993 la define como:

"El procedimiento mediante el cual la entidad formula públicamente una convocatoria para que, en igualdad de oportunidades, los interesados presenten sus ofertas y seleccione entre ellas la más favorable".

El Consejo de Estado ha precisado que esta definición debe entenderse como:

"[...] un procedimiento administrativo conformado por una serie de actuaciones articuladas entre sí, provenientes tanto de la Administración como de los oferentes, todas de público conocimiento, con el fin de seleccionar, en condiciones de igualdad, la propuesta más favorable al interés general".

De igual manera, ha sido considerada como un procedimiento administrativo preparatorio de la voluntad contractual, cuya finalidad es escoger al contratista idóneo que ofrezca las mejores condiciones para la entidad, dentro del marco legal y formalidades previstas para proteger la legitimidad de la contratación estatal.

Los aspectos operativos de este proceso han sido reglamentados por el Decreto 1510 de 2013, posteriormente compilado en el Decreto 1082 de 2015.

En cuanto a la clasificación doctrinal, las modalidades de selección pueden agruparse en: i) competitivas, y ii) no competitivas.

La licitación pública se ubica dentro de las modalidades competitivas y abiertas, pues permite la participación de múltiples proponentes bajo reglas uniformes, garantizando rivalidad efectiva y contribuyendo a mejores precios, calidad e innovación, según lo expuesto por Colombia Compra Eficiente en su *Guía de competencia en las compras públicas*.

En este procedimiento, cualquier interesado que cumpla con las condiciones de experiencia, capacidad técnica, financiera y demás requisitos del pliego puede presentar su propuesta. La entidad, por su parte, debe evaluar de manera objetiva todas las ofertas presentadas, publicar el informe de evaluación, permitir la presentación de observaciones y, finalmente, adoptar una decisión debidamente motivada sobre la adjudicación o, si es del caso, la declaratoria de desierta.

Finalmente, dado que el presupuesto oficial del presente proceso supera el valor límite establecido para la menor cuantía de la Entidad (hasta $364.000.000), la modalidad de selección aplicable es **Licitación Pública**, conforme a lo previsto en la Ley 80 de 1993 y la Ley 1150 de 2007.

Numeral 4 del Artículo 2.2.1.1.2.1.1: *"El valor estimado del contrato y la justificación de este"*.

Valor estimado del contrato: Conforme y en armonía con el estudio de mercado, la cuantía del contrato se estima en OCHOCIENTOS SESENTA Y SIETE MILLONES SETECIENTOS NOVENTA Y CUATRO MIL CUATROCIENTOS TREINTA Y SIETE PESOS M/CTE (867.794.437**)** incluido IVA según aplique, si a ello hubiera lugar, incluidos todos los impuestos, contribuciones, estampillas y la totalidad de costos directos e indirectos a que haya lugar. Mediante las cotizaciones y estudio del sector anexo se evidencia el análisis de precios que justifica la cuantía.

El presupuesto anteriormente referido, se encuentra discriminado de la siguiente manera:

ITEM DEFINIDO EN LAS ESPECIFICACIONES TECNICAS	ITEM	VALOR
1	INFRAESTRUCTURA COMO SERVICIO (IAAS)	$ 350.645.990
2	DRAAS EN NUBE.	$ 189.739.772
3	RENOVACIÓN DE LICENCIAMIENTO MICROSOFT 365, SERVICIO DE SOPORTE Y LICENCIAS ADICIONALES DE POWER BI, POWER APPS, PROJECT, POWER AUTOMATE, FABRIC Y COPILOT	$ 327.408.675

ESTUDIO PREVIO

TOTAL, PRESUPUESTO OFICIAL	$867.794.437

A continuación, se describen los componentes correspondientes al ítem número **3: *LICENCIAMIENTO, SUMINISTROS TECNOLÓGICOS Y SOPORTE INTEGRAL DE INFRAESTRUCTURA*,** los cuales deberán ser tenidos en cuenta por los proponentes en la estructuración de su oferta y que sirvieron como insumo para la Entidad en la determinación del presupuesto oficial del proceso.

ITEM DEFINIDO EN LAS ESPECIFICACIONES TÉCNICAS	DESCRIPCIÓN	VALOR UNITARIO
3.1	RENOVACIÓN CORREO ELECTRÓNICO Y OFIMÁTICA MICROSOFT OFFICE 365, SERVICIO DE SOPORTE Y LICENCIAS DE POWER BI MICROSOFT Y DEMÁS LICENCIAS QUE ACTUALMENTE TIENE EL INSTITUTO	$ 206.007.150
3.2	BOLSA DE SUMINISTRO DE ELEMENTOS DE INFORMATICA (MONTO AGOTABLE)	$ 22. 610.000
3.3	RENOVACIÓN LICENCIAMIENTO CISCO UMBRELLA PROTECCIÓN PARA TELETRABAJADORES (USUARIOS REMOTOS)	$12.922.400
3.4	ADQUISICIÓN DE LICENCIAMIENTO CISCO DUO-SISTEMA DE AUTENTIFICACIÓN DE MULTIPLE FACTOR	$14.768.300
3.5	ADQUISICIÓN FIREWALL FORTINET	$38.725.575
3.6	ADQUISICIÓN LICENCIAMIENTO VEEM BACKUP	$22.783.000
3.7	RENOVACIÓN ANTIVIRUS	$ 9.592.250
TOTAL, COMPONENTE NUMERO 3 LICENCIAMIENTO, SUMINSITROS TENCOLOGICOS Y SOPORTE INTEGRAL DE INFRAESTRUCTURA		$ 327.408.675

Para la estructuración del presupuesto, el Instituto consideró odas las erogaciones tributarias, así como las tarifas y contribuciones que deban cancelarse con ocasión de la celebración del contrato, así como el pago de estampillas, se dará aplicación a lo dispuesto en la Ordenanza 816 de 2017 “Por la cual se expide el Estatuto de Rentas del Departamento de Caldas y se dictan otras disposiciones” y las demás que la complementen o modifiquen.

Debe de considerarse que el presente proceso cuenta con el análisis de costos de los impuestos, la lista que se enuncia a continuación es meramente informativa y en caso de que exista un impuesto o gravamen que deba aplicarse al contrato el mismo deberá ser asumido por el contratista y no podrá oponer a INFICALDAS la presente relación:

Estampilla	% de estampilla
Pro-Desarrollo	1%
Pro-Universidad	2%
Pro-Adulto mayor	3%
Pro-Hospital	1%
Pro-Cultura	1%

Plan de adquisiciones de Bienes y Servicios: La necesidad plasmada en este estudio previo se encuentra en el Plan Anual de Adquisiciones 2026.

FORMA DE PAGO: El Instituto realizará este mediante actas parciales de acuerdo con los insumos o servicios efectivamente recibidos, mediando:

- Autorización del supervisor donde conste el pleno cumplimiento de las condiciones técnicas y de calidad;
- Presentación de la factura con el lleno de los requisitos que impone la norma

- Constancia de cumplimiento de obligaciones con el sistema integral de seguridad y parafiscales, precisando que el Instituto sólo adquiere obligaciones con el adjudicatario del proceso de selección y por tanto no aceptará pagos a terceros.
- Cuando el contrato se suscriba con personas jurídicas se debe acreditar el pago de seguridad social y aportes legales mediante certificación suscrita por el Revisor Fiscal, de acuerdo con los requerimientos de Ley, o por el Representante Legal, bajo la gravedad del juramento, cuando no se requiera Revisor Fiscal, en la que conste el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, cuando a ello haya lugar.
- Cuando el contrato se suscriba con personas naturales se debe acreditar el pago de seguridad social y aportes legales mediante certificación, de acuerdo con la normativa aplicable, en la que conste el pago de sus aportes y el de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, cuando a ello haya lugar, junto con las planillas de pago respectivas

Notas.

