20261305509233

DESCRIPCIÓN DE LA NECESIDAD QUE LA ENTIDAD PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN.

El Decreto 3573 del veintisiete (27) de septiembre 2011 creó la Autoridad Nacional de Licencias Ambientales – ANLA, como una Unidad Administrativa Especial del orden nacional, con autonomía administrativa y financiera, sin personería jurídica, la cual tiene por objeto garantizar que los proyectos, obras o actividades sujetos de licenciamiento, permiso o trámite ambiental cumplan con la normativa ambiental, de tal manera que contribuyan al desarrollo sostenible del País.

En concordancia con lo anterior y en cumplimiento de lo dispuesto en el Decreto 3573 de 2011 y el artículo 2.2.2.3.2.2 del Decreto 1076 de 2015, la ANLA tiene a su cargo la gestión de los proyectos que requieren licenciamiento ambiental. Dicho artículo, modificado por el artículo 2 del Decreto 852 del 5 de julio de 2024,[1] establece los sectores y, de estos, los proyectos, obras o actividades sobre los cuales la Autoridad Nacional de Licencias Ambientales tendrá la competencia exclusiva para otorgar o negar la licencia ambiental.

La ANLA tiene a su cargo la evaluación de proyectos para el otorgamiento o negación de licencias ambientales, así como el seguimiento de los ya licenciados, verificando el cumplimiento de las condiciones establecidas y de las medidas de prevención, mitigación, corrección, compensación y manejo de impactos ambientales. Esta labor constituye una función pública esencial para el desarrollo económico y sostenible del país, al garantizar que los proyectos, obras o actividades sujetos a licenciamiento, permiso o trámite ambiental cumplan la normativa ambiental, de carácter obligatorio y no susceptible de transacción o renuncia por parte de autoridades o particulares.

Las funciones de la ANLA son de gran relevancia para el desarrollo sostenible del país, por lo que las solicitudes de licenciamiento, permisos y trámites ambientales deben gestionarse con agilidad, rigor técnico y personal experto que apoye los procesos de evaluación y seguimiento. Esto contribuye a la mejora continua de la entidad, a la unificación de criterios y a brindar respuestas oportunas y efectivas a los usuarios.

De otra parte, el Gobierno Nacional expidió el Decreto No 376 del 11 de marzo de 2020 “Por el cual se modifica la estructura de Autoridad Nacional de Licencias Ambientales - ANLA” y estableció la siguiente estructura para el cumplimiento de su objeto y funciones:

[1] *"Por el cual se modifican los artículos 2.2.2.31.1, 2.2.2.3.2.2 Y 2.2.2.3.2.3 del Decreto 1076 de 2015, en relación con las competencias para otorgar la licencia ambiental a los proyectos de exploración y uso de fuentes de energía alternativa virtualmente contaminantes y se toman otras determinaciones*

1. Despacho del Director General
1.1 Oficina de Control Interno
1.2 Oficina de Control Disciplinario Interno
1.3 Oficina de Tecnología de la Información
1.4 Oficina Asesora Jurídica
1.5 Oficina Asesora Planeación
2. Subdirección Mecanismos de Participación Ciudadana Ambiental
3. Subdirección de Evaluación de Licencias Ambientales
4. Subdirección de Seguimiento de Licencias Ambientales
5. Subdirección de Instrumentos, Permisos y Trámites Ambientales
6. Subdirección Administrativa y Financiera

Que el artículo 5 del citado Decreto, establece como funciones a cargo de la ***Oficina de Tecnologías de la Información - OTI***, entre otras las siguientes:

> ***(...)***
>
> *2. Desarrollar, administrar, mantener y actualizar los sistemas de información de la Autoridad Nacional de Licencias Ambientales – ANLA.*
>
> *3. Liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información y las Comunicaciones -TIC del Estado.*
>
> *4. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad, en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad, seguridad y gestión de las Tecnologías de la Información y las Comunicaciones - TIC.*
>
> *(...)7. Impartir lineamientos tecnológicos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información de la entidad y la interoperabilidad de los sistemas que la soportan, así como el intercambio permanente de información.*
>
> *(...)"*

En relación con las anteriores funciones, es importante señalar que con el presente proceso, se da cumplimiento a lo establecido en el numeral 7 del Decreto mencionado, toda vez que ADQUIRIR EL LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA

LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION) PARA USUARIOS, APLICACIONES Y REDES, ASÍ COMO SU IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO, es necesario para garantizar la seguridad de la información de la Entidad.

De otra parte, mediante el artículo 3 de la Resolución 000968 de 22 de mayo de 2025, se crearon los siguientes Grupos Internos de Trabajo en la Oficina de Tecnologías de la Información de la Autoridad Nacional de Licencias Ambientales ANLA:

1. Grupo de Asuntos Geoespaciales.
2. Grupo de Sistemas de Información.
3. Grupo de Infraestructura Tecnológica.
4. Grupo de Arquitectura Institucional TI e Inteligencia Artificial.

Las funciones de los Grupos mencionados se encuentran establecidas en los Artículos 4,5, 6 y 7 de la citada Resolución.

PLAN NACIONAL DE DESARROLLO

En el marco de las políticas nacionales orientadas al fortalecimiento de la transformación digital, la seguridad y la confianza digital, y la modernización de las capacidades tecnológicas de las entidades públicas, resulta necesario que la Autoridad Nacional de Licencias Ambientales (ANLA), a través de la Oficina de Tecnologías de la Información, fortalezca sus mecanismos de protección de la infraestructura tecnológica, los sistemas de información y los activos de información institucionales, mediante la implementación de soluciones tecnológicas que permitan gestionar de manera segura, controlada y trazable el acceso a los recursos tecnológicos de la Entidad.

Esta necesidad se encuentra alineada con el Plan Nacional de Desarrollo 2022-2026 "Colombia, Potencia Mundial de la Vida", adoptado mediante la Ley 2294 de 2023, particularmente con lo establecido en su artículo 143, denominado "Transformación digital como motor de oportunidades e igualdad", que contempla, entre otros aspectos, el fortalecimiento del Gobierno Digital y la promoción de un entorno digital seguro que genere confianza en el uso y apropiación de las tecnologías de la información y las

comunicaciones. En este sentido, el fortalecimiento de los mecanismos de seguridad de acceso a los sistemas, aplicaciones y servicios tecnológicos institucionales constituye un elemento habilitador para avanzar en la transformación digital de la ANLA, garantizando que la adopción y utilización de tecnologías digitales se desarrolle bajo condiciones adecuadas de seguridad, disponibilidad y protección de la información.

De igual manera, las Bases del Plan Nacional de Desarrollo contemplan, dentro de la transformación de Seguridad Humana y Justicia Social, el componente de "Seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas", en el cual se reconoce la importancia de fortalecer las capacidades institucionales para prevenir, gestionar y responder ante amenazas digitales, proteger la información de las entidades gubernamentales, salvaguardar sus infraestructuras tecnológicas y garantizar la continuidad en la prestación de los servicios públicos en entornos digitales.

En concordancia con lo anterior, y teniendo en cuenta la evolución de las amenazas cibernéticas, la diversificación de los mecanismos de acceso a los recursos tecnológicos y la necesidad de proteger los sistemas de información institucionales frente a accesos no autorizados, se identifica la necesidad de adquirir e implementar una herramienta de seguridad basada en el modelo **Zero Trust Network Access (ZTNA)**, que permita fortalecer los controles de acceso a las aplicaciones, sistemas y servicios tecnológicos de la ANLA, bajo el principio de que ningún usuario, dispositivo o conexión debe considerarse confiable por defecto, independientemente de su ubicación o de que se encuentre dentro o fuera de la infraestructura tecnológica institucional.