1. INFICALDAS no reconocerá, por consiguiente, ningún reajuste realizado por el CONTRATISTA en relación con los costos, gastos o actividades adicionales que aquel requería para la ejecución del contrato y que fueron previsibles al momento de la presentación de la propuesta.
2. La Entidad no se hace responsable por las demoras presentadas en el trámite para el pago al contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas en el Contrato.
3. La Entidad hará las retenciones a que haya lugar sobre cada pago de acuerdo con las disposiciones legales vigentes sobre la materia.
4. Los pagos deberán tramitarse y publicarse a través de la plataforma SECOP II.

Numeral 5 del Artículo 2.2.1.1.2.1.1: *"Los criterios para seleccionar la oferta más favorable"*.

El Instituto adjudicará el contrato al proponente que después de cumplir con los requisitos habilitantes de capacidad jurídica, financiera, organizacional y experiencia, ocupe el primer lugar en el orden de elegibilidad conforme las reglas del fijadas en el pliego de condiciones. Los requisitos habilitantes serán verificados por el comité evaluador, analizando si los proponentes **cumplen o no cumplen** las exigencias fijadas para tal efecto, precisando que la selección de la oferta más favorable se hará ponderando factores de calidad y precio soportados en puntajes y fórmulas.

Para acreditar el cumplimiento de los requisitos enunciados por el artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015, se acudirá al Registro Único de Proponentes de los interesados en armonía con el contenido del pliego de condiciones. Sin perjuicio de la Ley 1882 de 2018 en materia de subsanabilidad, el registro deberá estar vigente y en firme para la fecha de cierre, advirtiendo en todo caso que los interesados deberán acreditar el cumplimiento de lo obligación impuesta por el artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015 en materia de renovación cuando hubiere lugar a ello. Para la acreditación de las condiciones que no resulten objeto de registro por parte de las Cámaras de Comercio, los interesados deberán presentar los documentos que señale el respectivo pliego de condiciones y sus adendas.

Capacidad Jurídica. De conformidad con el artículo 6 de la Ley 80 de 1993, podrán participar en el presente proceso de selección personas jurídicas capaces, independientemente consideradas o a través de la conformación de consorcios o uniones temporales, cuyo objeto social este directamente relacionada con el servicio requerido por el Instituto, siempre y cuando cuenten con habilitación de la autoridad competente para la prestación del mismo.

El Instituto anota que la capacidad está relacionada con: i. La posibilidad de adelantar actividades en ejercicio de su objeto social; ii. Las facultades de su representante legal u órganos de administración cuando resulte necesario según sus estatutos sociales; y iii. La ausencia de inhabilidades, incompatibilidades o prohibiciones para contratar derivadas de la Ley. Para tal efecto, el objeto social será constatado a través del registro único de proponentes y el certificado de existencia y representación, documento a través del cual se verificará quien ejerce la representación legal, sus facultades cuando hubiere lugar a ello, y la correspondencia del objeto social con lo estipulado en el presente capitulo.

Tratándose de uniones temporales o consorcios sus miembros deberán acreditar que dentro de sus objetos está comprendida las actividades que se comprometen a desollar según el documento de conformación correspondiente, precisando que la duración del mismo no podrá ser inferior al término fijado el presente pliego de condiciones para la ejecución del contrato y tres (3) años más.

ESTUDIO PREVIO

Cuando la propuesta supere al límite económico autorizado al representante, el oferente deberá allegar la autorización impartida por el órgano societario correspondiente para validar su actuación, precisando que cuando el Certificado de Existencia haga remisión a los estatutos de la Sociedad para establecer las facultades del representante legal, el oferente deberá anexar copia del apartado pertinente de los mismos. En consecuencia, para verificar la capacidad jurídica los proponentes deberán aportar los siguientes documentos:

1. **Carta de presentación de la propuesta** (modelo anexo al pliego de condiciones) diligenciada y suscrita por el representante legal del oferente.
2. **Certificado de existencia y representación legal** expedido por la cámara de comercio correspondiente dentro de los treinta (30) días calendario anteriores a la fecha de cierre del proceso donde conste: i. Que su objeto social le permite ejecutar el objeto del contrato; ii. Que la persona jurídica cuenta por lo menos con cuatro (04) años de constitución para la fecha de presentación de su oferta, y iii. Que su duración no será inferior al plazo de ejecución del contrato y tres (3) años más; iv. Que cuenta con establecimiento de comercio (principal, sucursal o agencia) debidamente registrado en la Cámara de Comercio de Manizales, Caldas- Colombia.

Tratándose de personas jurídicas extranjeras, deberán acreditar su existencia y representación legal mediante documento equivalente expedido por autoridad competente de país de origen expedido dentro de los noventa (90) días calendario anteriores a la fecha de cierre del proceso en el cual conste expresamente su existencia, fecha de constitución, objeto social, duración, nombre del representante legal o nombre de la persona que ostente la capacidad de contraer obligaciones en nombre de la persona jurídica y sus facultades, precisando en caso de limitaciones estatutarias de dicha capacidad, que resultará necesarios aportar la autorización o documento correspondiente del órgano societario que lo faculta.

3. **Fotocopia de la cédula de ciudadanía** del proponente o del representante legal de la persona jurídica.
4. **Registro único tributario (RUT)** actualizado para la vigencia 2025.
5. **Documento de conformación del consorcio o unión** temporal (modelo anexo al pliego de condiciones) cuando la oferta sea presentada bajo una de estas modalidades. El Instituto advierte que resultaran admisibles consorcios o uniones temporales conformadas por máximo dos (02) integrantes, anotando para efectos de armonización de la calificación con las disposiciones del Decreto 392 de 2018, que el porcentaje mínimo de participación deberá ser del 40%.

   Si la oferta es presentada por un consorcio o por una unión temporal, en la carta de presentación se debe indicar el nombre del consorcio o unión temporal y además el nombre de los integrantes del mismo. En el documento de conformación de consorcio o unión temporal se debe:

   a) Indicar en forma expresa si su participación es a título de consorcio o unión temporal.
   b) Designar la persona que para todos los efectos la representará legalmente.
   c) Fijar las reglas que regulen las relaciones entre sus miembros y sus responsabilidades.
   d) En el caso de la unión temporal señalar en forma clara y precisa, los términos y extensión de la participación en la propuesta y en su ejecución y las obligaciones y responsabilidades de cada uno en la ejecución del contrato (Actividades), los cuales no podrán ser modificados sin el consentimiento previo de la entidad contratante.
   e) Señalar la duración del mismo que no deberá ser inferior a la del contrato y tres (3) años más para constitución de garantías de estabilidad de obra y preservación del interés público.
   f) Ser suscrito por los dos integrantes y el representante del mismo.

6. Certificación de cumplimento de sus obligaciones con el sistema de seguridad social integral expedida conforme el artículo 50 de la Ley 789 de 2002. En caso de consorcios o uniones temporales, que cada uno de los integrantes deberá aportar la certificación de manera individual.

   Nota. Cuando la naturaleza jurídica del proponente lo imponga, a la certificación de cumplimiento de sus obligaciones con el sistema de seguridad social integral deberá adjuntar copia del documento de identidad, copia de la tarjeta profesional del contador y/o revisor fiscal que emita la certificación, y certificado de antecedentes disciplinarios del mismo vigente.