La implementación de esta solución permitirá evolucionar hacia un esquema de acceso seguro basado en la verificación continua de la identidad de los usuarios, la validación del estado de seguridad de los dispositivos, la aplicación de políticas de acceso de mínimo privilegio y la autorización específica para acceder únicamente a los recursos tecnológicos que correspondan a las funciones y responsabilidades de cada usuario. De esta manera, se busca reducir la superficie de exposición de la infraestructura institucional, limitar los riesgos asociados con el movimiento lateral de posibles atacantes, disminuir la dependencia de esquemas tradicionales de acceso remoto basados exclusivamente en la conectividad a redes privadas virtuales (VPN) y fortalecer la capacidad de prevención frente a incidentes de seguridad digital.

Así mismo, la solución contribuirá a fortalecer la protección de la información institucional, incluyendo aquella de carácter reservado, clasificado y los datos personales que sean objeto de tratamiento por parte de la Entidad, mediante mecanismos de autenticación,

autorización, segmentación de acceso, monitoreo y trazabilidad de las conexiones. Lo anterior permitirá mejorar la gestión de los riesgos de seguridad de la información y fortalecer los controles orientados a preservar la confidencialidad, integridad y disponibilidad de los activos de información de la ANLA.

Esta iniciativa también guarda correspondencia con el Modelo de Seguridad y Privacidad de la Información (MSPI), adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante la Resolución 500 de 2021 y sus lineamientos vigentes, en cuanto promueve la implementación de controles y buenas prácticas para la gestión de la seguridad de la información en las entidades públicas, así como con los objetivos de la Política de Gobierno Digital relacionados con el uso seguro y confiable de las tecnologías de la información.

En consecuencia, la contratación de una herramienta de seguridad ZTNA constituye una medida tecnológica orientada a fortalecer la postura de ciberseguridad de la ANLA, mejorar el control y la gobernanza de los accesos a los recursos tecnológicos institucionales, mitigar los riesgos derivados de las amenazas digitales y proporcionar condiciones de seguridad para la operación de los servicios tecnológicos y el desarrollo de las iniciativas de transformación digital de la Entidad.

Por lo anterior, se considera técnica y jurídicamente justificada la contratación de una solución tecnológica de Zero Trust Network Access (ZTNA), que permita fortalecer las capacidades institucionales de seguridad digital, proteger los activos de información y contribuir al cumplimiento de los objetivos de transformación digital, seguridad y confianza digital establecidos en el Plan Nacional de Desarrollo 2022-2026 y demás políticas y lineamientos aplicables a las entidades públicas.

POLÍTICA DE GOBIERNO DIGITAL.

La entidad debe dar cumplimiento al Decreto 767 de 2022, el cual establece la “Política de Gobierno Digital como instrumento gubernamental del orden nacional que propende por la transformación digital pública”[2], y se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo, entendidos así:

[2] Política de Gobierno Digital link: Política de Gobierno Digital

"***1. Gobernanza**: Los sujetos obligados implementarán la Política de Gobierno Digital bajo un modelo de gobernanza basado en el relacionamiento entre el orden nacional y territorial, y el nivel central y descentralizado, que involucre a los grupos de interés en la toma de decisiones y defina los focos estratégicos de acción y la distribución eficiente de los recursos disponibles, procurando una gestión pública colaborativa y ágil.*

***2. Innovación Pública Digital**: Los sujetos obligados implementarán la Política de Gobierno Digital con un enfoque transversal basado en el relacionamiento con los Grupos de Interés, que genere valor público a través de la introducción de soluciones novedosas y creativas y que hagan uso de las Tecnologías de la Información y las Comunicaciones y de metodologías de innovación, para resolver problemáticas públicas desde una perspectiva centrada en los ciudadanos y en general, los habitantes del territorio nacional.*

Con el fin de fortalecer los procesos de innovación pública digital, los sujetos obligados promoverán la implementación de mecanismos de compra pública que faciliten al Estado la adquisición de bienes o servicios de base tecnológica que den respuesta a desafíos públicos respecto de los cuales no se encuentra una solución en el mercado o, si la hay, requiera ajustes o mejoras. Asimismo, promoverán la adopción de tecnologías basadas en software libre o código abierto, sin perjuicio de la inversión en tecnologías cerradas.

***3. Habilitadores:** Los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores:*

***3.1. Arquitectura:** Este habilitador busca que los sujetos obligados desarrollen capacidades para el fortalecimiento institucional implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de proyectos con componentes de Tecnologías de la Información.*

Los sujetos obligados deberán articular su orientación estratégica, su modelo de gestión, su plan de transformación digital, y su estrategia de Tecnologías de información y las Comunicaciones, con el objetivo de dar cumplimiento a la Política de Gobierno Digital.

3.2. Seguridad y Privacidad de la Información: Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los

lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

3.3. Cultura y Apropiación: *Este habilitador busca desarrollar las capacidades de los sujetos obligados a la Política de Gobierno Digital y los Grupos de Interés, requeridas para el acceso, uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones. Se promoverá el uso y apropiación de estas entre las personas en situación de discapacidad y se fomentará la inclusión con enfoque diferencial.*

3.4. Servicios Ciudadanos Digitales: *Este habilitador busca desarrollar, mediante soluciones tecnológicas, las capacidades de los sujetos obligados a la Política de Gobierno Digital para mejorar la interacción con la ciudadanía y garantizar su derecho a la utilización de medios digitales ante la administración pública.*

4. Líneas de Acción: *Los sujetos obligados ejecutarán acciones orientadas a desarrollar servicios y procesos inteligentes, tomar decisiones basadas en datos y consolidar un Estado abierto, con el fin de articular las Iniciativas Dinamizadoras de la Política de Gobierno Digital. Estas Líneas de Acción se materializarán en las sedes electrónicas de cada uno de los sujetos obligados, siguiendo los estándares señalados para tal fin. En el proceso de registro de los nombres de dominio requeridos para la implementación de la Política de Gobierno Digital, se deberá realizar la articulación con el Ministerio de Tecnologías de la Información y las Comunicaciones, acorde con la normativa que regula la materia.*

4.1. Servicios y Procesos Inteligentes: *Esta línea de acción busca que los sujetos obligados desarrollen servicios y procesos digitales, automatizados, accesibles, adaptativos y basados en criterios de calidad, a partir del entendimiento de las necesidades del usuario y su experiencia, implementando esquemas de atención proactiva y el uso de tecnologías emergentes.*

4.2. Decisiones Basadas en Datos: *Esta línea de acción busca promover el desarrollo económico y social del país impulsado por datos, entendiéndolos como infraestructura y activos estratégicos, a través de mecanismos de gobernanza para el acceso, intercambio, reutilización y explotación de los datos, que den cumplimiento a las normas de protección*

y tratamiento de datos personales y permitan mejorar la toma de decisiones y la prestación de servicios de los sujetos obligados.

4.3. Estado Abierto: *Esta línea de acción busca promover la transparencia en la gestión pública con un enfoque de apertura por defecto, y el fortalecimiento de escenarios de diálogo que promuevan la confianza social e institucional, además la colaboración y la participación efectiva de los Grupos de Interés, para fortalecer la democracia y dar soluciones a problemas de interés público a través de prácticas innovadoras, sostenibles y soportadas en Tecnologías de la Información y las Comunicaciones.*

5. Iniciativas Dinamizadoras: *Comprende los Proyectos de Transformación Digital y las Estrategias de Ciudades y Territorios Inteligentes, a través de las cuales se materializan las Líneas de Acción, que permiten dar cumplimiento al objetivo de la Política de Gobierno Digital con la implementación de mecanismos de compra pública que promuevan la innovación pública digital.*

5.1. Proyectos de Transformación Digital: *Comprende aquellos proyectos que implementarán los sujetos obligados para aportar a la generación de valor público mediante el aprovechamiento de las capacidades que brindan el uso y la apropiación de las Tecnologías de la Información y las Comunicaciones y así alcanzar los objetivos estratégicos institucionales. Los proyectos de Transformación Digital deberán estar integrados al Plan Estratégico de Tecnología y Sistemas de Información (PETI).*

5.2. Estrategias de Ciudades y Territorios Inteligentes: *Las entidades territoriales podrán desarrollar estrategias de ciudades y territorios inteligentes, a través del uso de tecnologías de la información y las comunicaciones, como herramientas de transformación social, económica y ambiental de los territorios.*

Los elementos normativos antes vistos, se dimensionan de la siguiente manera:

Figura 1. Política de Gobierno Digital



Fuente: Gobierno Digital[3]

Vistos estos elementos, se encuentra que con el presente proceso de selección se desarrolla el **habilitador establecido el numeral 3.2 de la política de gobierno digital "*SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*"** por cuanto busca ***desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información***, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En este orden de ideas, estas disposiciones tienen como objetivo optimizar el funcionamiento de las entidades públicas y su interoperabilidad con otras entidades estatales y con la sociedad civil, a través del uso de las Tecnologías de la Información y las Comunicaciones, fortaleciendo sus competencias y las de sus servidores públicos, en temas relacionados con tecnologías de la información, como elementos generadores de valor en la gestión pública dirigidos en pro de beneficios sociales.

[3] Figura 1 https://gobiernodigital.mintic.gov.co/692/articles-237560_img_seccion.jpg

De otra parte, atendiendo a las funciones asignadas a esta dependencia y con el fin de dar cumplimiento al Decreto 767 del 2022 que establece los lineamientos generales de la política de gobierno digital, lineamientos que se encuentran ligados a los criterios del sistema de gestión de seguridad de la información propuesto en la estrategia de Gobierno Digital, la Oficina de Tecnologías de la Información ha venido adoptando medidas y mecanismos para preservar la integridad y disponibilidad de la información de la entidad, siendo esta hoy en día uno de los activos más importantes de la entidad. Que en el caso específico de la presente contratación está encaminada a evitar la fuga de información que se encuentre o no clasificada (información Pública Reservada, Pública Clasificada y Documentos en construcción acorde a la ley 1712 de 2014) tales como conceptos técnicos, expedientes y demás información misional de la entidad, que es quizás uno de los principales temores que afrontan las entidades.

Así mismo, se establece como propósito de la Política de Gobierno Digital el desarrollo de los siguientes componentes:

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.
- Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
- Tomar decisiones basadas en datos a partir del aumento el uso y aprovechamiento de la información.
- Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto
- Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.

Por lo anterior, el contrato a celebrar se encuentra asociado a los dos primeros componentes de la Política, así:

1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.

2. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

Lo mencionado, toda vez que, con el contrato a celebrar, se fortalecerá el sistema de seguridad de la información de la Entidad, al contar con el licenciamiento para la prevención de fuga de la información de la Entidad, lo que genera servicios digitales de confianza y procesos internos y seguros.

Así mismo, el artículo 6 de la Resolución 500 de 2021[4], expedida por la Ministra de Tecnologías de la Información y las Comunicaciones, establece que se deben determinar

[4] "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"

e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos, en virtud de lo anterior la oficina de Tecnologías de la Información, cuenta con una infraestructura de seguridad informática, que implica un alto nivel de complejidad en la administración, análisis y respuesta que se tiene frente a los diferentes frentes de seguridad informática, teniendo en cuenta que la Autoridad Nacional de Licencias Ambientales – ANLA cuenta con una política de Defensa en Profundidad, política que implica que varias herramientas de seguridad comparten funciones para que, en caso que alguna de estas sea vulnerada, otra capa de seguridad pueda monitorear, controlar o mitigar un ataque o falla. Lo mencionado, con el fin de establecer controles que garanticen la seguridad de la información de la Entidad.

PLAN ESTRATEGICO INSTITUCIONAL ANLA (2022-2030)

La **Línea Estratégica 3** del Plan Estratégico Institucional busca *"**Gestionar el conocimiento y garantizar el acceso a la información de los procesos de la autoridad para contribuir a la efectiva y oportuna toma de decisiones, a través de la innovación, las buenas prácticas y la transformación digital**"* prevé la generación de una cantidad importante de datos, información, ideas y experiencias que, en conjunto, se transforman en conocimiento.

Dentro de la citada línea estratégica se encuentra el **Objetivo Estratégico 6** el cual plantea "***Integrar y optimizar los sistemas de información de la autoridad, promoviendo su interoperabilidad y el flujo adecuado de la información***", y para alcanzar este objetivo se plantearon los siguientes objetivos de gestión:

1 OG - 07: Optimizar la infraestructura tecnológica de la Entidad
2 OG - 08: Fomentar el uso de nuevas tecnologías y su efectiva implementación al interior de la autoridad
3 OG - 09: Promover la gestión por procesos en la autoridad, mediante la implementación de herramientas y metodologías de vanguardia, con el fin de fortalecer la racionalización de trámites y la transformación digital en la autoridad.

Lo anterior, alineado con el presente proceso de contratación, ya que con la adquisición del licenciamiento para la prevención de fuga de información (DLP/ZTNA), se logra la optimización y el uso de esta tecnología para garantizar correctos monitoreos de seguridad y su respectivo control de acceso para la prestación de los servicios que ofrece la ANLA.

PLAN DE ACCIÓN INSTITUCIONAL- PAI PARA LA VIGENCIA 2026

Con e proceso de selección mediante la modalidad de abreviada por subasta inversa electrónica se pretende dar cumplimiento a los objetivos e indicadores establecidos en al Plan de Acción Institucional PAI en materia de Seguridad informática por la Oficina de Tecnologías de la Información así:

PROYECTO/FUENTE	OBJETIVO GENERAL	OBJETIVO ESPECIFICO	NOMBRE DEL INDICADOR	FORMULA INDICADOR	UNIDAD DE MEDIDA	META 2026
FORTALECIMIENTO DE LA GESTION INSTITUCIONAL Y TECNOLOGICA DE LA AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES EN EL TERRITORIO NACIONAL	Generar e implementar acciones estratégicas para la formulación de buenas prácticas y lineamientos que apoyen el adecuado funcionamiento, disponibilidad y usabilidad de los sistemas de información y la infraestructura tecnológica, a través de la formulación de Tecnologías de la Información - PETI, asegurando que el Sistema de Gestión de Seguridad de la	Reportar de manera acumulada, el número de procesos contractuales que se han adjudicado en el periodo reportado, con el objetivo de identificar oportunamente retrasos con respecto al avance esperado.	Procesos de adquisición de equipos de hardware y/o herramientas de software	Número de procesos de adquisición de equipos de hardware y/o herramientas de software adjudicados	NÚMERO	20

	Información (SGSI) es conforme con el estándar ISO/IEC 27001 y los requisitos aplicables de los grupos de valor, conforme a los lineamientos establecidos como oMGGTI, del marco de referencia de arquitectura empresarial MRAE, para la toma de decisiones, el mejoramiento del desempeño Institucional y la satisfacción de los grupos de interés.					

Fuente: SPGI – Listados de Indicadores

El cumplimiento de las metas establecidas en el Plan de Acción Institucional de la Oficina de Tecnologías de la Información de la ANLA implica que la gestión no pueda ser interrumpida, de tal manera que se realice la correcta planeación, ejecución y seguimiento de los proyectos tecnológicos de la Entidad.

En este contexto, la adquisición de licenciamiento (software) para prevenir la fuga de la información, aporta al cumplimiento del indicador, siendo esencial para garantizar la seguridad de la información.

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN (PETI)

Atendiendo a los lineamientos previstos en la Política de Gobierno Digital, en cumplimiento de lo dispuesto en el Manual de Gobierno Digital, el cual establece que: “La entidad debe identificar y documentar las necesidades de intercambio de información que se requieren y las entidades que proveen dicha información. Estas necesidades deben estar en el PETI.”, la entidad formuló el Plan Estratégico Integral de Tecnologías de la Información- PETI, el cual recoge las necesidades y oportunidades de mejoramiento de los interesados en lo relacionado con la gestión de TI para apoyar la estrategia y el modelo operativo de la organización apoyados en las definiciones de la Política de Gobierno Digital.