7. Sin perjuicio del beber de verificación del comité evaluador que integrará del Instituto, los interesados deberán aportar los certificados de ausencia de antecedentes judiciales, disciplinarios, fiscales y de medidas correctivas expedidos por las autoridades competentes en cada materia.
8. Adicionalmente, cuando el proponente sea persona natural hombre menor de 50 años, este deberá adjuntar copia de la libreta militar, y en caso de pérdida de la misma, certificación de la Dirección de Reclutamiento correspondiente donde conste que su situación militar se encuentra definida.
9. Registro Único de Proponentes (en adelante RUP) expedido dentro de los treinta (30) días calendario anteriores a la fecha de cierre del proceso. Sin perjuicio de la o dispuesto por la Ley 1882 de 2018 en materia de subsanabilidad, el registro deberá estar vigente y en firme, advirtiendo en todo caso que los interesados deberán acreditar el cumplimiento de lo previsto por el artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015 en materia de renovación cuando hubiere lugar a ello.

ESTUDIO PREVIO

Experiencia.

Los proponentes acreditarán su experiencia a través de la información contenida en el RUP, señalando en el Anexo correspondiente máximo seis (06) contratos liquidados antes de la fecha de cierre del presente proceso de selección, con los cuales deberá cumplir los siguientes requisitos:

a) Que se encuentran clasificados en por lo menos cuatro (4) de las categorías señaladas a continuación:

CODIGO UNSPSC	CONCEPTO
81111800	Servicios de sistemas y administración de componentes de sistemas
81112200	Mantenimiento y soporte de software
81111809	Servicio de instalación de sistemas
43230000	Software
43233700	Software de administración de sistemas
81112206	Mantenimiento de Software o búsqueda o recuperación de la información
81112208	Mantenimiento de Software de protección y seguridad
43211600	Accesorios de computador
81112501	Servicio de licencias del software del computador

b) El proponente deberá acreditar experiencia en:

1. Por lo menos un contrato cuyo objeto y/o actividades refleje la ejecución de Implementación, administración, migración u operación de servicios de infraestructura en la nube, incluyendo componentes IaaS, ambientes virtualizados, gestión de recursos computacionales, almacenamiento, redes virtuales y servicios asociados.
2. Por lo menos un contrato cuyo objeto y/o actividades refleje la ejecución de Prestación de servicios de Recuperación ante Desastres como Servicio (DRaaS) o soluciones de continuidad del negocio, que incluyan réplicas en la nube, planes de recuperación, activación de sitios alternos, pruebas de conmutación y restauración de servicios críticos.
3. Por lo menos un contrato cuyo objeto y/o actividades refleje la ejecución Suministro, licenciamiento, soporte, mantenimiento o administración de infraestructura tecnológica, incluyendo plataformas de virtualización, sistemas operativos, servidores, almacenamiento, redes, herramientas de gestión y componentes técnicos necesarios para la operación de servicios tecnológicos empresariales.

c) La sumatoria del valor de los contratos acreditados deberá ser igual o superior al ochenta por ciento (80 %) del presupuesto oficial del presente proceso de selección.

Nota. Conforme el "*Manual para determinar y verificar los requisitos habilitantes en los procesos de contratación*" (Versión M-DVRHPC-05) de la Agencia Nacional de Contratación, la experiencia del oferente plural (unión temporal o consorcio) corresponderá a la suma de la experiencia que acredite cada uno de sus integrantes. Por otra parte, cuando un proponente adquiera experiencia en un contrato ejecutado como integrante de un contratista plural, la experiencia derivada de dicho contrato corresponderá a la ponderación del valor del contrato por el porcentaje de participación en la ejecución del mismo.

Acreditación de Experiencia. Advirtiendo que resultarán admisibles máximo cuatro (4) contratos para probar la experiencia requerida en el presente literal, los interesados deberán señalar en el formato establecido por el Instituto para tal efecto, el consecutivo del reporte de los mismos en el RUP. Adicionalmente, y bajo el entendido que en el RUP no reposa la totalidad de la información requerida por la Entidad, los proponentes deberán adjuntar documento soporte respecto de cada contrato que pretenda hacer valer donde conste, por lo menos:

- ✓ Nombre de la Entidad estatal contratante.
- ✓ Nombre o razón social del contratista.
- ✓ Objeto del contrato.
- ✓ Fecha de la celebración.
- ✓ Plazo de ejecución del contrato
- ✓ Valor ejecutado.
- ✓ Nombre y cargo de la persona que expide la certificación.

Nota. En caso de discrepancias entre la información registrada en el formulario fijado por el Instituto para la acreditación de la experiencia y los documentos soporte de la misma, prevalecerá lo consignado en los documentos soporte. De igual

modo, en caso de existir discrepancias entre el contenido de soportes aportados por el proponente en su oferta y la RUP, prevalecerá lo consignado en RUP.

Capacidad Financiera y Organizacional.

El Instituto verificará la capacidad financiera y organizacional de los oferentes como requisito habilitante al amparo de la información contenida en el RUP, precisando cuando de consorcios o uniones temporales se trate, que cada uno de los integrantes deberá aportar el mismo. Para efectos de cálculo, en dichos eventos se procederá así:

- Consorcios: Calculando independientemente los indicadores de cada uno de los integrantes los cuales serán sumados y divididos por el número de integrantes para fijar los valores particulares del consorcio.
- Unión temporal: Calculando independientemente los indicadores de cada uno de los integrantes los cuales serán sumados ponderadamente en función del porcentaje de participación para fijar los valores particulares de la unión.

En términos de capacidad financiera los proponentes deberán cumplir los siguientes rangos:

Indicador	Rango
Liquidez: Activo corriente/Pasivo corriente.	≥ 1,90
Nivel de endeudamiento: Pasivo total/Activo total.	≤ 0,70
Cobertura de intereses: Utilidad operacional/Gasto de intereses.	≥ 3,55

En términos de capacidad organizaciones, los proponentes deberán cumplir los siguientes rangos:

Indicador	Rango
Rentabilidad del patrimonio: Utilidad operacional/Patrimonio.	Mayor o igual a 0,20
Rentabilidad sobre los activos: Utilidad operacional/Activo total.	Mayor o igual a 0,10

Capacidad operativa:

El proponente mediante carta de compromiso deberá certificar que para la ejecución del contrato cuenta con el equipo de trabajo que a continuación se relaciona:

ITEM	PERFIL	PREGRADO	ESPECIALIZACIÓN	PORCENTAJE DE DEDICACIÓN	EXPERIENCIA
1	Líder de Infraestructura Tecnológica	Profesional en Ingeniería de Sistemas	• Especialización en Infraestructura de Tecnologías de la Información y/o • Especialización en Arquitectura de TI y/o • Especialización en Administración de Infraestructura de TI y/o • Especialización en Gestión de Infraestructura Tecnológica Empresarial y/o áreas afines directamente relacionadas con las funciones del perfil.	50%	Mínimo dos (2) años de experiencia específica, contados a partir de la obtención del título de especialización. Además, deberá acreditar experiencia de al menos un (1) año en la participación o ejecución de proyectos de infraestructura tecnológica.
2	Líder de Seguridad de la Información	Profesional en ingeniera de sistemas	• Especialización en Seguridad de la Información y/o • Especialización en Gestión de Seguridad	50%	Mínimo dos (2) años de experiencia profesional certificada, contados a partir de la obtención del título universitario. Además, deberá acreditar experiencia

			de la Información (SGSI) y/o • Especialización en Gobierno y Gestión de TI con énfasis en Seguridad y/o • Especialización en Cumplimiento Normativo en Seguridad y/o áreas afines directamente relacionadas con las funciones del perfil.		de al menos un (1) año específica en actividades de gestión, análisis o implementación de controles de seguridad de la información, conformidad normativa o administración del SGSI.
3	Líder de Comunicaciones y Redes	Profesional en ingeniera de sistemas	• Especialización en Telecomunicaciones y/o • Especialización en Redes y Telecomunicaciones y/o • Especialización en Ingeniería de Telecomunicaciones y/o • Especialización en Sistemas de Comunicación Inalámbrica y/o • Especialización en Comunicaciones Móviles y Banda Ancha y/o áreas afines directamente relacionadas con las funciones del perfil.	50%	Mínimo dos (2) años de experiencia específica, contados a partir de la obtención del título de especialización. Además, deberá acreditar experiencia de al menos un (1) año en la implementación, administración o soporte de redes de comunicaciones, infraestructura de conectividad o tecnologías de telecomunicaciones.
4	Director del Proyecto	Profesional en ingeniera de sistemas	• Especialización en Gestión de Proyectos y/o • Especialización en Arquitectura de TI, Computación en la Nube y/o áreas afines directamente relacionadas con las funciones del perfil.	50%	Mínimo tres (3) años de experiencia específica, contados a partir de la obtención del título de especialización. Además, deberá acreditar al menos un (1) año de experiencia adicional en la dirección, coordinación o gestión de proyectos de infraestructura tecnológica, soluciones en la nube o servicios de continuidad del negocio (DRaaS).

ESTUDIO PREVIO

Para acreditar la formación académica, el adjudicatario deberá para la suscripción del contrato, presentar los siguientes documentos:

a. Copia de la cédula de ciudadanía.
b. Copia del acta de grado y/o diploma de grado de profesional y/o diploma del programa técnico o tecnológico, según aplique.
c. Copia de la tarjeta profesional (Cuando aplique).
d. Certificación de la vigencia de la matrícula profesional y antecedentes, en caso de que la ley exija este requisito para ejercer la profesión.
e. Copia del documento de convalidación de los títulos obtenidos en el exterior, de conformidad con las disposiciones legales vigentes sobre la materia, según corresponda (Cuando aplique).

Para acreditar la experiencia, el adjudicatario deberá allegar certificaciones que deberán contener como mínimo la siguiente información:

a. Nombre o razón social del contratante.
b. Nombre o razón social del contratista.
c. Objeto del contrato, funciones, obligaciones o actividades desempeñadas
d. Fecha de iniciación y de terminación del contrato o plazo del contrato.
e. Firma de la persona que suscribe la certificación y quien debe estar debidamente facultada para expedir la certificación.

En el evento que la certificación contenga el mes, pero no el día - fecha de inicio y/o terminación, ésta se contabilizará con el último día del mes respectivo para el inicio y el primer día del mes de terminación; o con el de la fecha de expedición del documento, según sea el caso.

En caso de que el profesional tenga vínculo laboral o contrato de prestación de servicios vigente, podrá aportar certificación de experiencia para lo cual se contabilizará el tiempo desde la fecha de inicio hasta la fecha de suscripción o firma de dicha certificación.

Se acepta como equivalente a la certificación de experiencia de los contratos ejecutados, copia del acta de liquidación o de recibo final (contratos celebrados con entidades públicas) y que de ellos se evidencie la información, de acuerdo con lo establecido en los literales a. al e.

Para efecto de contabilizar los años de experiencia que se verificará, se sumarán los intervalos laborados una sola vez, es decir, los tiempos traslapados no se tendrán en cuenta.

El equipo mínimo de trabajo para ejecutar el contrato que se vincule para la ejecución del contrato dependerá administrativamente del contratista y no tendrá vínculo laboral con **INFICALDAS.**

La Entidad se reserva el derecho de solicitar el cambio de algún integrante del equipo mínimo de trabajo para ejecutar el contrato, en los siguientes eventos:

a. Por autorización o solicitud de **INFICALDAS** por intermedio del supervisor del contrato designado por ésta, cuando advierta que el desarrollo de sus actividades no es satisfactorio, o sus actuaciones atentan contra la buena relación con el contratante, o cause algún impacto negativo a la Entidad.
b. Por fuerza mayor o caso fortuito debidamente comprobados.
c. En el evento de enfermedad o vacaciones será remplazado y sólo por el tiempo necesario. En caso de requerirse reemplazo de alguno de los integrantes o de todo el equipo mínimo de trabajo para ejecutar el contrato, se deberá contar con la aprobación por escrito del supervisor del contrato asignado por parte de INFICALDAS. Para autorizar el reemplazo, se deberá presentar a la **INFICALDAS** una persona que cumpla con los requisitos mínimos solicitados para determinado rol.

Evaluación de la Oferta.

El comité designado por el Instituto evaluará las ofertas de los proponentes que hayan acreditado el cumplimiento de los requisitos habilitantes, los cuales serán calificados así:

Requisitos	Calificación

Capacidad Jurídica.	Cumple / No Cumple
Experiencia.	Cumple / No Cumple
Capacidad Financiera y Organizacional.	Cumple / No Cumple
Capacidad Operativa.	Cumple / No Cumple
Garantía de Seriedad de la Oferta.	Cumple / No Cumple

Posterior a la dicha verificación, se procederá a realizar la calificación para establecer el orden de elegibilidad, así:

Criterio de Evaluación	**Puntos**	**Porcentaje (%)**
Calidad del servicio.	500	50%
Valor de la propuesta	385	38,5%
Incentivo a la Industria Nacional.	100	10%
Apoyo a personal con discapacidad.	10	1%
Apoyo a mujeres emprendedoras.	2.5	0,25%
Mipymes	2.5	0.25%
Total	**1000**	**100%**

Nota. Dada la naturaleza que el ordenamiento jurídico impone a los criterios fijados en el presente apartado, no resultará posible la subsanación de estos por tratarse condiciones para el otorgamiento de puntaje, por lo cual la ausencia de alguno de estos documentos dará lugar al rechazo de la propuesta.

A. Calidad del servicio (Hasta 500 Puntos)

El puntaje por este factor se otorgará teniendo en cuenta los siguientes criterios:

Tendrá una ponderación máxima de 300 puntos y se asignarán al proponente que ofrezca en menor tiempo de respuesta a las solicitudes o inconvenientes que tenga con el servicio INFICALDAS necesarios para optimizar la prestación del servicio. Se acredita mediante certificaciones en las cuales deberá decir en el tiempo de respuesta ofertado:

Concepto	**Puntaje**
Ofrecer un tiempo de respuesta igual o inferior a ocho (08) horas	300
Ofrecer un tiempo de respuesta igual o inferior a doce (12) horas	250
Ofrecer un tiempo de respuesta igual o inferior a veinticuatro (24) horas	200

TERABYTES ADICIONALES DE ALMACENAMIENTO RESPECTO A INFRAESTRUCTURA TECNOLÓGICA– 20 PUNTOS

Se le otorgará el siguiente puntaje al proponente que oferte almacenamiento adicional a los contemplados para la infraestructura almacenamiento.

Concepto	**Puntaje**
2 Terabytes adicionales	5
4 o más Terabytes adicionales	15

TERABYTES ADICIONALES DE ALMACENAMIENTO RESPECTO A LA INFRAESTRUCTURA DISPUESTA EN PLAN DE CONTINUIDAD DEL NEGOCIO– 20 PUNTOS

Se le otorgará el siguiente puntaje al proponente que oferte almacenamiento adicional a los contemplados para la infraestructura almacenamiento.