Así pues, dentro de este plan se busca asegurar la incorporación de mecanismos de seguridad de la información en cada uno de los dominios, esto por cuanto: “Toda la información que se intercambie en la integración e interoperabilidad de la ANLA debe estar alineada con los controles y medidas que aseguren que la información esté protegida, preservada y se mantenga privada. Esto es, generar un entorno seguro y de confianza que permita que los usuarios y la ANLA transmitan información teniendo una sensación positiva frente a que se no se van a violentar sus

intereses, se va a cuidar la privacidad de la información y se va a respetar la normativa aplicable en cada intercambio de información. Adicionalmente, se debe dotar de medidas especiales de seguridad (evitando el uso no autorizado de la información y asegurando su integridad, disponibilidad, confidencialidad y resguardo) a toda aquella información y datos que sean de los ciudadanos, las empresas o las entidades públicas y cuya pérdida o alteración signifique un riesgo para dichos usuarios.”[5].

De igual manera en articulación con la Política de Gobierno Digital, en el Plan en comentó la entidad estableció los siguientes objetivos de seguridad digital:

“Objetivo Transformacional: Fortalecer la cultura de seguridad de la información de los usuarios internos de la ANLA a través del uso y la apropiación de buenas prácticas, así como la implementación de medidas preventivas y de mitigación en el marco de la gestión de riesgos digitales.

Objetivo Operativo: Implementar los productos asociados al Plan de Seguridad y Privacidad, así como el Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información de la ANLA las acciones, productos esperados, fechas de inicio y finalización de la implementación de los productos del Plan de Seguridad y Privacidad de la Información,

[5] Plan Estratégico Integral de Tecnologías de la Información- PETI: https://www.anla.gov.co/oficina-de-planeacion/plan-estrategico-de-las-tics/vigencias-peti

así como la política MIPG de Seguridad Digital y el Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información de la ANLA. El plan de seguridad y privacidad de la información contenido en el Plan de seguridad

digital busca establecer las acciones necesarias al buen uso y a la apropiación de los usuarios de los lineamientos de la información y privacidad de la información, así mismo establece las acciones para una correcta administración de las herramientas de seguridad informática para el control, monitoreo y gestión de las amenazas y vulnerabilidades de hardware/software con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información institucional).”[6]

Así las cosas, dentro de los motivadores estratégicos a nivel entidad que da línea en la orientación y alineación a la Estrategia de Tecnologías de la Información (PETI) tenemos el Modelo Integrado de Planeación y Gestión (MIPG) en el cual se encuentra el mapa de procesos de la ANLA, ubicando dentro de los procesos estratégicos el identificado como ***Direccionamiento Tecnológico*** como se aprecia en la siguiente imagen, en el cual se estructura el esquema de seguridad de la entidad:

[6] Ibidem



Fuente: Sistema de Planeación y Gestión -SPGI – GESPRO

Finalmente, adquirir el licenciamiento de una solución avanzada de seguridad para la prevención de fuga de información y control de acceso (Zero Trust Network Access y Data Loss Prevention) para usuarios, aplicaciones y redes y de la suscripción del soporte y mantenimiento, es crucial para la política de seguridad y privacidad de la información, porque permite asegurar la adecuada utilización de la tecnología, asegurar la integridad, confiabilidad y disponibilidad de los activos de información, de los servicios ofrecidos a los ciudadanos y empresas que solicitan la

gestión de los tramites ambientales, a través de la prevención de fuga de la información

Por otro lado, el Plan Estratégico de Tecnologías de la Información (PETI) incorpora los componentes estructurales asociados a la conformación de los grupos internos de trabajo de la Oficina de Tecnologías de la Información (OTI), en línea con las funciones establecidas en el Decreto 376 de 2020.

También incorpora los componentes transversales de transformación digital, adquisiciones de TI, uso y apropiación, administración de riesgos y seguridad y privacidad de la información, dentro de los cuales encontramos los siguientes que fortalecen la seguridad de la información de la entidad:

COMPONENTE ESTRUCTURAL

Dominio de Arquitectura Seguridad de la Información

- ✓ Desarrollar las acciones propuestas en pro de fortalecer la arquitectura de seguridad generando lineamientos de gestión de la seguridad y privacidad de la información.
- ✓ Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los colaboradores de la ANLA.

COMPONENTES TRANSVERSALES

Seguridad Digital

- ✓ Fortalecer la cultura de seguridad de la información de los usuarios internos de la ANLA a través de la implementación de medidas preventivas y de mitigación en el marco de la gestión de riesgos digitales.

Seguridad y Privacidad de la información

- ✓ Implementar los productos asociados al Plan de Seguridad y Privacidad, así como el Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información de la ANLA.
- ✓ Plan integrado del Decreto 612

Tratamiento de Riesgos

- ✓ Disminuir la probabilidad de ocurrencia y el impacto de los riesgos de gestión de competencia de la Oficina de Tecnologías de la Información.
- ✓ El plan de tratamiento de riesgos contenido en el Plan de seguridad digital busca establecer la adecuada gestión y administración de riesgos institucionales, de acuerdo con los lineamientos definidos por MINTIC y DAFP para reducir la

probabilidad e impacto de los riesgos identificados en caso de una eventualidad materialización.

- ✓ Plan integrado del Decreto 612[7]

Política Del Sistema Integrado de Gestión

"La Política del Sistema Integrado de Gestión[8] es la declaración general que representa la posición de la Autoridad Nacional de Licencias Ambientales con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la implementación del Subsistema de Gestión de Seguridad de la Información por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

A continuación, se establecen los ***lineamientos de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de ANLA****:*

- *Definir, implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información.*
- *Definir, compartir y publicar las responsabilidades frente a la seguridad de la información de acuerdo con el alcance de cada uno de los funcionarios, contratistas o terceros.*
- *Proteger los activos críticos de información y la información creada, procesada, transmitida o resguardada por procesos internos.*
- *Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.*
- *Controlar la operación de los procesos internos garantizando la seguridad de los recursos tecnológicos y las redes de datos.*
- *Implementar controles de acuerdo con la clasificación de la información, de su propiedad o uso, además de controles de acceso a la información, sistemas y recursos de red.*
- *Garantizar que la seguridad de la información sea parte integral del ciclo de vida de los sistemas de información.*
- *Establecer un plan de formación y mejoramiento del modelo de seguridad de la información, para lograr una adecuada gestión de los eventos e incidentes de seguridad y las vulnerabilidades asociadas con los sistemas de información.*

[7] https://www.anla.gov.co/images/documentos/planes/peti/2025-04-28-anla-PETI-2025-v2.pdf
[8] Política del Sistema Integrado de Gestión Link: https://gespro.anla.gov.co:4434/reportes_pdf/vista_publicada?vs=1749218007

- *Garantizar la disponibilidad de sus procesos críticos y la continuidad de la operación.*
- *Mejorar la eficiencia y la eficacia de los procesos de privacidad y seguridad de la información necesarios para la prestación de servicios.*
- *Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en materia de privacidad y seguridad de la información.*
- *Disponer de personal competente para el cumplimiento de las acciones de privacidad y seguridad de la información.*

El incumplimiento a la presente política de privacidad y seguridad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al gobierno nacional en cuanto a seguridad y privacidad de la información. Igualmente, ANLA tomará las medidas pertinentes para proteger la información.[9]"

Sistema de Gestión de Seguridad de la Información SGSI Alineado a la Norma ISO 27001:2022

La adopción de la norma ISO/IEC 27001, permite a las organizaciones fortalecer su sistema de gestión de la seguridad de la información, mediante la identificación y tratamiento proactivo de los riesgos asociados a la protección, manejo y confidencialidad de los datos institucionales. En este sentido, la contratación de LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION), resulta fundamental para garantizar el cumplimiento de las políticas de seguridad, controlando el flujo de información sensible y evitando su exposición no autorizada.