Concepto	**Puntaje**
2 Terabytes adicionales	5
4 o más Terabytes adicionales	15

ACREDITACIÓN DE CALIDAD- 60 PUNTOS

El proponente que acredite contar con certificación en la norma ISO 27001 será acreedor de 60 puntos dentro del proceso

ESTUDIO PREVIO

TIEMPO DE ENTREGA DE SUMINISTRO DE RESPUESTOS - 50 PUNTOS

Concepto	Puntaje
Ofrecer un tiempo de respuesta igual o inferior a veinticuatro (24) horas	50
Ofrecer un tiempo de respuesta igual o inferior a cuarenta y ocho (48) horas	30
Ofrecer un tiempo de respuesta igual o inferior a setenta y dos (72) horas	15

EXPERIENCIA ADICIONAL DEL PROFESIONAL DE SOPORTE EN SITIO: 50 PUNTOS

El proponente que mediante carta de compromiso certifique que el profesional solicitado por INFICALDAS para "**Servicio de ingeniería de infraestructura y soporte especializado** cuenta con experiencia adicional en configuración, gestión y soporte de infraestructura de servidores en nube se otorgará el siguiente puntaje:

Experiencia adicional a la mínima requerida por parte de INFICALDAS	Puntaje
3 años de experiencia adicional a la mínima requerida	50
6 años de experiencia adicional a la mínima requerida	30

El cumplimiento de dicho requisito será verificado por parte del supervisor del contrato previa suscripción del acta de inicio del contrato respectivo, so pena de hacer efectiva la garantía de seriedad de la oferta.

B. Valor de la propuesta respecto a medios complementarios: Hasta 385 Puntos

Advirtiendo que las ofertas económicas que superen el presupuesto oficial serán rechazadas, el Instituto pone de presente que las mismas deberán formalizarse a través del formulario dispuesto en la plataforma del Secop II, teniendo en cuenta los requerimientos del Instituto. En la revisión del formulario de precios se tendrá en cuenta lo siguiente, anotando que la Entidad podrá efectuar correcciones aritméticas originadas cuando registre un error que surja de un cálculo meramente aritmético con ocasión de una operación erróneamente realizada

a) Que se haya consignado y ofrecido todos y cada uno de los ítems que integran el servicio, así como el valor unitario de cada uno de ellos en números enteros (sin decimales).
b) Que el valor total sea igual o inferior al presupuesto oficial.
c) Que el formulario de la propuesta económica no presente tachadura o enmendadura.

El comité evaluador, a partir del valor de las ofertas de los proponentes habilitados, asignará máximo trescientos ochenta y cinco (385) puntos acumulables de acuerdo con el método escogido para la ponderación de las mismas, precisando que la elección del mismo estará definida por los dos primeros decimales de la TRM informada por el Banco de la Republica para la fecha correspondiente para el segundo día hábil siguiente a la fecha de vencimiento del traslado del informe de evaluación señalado en el cronograma del proceso (verificado en www.banrep.gov.co/es/tasa-cambio-del-peso-colombiano-trm), así:

Rango (inclusive)	Método
De 0.00 a 0.33	Mediana con valor absoluto.
De 0.34 a 0.66	Media geométrica.
De 0.67 a 0.99	Media aritmética baja.

El Instituto tendrá en cuenta hasta el tercer (3) decimal del valor obtenido como puntaje, precisando que la fórmula elegida será aplicada solo con respecto de las propuestas debidamente habilitadas. Sin perjuicio de lo anterior, las propuestas que al aplicar las fórmulas obtengan puntajes negativos obtendrán cero (0) puntos en la calificación de la oferta económica.

- **Mediana con valor absoluto.** El comité evaluador ordenará los valores de las propuestas hábiles descendentemente. Si el número de valores es impar, la mediana corresponde al valor central, si el número de valores es par, la mediana corresponde al promedio de los dos valores centrales.

$$\mathrm{Me} = \mathrm{Mediana}(\mathrm{V}_1; \mathrm{V}_2 . . ; \ldots \mathrm{V}_\mathrm{m})$$

Donde:

V_i: Es el valor total corregido de cada una de las propuestas "i".
m: Es el número total de propuestas económicas válidas recibidas por la Entidad.

Me: Es la mediana calculada con los valores de las propuestas económicas válidas.

Bajo este método la Entidad asignará puntaje así:

I. Si el número de valores de las propuestas hábiles es impar, el máximo puntaje será asignado a la propuesta que se encuentre en el valor de la mediana. Para las otras propuestas, se utiliza la siguiente fórmula:

$$\text{Puntaje} = \left[\left\{1 - \left|\frac{\text{Me} - \text{V}_\text{i}}{\text{Me}}\right|\right\} * 70\right]$$

Donde:

Me: Es la mediana calculada con los valores de las propuestas económicas válidas.
V_i: Es el valor total corregido de cada una de las propuestas "i".

II. Si el número de valores de las propuestas hábiles es par, se asignará el máximo puntaje a la propuesta que se encuentre inmediatamente por debajo de la mediana. Para las otras propuestas, se utiliza la siguiente fórmula

$$\text{Puntaje} = \left[\left\{1 - \left|\frac{\text{V}_\text{Me} - \text{V}_\text{i}}{\text{V}_\text{Me}}\right|\right\} * 70\right]$$

Donde:

V_Me: Es el valor de la propuesta económica válida inmediatamente por debajo de la mediana.
V_i: Es el valor total corregido de cada una de las propuestas "i".

- **Media geométrica.** Para calcular la media geométrica se tomará el valor de las propuestas hábiles del respectivo factor de calificación para asignar el puntaje de conformidad con el siguiente procedimiento:

$$\text{MG} = \sqrt[\text{n}]{\text{V}_1 * \text{V}_2 * \text{V}_3 * \ldots * \text{V}_\text{n}}$$

Donde:

MG: Es la media geométrica de los tres menores valores.
V1: Es el valor de una propuesta habilitada.
Vn: Es el valor de la propuesta n habilitada.
n: La cantidad total de propuestas habilitadas.

Para efectos de la asignación de puntaje, se asignará el máximo puntaje al valor de la propuesta que se encuentre más cerca (por exceso o por defecto) al valor de la media geométrica calculada para el factor correspondiente. Las demás propuestas recibirán puntaje de acuerdo con la siguiente ecuación:

$$\text{Puntaje} = \textit{Puntaje máximo} * \left(1 - \left(\frac{|\text{MG} - \text{V}_\text{i}|}{\text{MG}}\right)\right)$$

Cuando el resultado de la formula anterior sea un número negativo se asignará cero (0) puntos.

- **Media aritmética baja**. Consiste en determinar el promedio aritmético entre la propuesta válida más baja y el promedio simple de las ofertas hábiles para calificación económica.

$$\overline{\text{X}_\text{B}} = \frac{(\text{V}_\text{min} + \overline{\text{X}})}{2}$$

Donde:

V_min: Es el valor total corregido de la propuesta válida más baja.
$\overline{\text{X}}$: Es el promedio aritmético simple de las propuestas económicas válidas.
$\overline{\text{X}_\text{B}}$: Es la media aritmética baja.