La contratación de estos licenciamientos contribuye al fortalecimiento de la infraestructura tecnológica y al aseguramiento de la información institucional, en coherencia con los lineamientos de la ISO/IEC 27001 y las buenas prácticas en materia de gestión de seguridad de la información.

La Entidad cuenta con el Sistema de Gestión de Seguridad de la Información SGSI alineado al cumplimiento normativo ISO 27001:2022 como una herramienta clave para la gestión de riesgos, la resiliencia cibernética y la excelencia operativa.

[9] POLÍTICA (ESTRUCTURADA) GENERAL DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN: https://www.anla.gov.co/images/documentos/politicas/oti/politica-de-privacidad-y-seguridad-de-la-informacion-anla.pdf

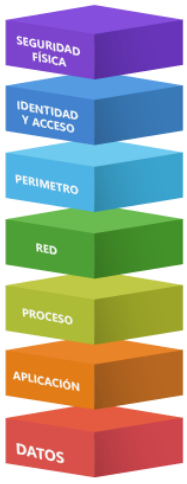
Por lo anterior, el control 8.20 “Seguridad de la Red” de la ISO 27001:2022 es un componente clave de la Política de Seguridad y Privacidad de la Información de la ANLA, siendo un control preventivo y de detección de doble propósito al asegurar que la actividad de la red esté adecuadamente registrada, segmentada y llevada a cabo por personal autorizado, implementando controles que faciliten la transferencia de datos a través de todas las redes relevantes (incluidas las redes de terceros) y garantizar el funcionamiento continuo de todas las aplicaciones conectadas.

Por lo anterior, el presente proceso pretende dar cumplimiento a la implementación de este control.

SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA DE LA ANLA

Actualmente la Autoridad Nacional de Licencias Ambientales – ANLA, dispone de una infraestructura de seguridad informática compuesta por diversas soluciones diseñadas para proteger sus redes y sistemas. Esta infraestructura incluye:

Figura 3
Capas de Seguridad



Protección mediante un **enfoque por capas defensivas**:

- Seguridad **física**, como limitar el acceso solo para el personal autorizado.*
- Seguridad de **identidad y acceso**, que permite controlar el acceso a la infraestructura y al control de cambios
- **Seguridad perimetral**, incluida la protección frente a ataques de denegación de servicio Distributido (DDoS) para filtrar los ataques a gran escala antes de que puedan producir una denegación de servicio para los usuarios.
- **La Seguridad de la red** limita la comunicación entre los recursos mediante la segmentación y los controles de acceso.
- La capa de **proceso** protege el acceso a maquinas virtuales, locales o en la nube, al cerrar puertos.
- La capa de **aplicación** garantiza que las aplicaciones sean seguras y estén libres de vulnerabilidades de Seguridad
- La Seguridad de la capa de **datos** controla el acceso a los datos empresariales y de clientes, mientras que el cifrado protege esos datos.

Fuente: Seguridad en Profundidad[10]

Para la prevención:

- Soluciones antimalware (antivirus): Protegen los equipos de cómputo y servidores contra ataques de malware, como virus y otros tipos de software malicioso como Ransomware
- Correlacionador de eventos que monitorea los logs de todas las aplicaciones y servicios y frente a un comportamiento anormal este genera un alertamiento.
- Filtrado web para proteger la información en internet.
- Pruebas de Ingeniería social para identificar fallas humanas en los procesos del día a día.
- Pruebas de Ethical Hacking para identificar vulnerabilidades de los sistemas de información que permita tomar acciones preventivas.

Para el Control:

- Firewall de red que controla el acceso a la red interna y a la red pública de la ANLA.
- Herramienta de Acceso a la Red de Cero Confianza (ZTNA y DLP) que protege el acceso a la información
- Firewall de Aplicaciones Web para proteger restringir el acceso a las aplicaciones y servicios web.
- Solución de Protección ante ataques de denegación de servicio (DDOS), el cual bloquea solicitudes de acceso cuando evidencia ataques masivos de trafico de red.
- Herramienta local para la protección de puertos periféricos y archivos ejecutables.

Para el Monitoreo:

[10] Figura 3 Defensa en Profundidad disponible en: https://www.encamina.com/seguridad-en-microsoft-365-y-azure/

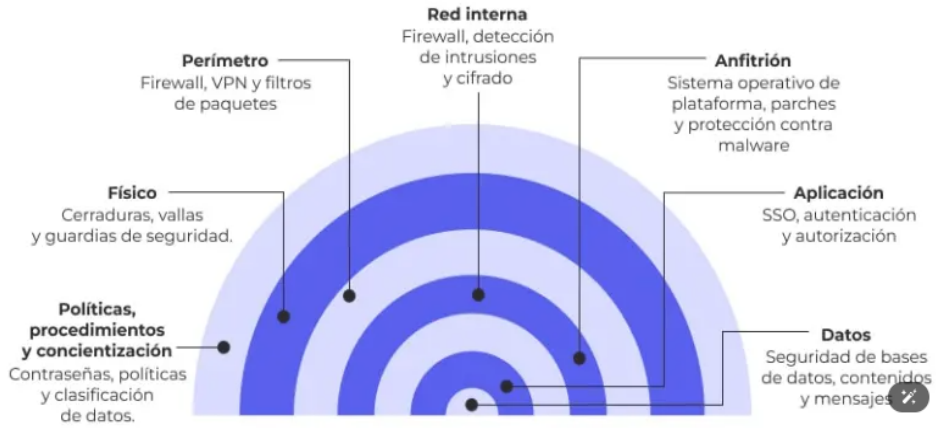
- Correlacionador de eventos que monitorea los logs de todas las aplicaciones y servicios y frente a un comportamiento anormal este genera un alertamiento.
- Herramienta de análisis de vulnerabilidades que permite tomar acciones frente a nuevas vulnerabilidades informáticas.

Estas soluciones trabajan en conjunto para asegurar la protección integral de la información y los recursos tecnológicos de la entidad, garantizando su seguridad frente a una amplia gama de amenazas.

Esta perspectiva de la seguridad informática se definió con el objetivo de fortalecer las defensas tecnológicas de la entidad. Incluye la adquisición e implementación de herramientas avanzadas de hardware y software que previenen, monitorean y controlan una amplia variedad de amenazas cibernéticas, tales como ataques informáticos, fugas de información y accesos no autorizados a los sistemas. Para lograr una protección integral, se ha establecido una política de seguridad multicapa, conocida como **Defensa en Profundidad**, que actúa como un blindaje robusto, asegurando que la entidad esté protegida en múltiples frentes. Esta estrategia no solo refuerza la seguridad en los puntos de acceso, sino que también proporciona un monitoreo constante y una respuesta proactiva ante posibles incidentes, garantizando así la continuidad operativa y la integridad de los datos frente a cualquier amenaza.

CAPAS DE DEFENSA EN PROFUNDIDAD

SEGURIDAD DE LA INFORMACIÓN



Fuente: wallarm.com[11]

DEFINICIONES:

Para dar mayor entendimiento a los términos técnicos empleados en este documento, se da el significado de los mismos a continuación:

Activos de Información: Es cualquier información o elemento relacionado con el tratamiento de dicha información que tengan valor para la organización de tal manera que difiere a la definición de registros de activos de información dada por la ley 1712 del 2014.

Herramientas Informáticas: Son un conjunto de programas, aplicaciones o, simplemente instrucciones, que al utilizarlas permitirán al usuario realizar un trabajo determinado de la mejor manera posible en algún dispositivo informático.

Fuga de Información: Por sus siglas en ingles DLP – Data Loss Prevention se refiere al incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma (tanto todos como un grupo reducido). Se trata de un incidente que puede ser tanto interno como externo, y a la vez intencional o no.

ZTNA: El Acceso a la red Zero Trust (ZTNA) es la tecnología que permite implementar un modelo de seguridad Zero Trust. "Zero Trust", un modelo de seguridad informática que asume que las amenazas están presentes tanto dentro como fuera de una red. En consecuencia, Zero Trust requiere una verificación estricta para cada usuario y para cada dispositivo antes de autorizarles el acceso a los recursos internos.

REQUERIMIENTO DE LA ANLA RESPECTO DE UN SOFTWARE ESPECIALIZADO PARA PREVENIR LA FUGA DE INFORMACIÓN

Contar con licencias de DLP (Prevención de Fuga de Información) y ZTNA (Acceso a la Red de Confianza Cero) responde a una necesidad técnica crítica y obligatoria para

[11] https://i0.wp.com/lab.wallarm.com/wp-content/uploads/2024/06/264.2-min.jpg?w=770&ssl=1

garantizar la seguridad digital, la mitigación de riesgos de ciberseguridad y la protección de los activos de información estratégica e institucional de la ANLA.

Lo anterior, igualmente encuentra sustento en la aplicación de la siguiente normativa, entre otras, relacionada con el control de información:

- **Ley 1581 de 2012 (Protección de Datos Personales):** Obliga a proteger los datos sensibles de los ciudadanos. No evitar una fuga puede acarrear sanciones de la Superintendencia de Industria y Comercio (SIC) y responsabilidad disciplinaria.
- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Liderado por el MinTIC, exige implementar controles técnicos para asegurar la confidencialidad, integridad y disponibilidad de la información pública.

Con el propósito de asegurar la adecuada utilización de la tecnología, asegurar la integridad, confiabilidad y disponibilidad de los activos de información, de los servicios ofrecidos a los ciudadanos y empresas que solicitan la gestión de los tramites ambientales, a través de la prevención de fuga de la información que de acuerdo a las estadísticas en Latinoamérica es uno de los incidentes de seguridad que se presenta con mayor frecuencia, los incidentes relacionados a la fuga de información en la ANLA son gestionados, monitoreados y controlados por el equipo de trabajo de Seguridad de la Información el cual pertenece al Despacho de la Oficina de Tecnologías de la Información.

Figura 4Informe de Ciberseguridad 2026[12]



De acuerdo con el Informe de Ciberseguridad Empresarial Colombia 2026, se evidencia más de 62.299 denuncias por delitos informáticos en el 2025, un costo promedio de una brecha de 4,99 Millones de dólares, un 62% de brechas de seguridad por factores humanos, y un 31% de brechas por vulnerabilidades tecnológicas. Asi mismo de acuerdo con varias empresas de seguridad y tecnología las Empresas en Colombia son las más atacadas por semana y el ransomware sigue su ascenso, “durante septiembre de 2025, una de cada 54 interacciones o “prompts” realizados desde redes corporativas presentó un alto riesgo de exposición de datos sensibles, un fenómeno que afecta ya al 91 % de las organizaciones que utilizan regularmente herramientas de GenAI. Además, el 15 % de los prompts

[12] Informe de Ciberseguridad Colombia 2026: Datos y Tendencias: https://star-ti.com/informe-ciberseguridad-colombia-2026/#hallazgos

analizados contenían información potencialmente confidencial, como datos de clientes, fragmentos de código propietario o comunicaciones internas. Estos hallazgos ponen de manifiesto la necesidad urgente de establecer medidas de gobernanza y control de seguridad en el uso de la IA Generativa. Sin protecciones adecuadas, los beneficios de productividad que ofrece esta tecnología pueden verse eclipsados por riesgos significativos para la seguridad de los datos"[13].

Por lo que la ANLA requiere del licenciamiento de un software especializado que cumpla con las leyes colombianas en cuanto a legalidad de software y que formen parte de la operación continua de la entidad, de conformidad con lo estipulado en las leyes vigentes sobre propiedad intelectual y de derechos de autor.

Lo anterior, permite a la Entidad contar con las licencias de un software especializado que permita minimizar en gran medida el riesgo ante la materialización de fugas de información que pudiesen llegar a perjudicar la toma de decisiones de la entidad, tanto administrativa como misionales de seguimiento y evaluación de licenciamientos ambientales, de forma que este tipo de herramientas permita el monitoreo y control de acceso a los documentos sensibles.

Por lo mencionado, la entidad tiene la necesidad de adquirir las licencias para el uso de un software especializado (DLP/ZTNA) que permita el control de **fuga de información** en cualquier parte en que se encuentren los colaboradores (Funcionarios y contratistas), con la particularidad que esa detección de fuga de información no esté atada a la búsqueda de palabras clave sino también al tipo de contenido, destinatario, clasificación, etiquetado de la información, y a los roles de quienes manejan la información institucional.

¿Qué permite el Software especializado DLP?

El software especializado DLP (Prevención de Fuga de la Información), permite detectar, analizar y bloquear, si el dato es sensible, alertar y educar al usuario sobre el riesgo de una fuga de información; del mismo modo, tiene la capacidad de identificar en tiempo real intentos de fuga de la información a través de varias aplicaciones y medir el nivel de riesgo

[13] Empresas en Colombia son las más atacadas por semana en septiembre y el ransomware sigue su ascenso: https://www.pantallazosnoticias.com.co/mpresas-en-colombia-son-las-mas-atacadas-por-semana-en-septiembre-y-el-ransomware-sigue-su-ascenso/

de cada una de ellas, controlar información en tránsito, y tomar acciones en tiempo real para aplicaciones administrativas y no administradas.

Este tipo de licenciamiento de software especializado recae en cabeza de la entidad, permitiendo de esta manera gestionar la asignación y retiro de las mismas en cualquier momento, a cualquier colaborador de la misma a través de la consola de administración de software especializado.

Contar con una solución de ZTNA integrada con DLP es hoy una necesidad crítica para la Entidad debido a que ZTNA por sí solo controla *quién* entra a la red y a qué aplicaciones accede, pero no tiene visibilidad sobre *qué hacen* los usuarios con la información una vez que se les permite el acceso.

La integración de Zero Trust Network Access (ZTNA) y Data Loss Prevention (DLP) cierra esta brecha de seguridad mediante la combinación de dos pilares esenciales:

Tecnología	Función Principal	Limitación Sin Integración
ZTNA	Autentica la identidad, evalúa el estado del dispositivo y autoriza el acceso según el contexto (mínimo privilegio).	Es ciego al movimiento del dato; un usuario autorizado legítimamente podría extraer archivos confidenciales.
DLP	Descubre, monitorea y bloquea la fuga o exfiltración de información sensible (PII, datos financieros, propiedad intelectual).	No controla el perímetro ni el contexto de conexión del usuario de manera nativa.

Beneficios clave de la integración:

- Control del ciclo de vida del dato: No solo se valida al usuario de manera continua, sino que se inspecciona en tiempo real si el contenido transferido viola las políticas de cumplimiento o seguridad corporativa.

- Visibilidad unificada en entornos híbridos: Permite aplicar las mismas reglas de protección de datos tanto a usuarios remotos como presenciales dentro de una arquitectura SASE (Secure Access Service Edge).

- Reducción de riesgos internos: Evita que credenciales legítimas robadas o empleados malintencionados descarguen masivamente bases de datos corporativas hacia dispositivos no gestionados.

En la **vigencia 2025**, se suscribió el **Contrato de Licenciamiento No 1583-2025**, con el objeto de ADQUIRIR EL LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION) PARA USUARIOS, APLICACIONES Y REDES, ASÍ COMO SU IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO, con el fin de identificar la información sensible no solo por su clasificación, sino que también por sus características, su contenido, su uso, entre otros factores; siendo el DLP una herramienta de control que permitirá monitorear y controlar los flujos de información en favor de la transparencia en los procesos de la entidad. Por lo cual, teniendo en cuenta que el licenciamiento con su soporte vence el 25 de diciembre de 2025, se hace necesaria la contratación de su adquisición.