La Entidad procederá a ponderar las propuestas de acuerdo con la siguiente formula:

$$\text{Puntaje} = \left\{ \begin{array}{l} \textit{Puntaje máximo} * \left(1 - \left(\frac{\overline{X_B} - V_i}{\overline{X_B}}\right)\right) \text{ Para valores menores o iguales a } \overline{X_B} \\ \textit{Puntaje máximo} * \left(1 - \left(\frac{|\ \overline{X_B} - V_i\ |}{\overline{X_B}}\right)\right) \text{ Para valores mayores a } \overline{X_B} \end{array} \right\}$$

Donde:

$\overline{X_B}$: Es la media aritmética baja.
V_i: Es el valor total corregido de cada una de las propuestas "i".

Precio Artificialmente Bajo. En el evento en el que el precio de una oferta no parezca suficiente para garantizar una correcta prestación del servicio conforme la información obtenida en la etapa de planeación, y en particular, durante el estudio del sector, el Instituto atenderá lo dispuesto por el artículo 2.2.1.1.2.2.4. del Decreto 1082 de 2015, sin perjuicio de Guía para manejo de ofertas artificialmente bajas en procesos de contratación de la Agencia Nacional de Contratación como un criterio metodológico.

C. Incentivo a la Industria Nacional: Hasta 100 Puntos

En concordancia con la Ley 816 de 2003, el Instituto asignará puntaje por apoyo a la industria nacional, indicando procedencia de los bienes y servicios dispuestos para la ejecución del contrato. El puntaje se asignará de la siguiente manera:

a) Cuando el proponente oferte bienes o servicios 100% nacionales para ejecución del contrato derivado del proceso de selección se le asignarán 100 puntos (10%).
b) b. Cuando el proponente oferte servicios con personal nacional y extranjero para ejecución del contrato derivado del proceso de selección se le asignarán 50 puntos (5%).
c) c. Si no se diligencia o se diligencia marcando ambas posibilidades en el Anexo fijado en el pliego de condiciones, el oferente no obtendrá puntuación en este factor.

D. Apoyo a personal con discapacidad: Hasta 10 Puntos

En aplicación del Decreto 392 de 2018, y con el ánimo de incentivar el sistema de preferencias en favor de personas con discapacidad, se otorgarán diez (10) puntos (equivalente al 1% que señala la norma), a los proponentes que acrediten la vinculación de trabajadores con discapacidad en su planta de personal, de acuerdo con las siguientes reglas:

- ✓ La persona natural, el representante legal de la persona jurídica o el revisor fiscal, según fuere el caso, certificará el número total de trabajadores vinculados a la planta de personal del oferente a la fecha de cierre del proceso.
- ✓ Acreditar el número mínimo de personas con discapacidad en su planta de personal conforme el certificado expedido por el Ministerio de Trabajo, el cual deberá estar vigente a la fecha de cierre del proceso de selección.

Verificado lo anterior, se otorgarán diez (10) puntos (equivalente al 1% que señala la norma) a quienes acrediten el número mínimo personas con discapacidad, señalados a continuación:

Planta de trabajadores del proponente	Mínimo de trabajadores con discapacidad exigido
Entre 1 y 30	1
Entre 31 y 100	2
Entre 101 y 150	3
Entre 151 y 200	4
Más de 200	5

Si la oferta es presentada por un consorcio o unión temporal, se tendrá en cuenta la planta de personal del integrante del proponente plural que aporte como mínimo el 40% de la experiencia requerida para la respectiva contratación. Conforme el artículo 24 de la Ley 361 de 1997, el personal postulado deberá estar contratado "*(…) por lo menos con anterioridad a un año; igualmente deberán mantenerse por un lapso igual al de la contratación*".

E. Apoyo a mujeres emprendedoras: Hasta 2.5 Puntos

En aplicación del Decreto 1860 de 2021, y con el fin de apoyar los emprendimientos y empresas de mujeres, se otorgarán dos punto cinco (2.5) puntos (equivalente al 0,25% que señala la norma), a los proponentes que acrediten alguno de los supuestos del artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015.

Para tal efecto, los proponentes emitirán las certificaciones de trata el citado artículo bajo gravedad de juramento, dentro de los treinta (30) días calendario anteriores a la fecha de cierre del proceso de selección.

F. Mipyme domiciliada en Colombia: 0.25 Puntos

La Entidad otorgará un puntaje de cero punto veinticinco (0.25) puntos al Proponente que acredite la calidad de Mipyme domiciliada en Colombia de conformidad con el artículo 2.2.1.2.4.2.4 del Decreto 1082 de 2015, en concordancia con el parágrafo del artículo 2.2.1.13.2.4 del Decreto 1074 de 2015, o la norma que lo modifique, complemente o sustituya.

Así las cosas, para obtener el puntaje. el Proponente entregará copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación. Si el Proponente debió subsanar la entrega del RUP, éste será válido para los criterios diferenciales en cuanto a los requisitos habilitantes relacionados con el número de contratos aportados para demostrar la experiencia solicitada y los índices de la Capacidad Financiera y Organizacional. Sin embargo, el certificado, no se tendrá en cuenta para la asignación del puntaje adicional, por lo que obtendrá cero (0) puntos por este factor de evaluación.

Tratándose de Proponentes Plurales este puntaje se otorgará si por lo menos uno de los integrantes acredita la calidad de Mipyme y tiene una participación igual o superior al diez por ciento (10%) en el Consorcio o en la Unión Temporal.

G. Orden de Elegibilidad y Adjudicación.

El orden de elegibilidad estará dado por la sumatoria de los puntajes obtenidos por los proponentes (habilitados) en cada uno de los factores establecidos el presente pliego de condiciones. Así las cosas, el ordenador del gasto mediante acto administrativo motivado, adjudicará el proceso al proponente ubicado en primer de orden de elegibilidad, siempre y cuando cumpla la totalidad de las exigencias del Instituto.

Nota. La decisión de adjudicación es irrevocable, salvo cuando se presente el supuesto establecido en el artículo anteriormente referido. En el evento que el ordenador del gasto no acoja el resultado de la evaluación practicada por el comité integrado para tal efecto, así lo justificará en el acto administrativo correspondiente.

H. Factores de Desempate.

Atendiendo el artículo 2.2.1.1.2.2.9 del Decreto 1082 de 2015 y el artículo 2.2.1.2.4.2.17 del Decreto 1860 de 2021 en caso de empate en el puntaje total de dos o más ofertas, el Instituto escogerá el oferente que tenga el mayor puntaje en el primer criterio de evaluación de los factores establecidos en la normatividad enunciada. Si persiste el empate, escogerá al oferente que tenga el mayor puntaje en el segundo criterio de evaluación, y así sucesivamente, hasta agotar la totalidad de los criterios fijados por la administración. Si persiste el empate, el Instituto con el fin de garantizar la selección objetiva, procederá a desempatar mediante sorteo, así:

a. Ordenará a los proponentes empatados en orden alfabético según el nombre de la persona. Una vez ordenados, le asignará un número a cada uno de forma ascendente, de tal manera que al primero le corresponda el número 1.
b. Luego, tomara la parte entera (números a la izquierda de la coma decimal) de la TRM que rigió el día del cierre del proceso y dividirá esta entre el número de proponentes en empate, para posteriormente tomar su residuo y utilizarlo en la selección final.
c. Realizado calculo anterior, seleccionará a aquel proponente que presente coincidencia entre el número asignado y el residuo encontrado. En caso de que el residuo sea cero (0), se escogerá al proponente con el mayor número asignado.

Numeral 6 del Artículo 2.2.1.1.2.1.1: *"El análisis de Riesgo y la forma de mitigarlo"*.

Atendiendo las disposiciones de la Ley 1150 de 2007 y el Decreto 1082 de 2015, y en armonía con la metodología señalada en el *"Manual para la Identificación y Cobertura del Riesgo en Procesos de Contratación"* de la Agencia Nacional de Contratación, se tipifican, estiman y asignan los riesgos asociados al proceso. Aquí el Instituto precisa que los mecanismos de cobertura adoptados, incluida la garantía única de cumplimiento, permiten mantener las condiciones económicas y financieras existentes al momento de presentación de la propuesta por parte del contratista y por lo tanto, procurar el equilibrio económico del contrato conforme la Ley 80 de 1993.

Teniendo en cuenta la naturaleza jurídica del contrato a celebrar, los riesgos derivados del mismo son los relacionados a continuación:

RIESGOS PREVISIBLES

El Documento Conpes 3714 de 2011 clasifica los Riesgos de acuerdo con los siguientes tipos:

ESTUDIO PREVIO

Riesgos Económicos: son los derivados del comportamiento del mercado, tales como la actuación de los precios de los insumos, desabastecimiento y especulación de estos, entre otros.

Riesgos Sociales o Políticos: son los derivados de los cambios de las políticas gubernamentales y de cambios en las condiciones sociales que tengan impacto en la ejecución del contrato.

Riesgos Operacionales: son los asociados a la operatividad del contrato, tales como la ausencia del presupuesto o del, del plazo o los derivados de procesos, procedimientos, parámetros, sistemas de información y tecnológicos, equipos humanos o técnicos inadecuados o insuficientes.

Riesgos Financieros: son (i) el riesgo de consecución de financiación o riesgo de liquidez para obtener recursos para cumplir con el objeto del contrato, y (ii) el riesgo de las condiciones financieras establecidas para la obtención de los recursos, tales como plazos, tasas, garantías, contragarantías, y refinanciaciones, entre otros.

Riesgos Regulatorios: derivados de cambios regulatorios o reglamentarios que afecten la ecuación económica del contrato.

La descripción de cada uno de los Riesgos y la determinación de las posibles consecuencias de la ocurrencia de estos serán definidos a continuación teniendo en cuenta lo establecido en el Documento CONPES 3714 de 2011 y el Manual para la identificación y cobertura del Riesgo de Colombia Compra Eficiente.

N	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/ Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del	Responsable por implementar	Fecha estimada en que se	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza	Periodicidad
	General	Externo	Selección	Económico	Ofertas artificialmente bajas. Le corresponde al oferente garantizar que con los precios ofertados cumpla las condiciones técnicas y de calidad de las actividades a desarrollar en el contrato.	Se podría presentar en la ejecución del proyecto una deficiente calidad de los trabajos y/o servicios.	3	1	4	Riesgo bajo	Contratista	Solicitar soporte que justifique los valores ofrecidos en la oferta. Seguimiento a la ejecución del proyecto a fin de que se cumpla con las especificaciones técnicas a cabalidad	3	1	4	Riesgo bajo	NO	UNIDAD EJECUTORA	N/A	EN LA SELECCIÓN Y LA EJECUCIÓN DEL CONTRATO	Revisión de las justificaciones dadas por el oferente. Seguimiento de las labores ejecutadas	En la selección y ejecución del proyecto.

ESTUDIO PREVIO

N	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/ Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del	Responsable por implementar	Fecha estimada en que se	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza	Periodicidad
1	General	Interno	Planeación	Operacional	Se presenta cuando la definición de la necesidad y el objeto establecido en el estudio previo, no se ajusta a la modalidad de selección aplicable.	Retrasos en la revisión y ajuste del estudio previo por parte del abogado a cargo del tema y aprobación del mismo	4	2	6	Riesgo Alto	ENTIDAD	Revisión y apoyo jurídico a las dependencias que solicitan la contratación, aclarando los requisitos y la aplicabilidad de cada una de las modalidades de selección.	2	1	3	Riesgo Bajo	NO	UNIDAD EJECUTOTA	PRE CONTRACTUAL	FIRMA DEL CONTERATO	Asesoría a las dependencias, revisión y ajuste del Estudio Previo. Constante actualización normativa.	Cada vez que se presenta una solicitud de contratación.
2	General	Externo	Contratación	Tecnológico	Ocurre cuando se presentan fallas en la disponibilidad del Sistema de Contratación Pública SECOP (www.colombiacompra.gov.co)	Retraso o incumplimiento de los plazos legales para la publicación de los actos y/o documentos derivados de los procesos contractuales	3	1	4	Riesgo Bajo	ENTIDAD	Reporte al Administrador del SECOP, y dejar evidencia de la interrupción del servicio.	1	1	2	Riesgo Bajo	Baio	UNIDAD EJECUTIRA	PRE CONTRACTUAL	FIRMA DEL CONTERATO	Revisando la Página de SECOP para el cargue de la información	Cada vez que hay que publicar actos administrativos de contratación

ESTUDIO PREVIO

N	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/ Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del	Responsable por implementar	Fecha estimada en que se	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza	Periodicidad
3	General	Externo	Ejecución	Operacional	Ocurre cuando se presentan retrasos o incumplimientos en la entrega de los informes y/o productos a cargo del contratista, con ocasión de la ejecución del contrato.	Afectación de la ejecución del contrato, satisfacción de la necesidad y posible incumplimiento de las obligaciones y actividades pactadas en el contrato.	3	4	7	Riesgo Alto	CONTRQATISTA	Seguimiento y verificación del cumplimiento de las obligaciones pactadas en el contrato.	1	1	2	Riesgo Bajo	NO	SUPERVISOR	INICIO DEL CONTRATO	ACTA DE ENTREGA Y RECIBO DEFINITIVO DEL CONTRTAO	A través de la verificación de cumplimiento de las obligaciones del contratista, en los plazos establecidos en el	Permanente y previo a la expedición del recibo a satisfacción.
4	General	Interno	Contratación	Financiero	Se presenta cuando la entidad no cuenta con los recursos para pagar el valor del contrato en los plazos establecidos.	Genera mora de la entidad en el pago que puede afectar al contratista, hasta el punto de romper la ecuación económica del contrato.	1	2	3	Riesgo Bajo	ENTIDAD	Verificación del valor total del contrato y/o sus adiciones en valor, de manera previa a la expedición del registro presupuestal.	1	2	2	Riesgo Bajo	NO	Área de presupuesto	INICIO DEL CONTRATO	TERMINACIÓN DEL CONTRTAO	En el momento de expedir el registro presupuestal al contrato y/o sus adiciones en	Cada vez que se expide registro presupuestal a un contrato y/o adición.

ESTUDIO PREVIO

N	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/ Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del	Responsable por implementar	Fecha estimada en que se	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza	Periodicidad
5	General	Interno	Ejecución	Seguridad y Salud en el Trabajo	El no pago de Seguridad social, riesgos laborales e indemnizaciones de cada uno de los empleados que intervengan en las labores contratadas para la ejecución del contrato	Futuras demandas laborales	2	5	7	Riesgo Alto	Partes intervinientes del contrato	Verificación de la certificación de seguridad social por parte del supervisor antes de efectuar cualquier tipo de pago	2	2	4	Riesgo Bajo	NO	Entidad contratante	Ejecución	Ejecución	Control y vigilancia a cargo del supervisor	Permanente
	Especifico	Externa	Ejecución	Operacional	Cambio del Equipo de Trabajo. Se refiere a la posibilidad que durante la Ejecución sea necesario el cambio parcial o total del equipo de trabajo.	Realizar reprocesos y retrasos	4	3	7	Riesgo Alto	Contratista	Definición de los perfiles organizacionales para la ejecución del contrato. El contratista deberá garantizar una estabilidad organizacional y laboral favorable que mitigue la deserción de personal.	3	3	6	Riesgo Alto	SI	Contratista	Ejecución	Ejecución	Seguimiento por parte del supervisor	Permanente

Numeral 7 del Artículo 2.2.1.1.2.1.1: *"Las garantías que la Entidad contempla exigir en el Proceso"*.

En armonía con la matriz de riesgos asociada al proceso, se precisan las garantías que la administración estima necesarias para la guarda de sus intereses:

ESTUDIO PREVIO

Fase precontractual. El proponente adjuntará a su ***propuesta garantía única que ampare la seriedad de su propuesta*** en favor del Instituto expedida por aseguradora o entidad bancaria domiciliada en Colombia y vigilada por la Superintendencia Financiera. En caso de requerirse ampliación de la vigencia, esta deberá ser ajustada conforme los requerido de la administración. Para efectos de constitución, los interesados deberán tener en cuenta la siguiente información:

Beneficiario:	Instituto de Financiamiento, Promoción y Desarrollo de Caldas INFICALDAS (NIT. 890.806.006-3).
Afianzado:	El proponente (según certificado de existencia y representación). En el caso de consorcios o uniones temporales deberá tomarse a nombre de la figura asociativa elegida (indicando integrantes y porcentaje de participación) y no a nombre de su representante.
Vigencia:	Tres (3) meses contados a partir de la fecha de presentación de la oferta.
Cuantía:	Equivalente al diez por ciento (10%) del presupuesto oficial
Amparo:	El texto de la garantía deberá indicar textualmente el número, año y objeto del proceso.
Firmas:	Deberá ser suscrita por quien la expide.

La ausencia de la garantía de seriedad de la oferta al momento su presentación resultará subsanable y constituirá causal de rechazo conforme la Ley 1882 de 2017. El Instituto hará efectiva la garantía de seriedad a título de indemnización, sin menoscabo de las acciones para el reconocimiento de perjuicios no cubiertos cuando hubiere lugar a ello.

Fase Contractual. Admitiendo la prevalencia del interés de la administración, el contratista (adjudicatario del proceso) deberá constituir en favor del Instituto, garantía única de cumplimiento que podrá consistir en póliza de seguro expedida por una compañía de seguros legalmente establecida en Colombia, o garantía bancaria otorgada por un banco local, que ampare y cumpla las siguientes condiciones:

Amparo	Suficiencia	Vigencia***
Cumplimiento incluido amparo de posibles multas y la cláusula penal pecuniaria.	20% del valor del Contrato	Plazo de ejecución del contrato y cuatro (4) meses más.
Calidad de los bienes y servicios prestados.	20% del valor del Contrato	Plazo de ejecución del contrato y cuatro (4) meses más.
Pago de salarios, prestaciones e indemnizaciones laborales.	20% del valor del Contrato	Plazo de ejecución y tres (3) años más.

*** Si el contrato se prorrogare o adicionare, el futuro contratista deberá ajustar la garantía única.

Numeral 8 del Artículo 2.2.1.1.2.1.1: *"La indicación de si el Proceso está cobijado por un Acuerdo Comercial"*.

Según el *Manual para el manejo de Acuerdos Comerciales* (CCE-EICP-MA-03 V1. 24/11/2021) de la Agencia Nacional de Contratación, las entidades descentralizadas del orden departamental están cubiertas por los *"Acuerdos Comerciales con Chile, el Triángulo Norte (únicamente con El Salvador y Guatemala), la Unión Europea (aplicable al Reino Unido e Irlanda del Norte) y por la Decisión 439 de 1998 de la Comisión de la CAN"* (página 30).

A continuación, se evidencia el análisis practicado por el instituto para establecer los Acuerdos aplicables, entendidos como condición para fijar los términos de la presente convocatoria pública:

Acuerdo Comercial		**¿Vigente?**	**Entidad Estatal cubierta**	**Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial**	**Excepción Aplicable al Proceso de Contratación**	**Proceso de Contratación cubierto por el Acuerdo Comercial**
Alianza Pacífico	Chile	SI	NO	NO	NO	NO
	Perú	SI	NO	NO	NO	NO
	México	SI	NO	NO	NO	NO
Canadá		SI	NO	NO	NO	NO
Chile		SI	SI	Bienes y servicios ($287.055.445) Servicios de construcción ($28.705.544.496)	NO	SI
Corea		SI	NO	NO	NO	NO
Costa Rica		SI	NO	NO	NO	NO
Estados AELC		SI	NO	NO	NO	NO

ESTUDIO PREVIO

Acuerdo Comercial		¿Vigente?	Entidad Estatal cubierta	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
Estados Unidos		SI	NO	NO	NO	NO
México		SI	NO	NO	NO	NO
Triángulo Norte	El Salvador	SI	SI	Menor cuantía de la entidad ($398.580.000)	NO	SI
	Guatemala	SI	SI	Menor cuantía de la entidad ($398.580.000)	NO	SI
	Honduras	SI	NO	NO	NO	NO
Unión Europea		SI	NO	NO	NO	NO
Israel		SI	NO	NO	NO	NO
Reino Unido e Irlanda del Norte		SI	SI	Bienes y servicios ($746.344.157) Servicios de construcción ($28.705.544.496)	NO	SI
Comunidad Andina		SI	SI	N/A	NO	SI

Sarlaft. En cumplimiento de la Circular Externa 034 de 2013 del Superintendencia Financiera, el adjudicatario del proceso autorizara la verificación de los documentos y de la información aportada para la celebración del contrato en el marco del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo conforme los procedimientos y políticas implementado por el Instituto.

CERTIFICACIÓN EXPRESA FRENTE A LA FORMULACIÓN DE LOS DOCUMENTOS PRECONTRACTUALES.

Dando cumplimiento a lo dispuesto en el Artículo 25 de la Ley 80 de 1993 y el Artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, certifico que el Estudio del Sector para determinar el valor estimado del contrato fue revisado a detalle, contrastando la información de precios con fuentes especializadas, estadísticas sectoriales y/o contratos de objeto similar previamente ejecutados. Se concluye que los valores unitarios definidos para efectos del seguimiento efectivo de la ejecución del contrato son acordes, adecuados y proporcionales a los precios promedio del mercado para este tipo de procesos, garantizando la suficiencia y la no desproporcionalidad en la determinación del valor contractual.

Certifico adicionalmente que las Condiciones Técnicas y las especificaciones del servicio requeridas, incorporadas en los Estudios Previos, han sido revisadas exhaustivamente y se ha verificado que: (i) Son estrictamente necesarias para el cabal cumplimiento del objeto a contratar. (ii) Son adecuadas, razonables y proporcionales a la magnitud, complejidad y naturaleza de la consultoría requerida, y, fundamentalmente, (iii) No incorporan requisitos o exigencias que restrinjan o limiten de forma injustificada la concurrencia o pluralidad de oferentes, promoviendo la competencia en el proceso de selección, en desarrollo del principio de selección objetiva.

Con base en lo anterior, se da por validado técnica y económicamente el componente de valores y condiciones técnicas de los Estudios Previos, sirviendo el presente estudio previo como soporte para la continuación de la etapa precontractual.

Realizado en Manizales, a los veinticuatro (24) días del mes de diciembre de dos mil veinticinco (2025).

JOHN JAIRO GIRALDO VILLA
Profesional Especializado Sistemas
INFI

Proyectó: Valentina Gálvez Carvajal- abogada contratista- apoyo al área de sistemas