¿Qué permite el Software especializado ZTNA?

El modelo Zero Trust se basa en una autenticación y autorización sólidas de cada dispositivo y persona antes de que tenga lugar cualquier acceso o transferencia de datos en una red privada, independientemente de si están dentro o fuera del perímetro de esa red, lo cual permite monitorear, controlar y restringir el acceso a información privilegiada, así como prevenir la fuga de información directamente desde las aplicaciones.

Antecedentes de contratación de licenciamiento DLP de la entidad:

En la vigencia 2022, se adelantó un proceso de selección mediante Subasta Inversa Electrónica No. 020 de 2022, resultado de la cual se suscribió el Contrato de Licenciamiento No 1147 de 2022 con la empresa SAFETY IN DEEP, en donde se adquirieron 820 licencias de software especializado DLP (Prevención de Fuga de la Información) Netskope Data Loss Prevention SAAS/PAAS.

Para la vigencia 2023, se adelantó el proceso de Selección mediante Subasta Inversa Electrónica 015 de 2023, por el cual se suscribió el Contrato de Licenciamiento 1269 de 2023, con la empresa SAFETY IN DEEP SAS, por el cual se adquirieron 680 nuevas licencias correspondientes al Licenciamiento de software Netskope Data Loss Prevention SAAS/PAAS y se renovaron 820 licencias de software Netskope Data Loss Prevention SAAS/PAAS adquiridas en la vigencia 2022, hasta el 14 de mayo de 2024, contando así la entidad con otras capas de seguridad que nos cubren frente a riesgos de Fuga de Información.

Para la vigencia 2024, se adelantó el proceso mediante Selección Abreviada por Subasta Inversa 032 de 2024, por el cual se suscribió el Contrato de Licenciamiento No 1350-2024 con la Empresa SAFETY IN DEEP SAS, que tuvo por objeto “Adquirir el licenciamiento de una solución avanzada de seguridad para la prevención de fuga de información y control de acceso (Zero Trust Network Access y Data Loss Prevention) para 1000 usuarios, aplicaciones y redes, así como su implementación, soporte y mantenimiento.

Para la Vigencia 2025, se adquirieron 1.800 licencias para los funcionarios y contratistas de le Entidad, teniendo en cuenta que el licenciamiento es necesario para la ANLA y dado que el licenciamiento actual tiene vigencia hasta el **21 de diciembre de 2026**. Para la vigencia 2026, se requiere adquirir el licenciamiento de una solución avanzada de seguridad para la prevención de fuga de información y control de acceso (Zero Trust Network Access y Data Loss Prevention) para usuarios, aplicaciones y redes, así como su implementación, mantenimiento y soporte, con cobertura de 1800 licencias para todos los colaboradores de la Entidad, con cubrimiento desde **el 22 de diciembre de 2026 al 21 de diciembre del 2027**.

Necesidad a contratar en la vigencia 2026:

La necesidad del licenciamiento a adquirir, obedece a que el software especializado DLP/ZTNA (prevención de fuga de la información/cero confianza de acceso a la red), permite detectar, analizar y bloquear, si el dato es sensible, alertar y educar al usuario sobre el riesgo de una fuga de información; del mismo modo, tiene la capacidad de identificar en tiempo real intentos de fuga de la información a través de varias aplicaciones y medir el nivel de riesgo de cada una de ellas, controlar información en tránsito, y tomar acciones en tiempo real para aplicaciones administrativas y no administradas, ahora bien, es de aclarar que este licenciamiento de software especializado recae en cabeza de la entidad, permitiendo gestionar la asignación y retiro de las mismas en cualquier momento a cualquier colaborador de la entidad a través de la consola de administración de software especializado a adquirir. Lo anterior permite a la entidad dar cumplimiento de la resolución 500 de 2021 de MinTIC, modificada por las resoluciones 746 de 2022 y 02277 de 2025 siendo este fundamento normativo principal en materia de seguridad digital para los sujetos obligados. La cual exige a la entidades públicas: en su Artículo 3: la adopción de medidas técnicas, administrativas y de talento humano, en su Artículo 6: la implementación de controles según el análisis y evaluación de riesgos, en su Artículo 10: la protección de la privacidad de la información, en su Artículo 17, numeral 1.2: mecanismos para prevenir la fuga de datos e información y en su Artículo 17, numerales 1.1 y 1.5: controles de acceso, gestión de identidades, identificación y mitigación de riesgos.

El licenciamiento solicitado debe ser adquirido en modalidad SAAS/PAAS, es decir, software como servicio o plataforma como servicio en el entendido que la solución debe ser administrada en nube para los aquellos equipos que no son administrados por la entidad, con vigencia de un año en el entendido de que hay equipos personales que deben ser protegidos y no son administrados por la Entidad ya que no son propiedad de la Entidad.

La finalidad de la adquisición de este licenciamiento de software especializado es proteger la información institucional, independientemente si esta es accedida desde un equipo de la entidad o un equipo personal de algún colaborador, para lo cual se requiere la adquisición de 1800 licencias (499 funcionarios de planta + 1301 para contratistas entes externos y colaboradores de la entidad) de software especializado DLP/ZTNA (prevención de fuga de la información/cero confianza de acceso a la red).

Por lo mencionado, con el contrato a celebrar se adquirirán las siguientes licencias las cuales cubren una solución integral de para la prevención de fuga de información y control de acceso a la misma:

ITEM	SKU	Descripción	Vigencia de Garantía o Licenciamiento	Cantidad
1	CP-SASE-BROWSER-T2-Y	Licenciamiento de la solución avanzada de seguridad de acceso (Security Zero Trust Enterprise Browser) para usuarios y aplicaciones web, con componente de protección de fuga de datos junto con su respectiva suscripción de soporte de estas.	Un año a partir del 22 de Dic de 2026	1800

Así mismo, se contratará la siguiente suscrición de servicios:

ITEM	SKU	Descripción	Vigencia	Cantidad
1	NA	Suscripción de soporte y mantenimiento por un año de mil (1800) licencias de ZTNA - Advanced Zero Trust Network	Un año durante la vigencia del licenciamiento, es decir a partir del 22	1

ITEM	SKU	Descripción	Vigencia	Cantidad
			de diciembre de 2026	

¿QUÉ OCURRE SI LA ENTIDAD NO ADQUIERE ESTE LICENCIAMIENTO?

En caso de no llevarse a cabo la contratación de una solución tecnológica basada en el modelo Zero Trust Network Access (ZTNA), la entidad continuaría expuesta a riesgos de seguridad de la información asociados a la ausencia o insuficiencia de mecanismos avanzados para la validación continua de usuarios, dispositivos y condiciones de acceso a los recursos tecnológicos institucionales, la no adquisición de esta solución podría generar las siguientes consecuencias:

- Incremento del riesgo de fuga y exposición de información institucional: La entidad mantendría una mayor exposición a la extracción, transferencia, divulgación o uso no autorizado de información institucional, debido a la falta de mecanismos especializados que permitan establecer controles sobre el acceso y la interacción de los usuarios con los recursos tecnológicos y la información. Esto podría ocasionar la pérdida de confidencialidad de la información, afectaciones a la integridad de los activos de información y eventuales impactos reputacionales, administrativos y económicos.
- Persistencia de vulnerabilidades en los mecanismos de control de acceso: Sin una solución ZTNA, se limitaría la capacidad institucional para implementar un modelo de acceso basado en el principio de mínimo privilegio y confianza cero, en el que cada solicitud de conexión sea evaluada de acuerdo con la identidad del usuario, el estado de seguridad del dispositivo, el contexto de conexión y las políticas institucionales. En consecuencia, podrían mantenerse condiciones de acceso excesivamente amplias o permisos que no correspondan plenamente con las necesidades funcionales de los usuarios.
- Mayor exposición frente a amenazas cibernéticas y accesos no autorizados: La ausencia de controles de acceso adaptativos y de validación continua incrementaría la exposición ante amenazas como el uso indebido de credenciales, la suplantación de identidad, el acceso desde dispositivos no confiables, el movimiento lateral dentro de la infraestructura tecnológica y la explotación de sesiones legítimas comprometidas. Esto podría facilitar que un incidente de seguridad inicialmente limitado alcance otros sistemas, servicios o repositorios de información institucional.
- Limitaciones para garantizar el acceso seguro a los recursos tecnológicos: La entidad tendría menores capacidades para establecer conexiones seguras, segmentadas y controladas hacia sus aplicaciones, plataformas, sistemas de información y demás recursos tecnológicos, especialmente en escenarios de trabajo remoto, movilidad institucional y acceso desde redes externas. Esto podría

dificultar la aplicación homogénea de políticas de seguridad y aumentar la dependencia de mecanismos tradicionales de acceso que no necesariamente ofrecen el nivel de granularidad y verificación requerido.

- Disminución de la capacidad de monitoreo, trazabilidad y respuesta ante incidentes: La no adquisición de la solución limitaría la posibilidad de centralizar y fortalecer la visibilidad sobre las solicitudes de acceso, las actividades de los usuarios y los comportamientos que puedan representar riesgos para la información. Esto dificultaría la identificación temprana de actividades anómalas, la generación de alertas oportunas, la investigación de incidentes y la adopción de medidas preventivas y correctivas.
- Posibles afectaciones a la continuidad de los servicios institucionales: Un incidente de seguridad relacionado con accesos indebidos o fuga de información podría generar indisponibilidad de aplicaciones, interrupciones operativas, necesidad de aislar sistemas comprometidos, recuperación de información y ejecución de actividades extraordinarias de contención. Estas situaciones podrían afectar la prestación de los servicios institucionales y el cumplimiento de las funciones misionales de la entidad.
- Limitaciones para fortalecer el cumplimiento de las políticas y lineamientos de seguridad de la información: La falta de esta capacidad tecnológica dificultaría la evolución de los controles institucionales hacia esquemas modernos de seguridad basados en la gestión de identidades, la validación contextual, la segmentación de accesos y la protección de la información. Asimismo, podría generar brechas frente a los objetivos institucionales de fortalecimiento de la seguridad digital, gestión de riesgos tecnológicos y protección de los activos de información.
- Incremento de los costos potenciales asociados a incidentes de seguridad: La materialización de un incidente de fuga de información o de acceso no autorizado podría generar costos asociados a la atención y contención del incidente, recuperación de servicios, análisis forense, restablecimiento de sistemas, acciones correctivas y eventuales consecuencias administrativas, legales y reputacionales. Por tanto, no adelantar la contratación podría mantener a la entidad en un escenario de mayor exposición a costos derivados de eventos que podrían prevenirse, mitigarse o detectarse oportunamente mediante controles tecnológicos adecuados.

En virtud de lo anterior, la Oficina de Tecnologías de la Información considera que no adelantar la contratación de una solución tecnológica ZTNA representaría la continuidad de brechas en las capacidades institucionales de protección de la información y control de acceso, manteniendo niveles de exposición a riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad de los activos de información.

La contratación de esta solución constituye una medida de fortalecimiento de la postura de ciberseguridad institucional, toda vez que permitirá avanzar hacia un esquema de acceso seguro basado en el principio de confianza cero, con validación de identidad, evaluación de condiciones de acceso, aplicación del principio de mínimo privilegio y mayor visibilidad sobre las conexiones y actividades de los usuarios.

En consecuencia, desde el punto de vista técnico, la contratación se considera necesaria para fortalecer los mecanismos de prevención de fuga de información, reducir la superficie de exposición ante amenazas cibernéticas, mejorar la capacidad de detección y respuesta ante eventos de seguridad y contribuir a la protección de los recursos tecnológicos y de la información institucional

LA IMPORTANCIA DE LA ADQUISICIÓN DEL LICENCIAMIENTO DE ZTNA Y DLP:

La importancia de esta contratación radica en la necesidad mantener a través de esta tecnología un modelo de seguridad que supere los esquemas tradicionales de confianza basados exclusivamente en la ubicación de los usuarios dentro o fuera de la red institucional, adoptando un enfoque en el que ninguna conexión se considere confiable por defecto y en el que cada solicitud de acceso sea evaluada de acuerdo con la identidad del usuario, las características y condiciones de seguridad del dispositivo, el contexto de conexión y las políticas de seguridad definidas por la entidad.

En este sentido, la implementación de una solución ZTNA permite fortalecer la protección de los activos de información institucionales, mediante la aplicación del principio de mínimo privilegio, garantizando que los usuarios accedan únicamente a las aplicaciones, sistemas, plataformas y recursos tecnológicos que requieren para el desarrollo de sus funciones. De igual manera, contribuirá a reducir la exposición de los servicios institucionales frente a accesos no autorizados, suplantación de identidad, utilización indebida de credenciales y posibles compromisos de dispositivos o sesiones de usuario.

Adicionalmente, la solución permitirá fortalecer las capacidades de prevención y control de fuga de información, mediante la aplicación de políticas de acceso y mecanismos de supervisión que contribuyan a identificar, restringir y gestionar actividades que puedan representar un riesgo para la confidencialidad de la información. Esto resulta especialmente relevante considerando que la información institucional constituye un activo estratégico para el cumplimiento de las funciones misionales y administrativas de la entidad, por lo cual requiere mecanismos de protección acordes con su nivel de criticidad y sensibilidad.

Otro aspecto fundamental de esta contratación corresponde al fortalecimiento de la seguridad en los escenarios de acceso remoto, movilidad institucional y utilización de servicios tecnológicos desde redes externas. La solución ZTNA permitirá establecer conexiones seguras, controladas y segmentadas hacia los recursos autorizados, disminuyendo la exposición de la infraestructura tecnológica y evitando que el acceso a la

red institucional implique automáticamente la posibilidad de acceder a todos sus servicios o sistemas de información.

Así mismo, la adquisición de esta tecnología contribuye a mejorar la visibilidad, trazabilidad y capacidad de supervisión de los accesos a los recursos tecnológicos, facilitando el seguimiento de las actividades realizadas por los usuarios, la identificación de comportamientos inusuales y la generación de alertas ante posibles eventos de seguridad. Estas capacidades permitirán fortalecer los procesos de gestión de incidentes, análisis de riesgos y adopción de medidas preventivas y correctivas por parte de la Oficina de Tecnologías de la Información.

Desde la perspectiva de la gestión institucional de riesgos, la contratación representa una medida preventiva orientada a disminuir la probabilidad de materialización de incidentes relacionados con la exposición, pérdida, divulgación o acceso no autorizado a la información, así como a reducir los posibles impactos operativos, económicos, administrativos y reputacionales derivados de este tipo de eventos.

De igual manera, esta adquisición contribuirá al fortalecimiento de los controles tecnológicos asociados a la confidencialidad, integridad y disponibilidad de la información, y al cumplimiento de los lineamientos institucionales de seguridad y privacidad de la información, gestión de riesgos de seguridad digital y buenas prácticas de ciberseguridad aplicables a la entidad.

Es importante señalar que la solución tecnológica ZTNA no constituye únicamente una herramienta de conectividad, sino un componente estratégico dentro de la arquitectura de seguridad institucional, dado que permite establecer un modelo de acceso basado en la verificación permanente, la segmentación de recursos, la gestión de identidades y la aplicación de políticas de seguridad contextualizadas. Su implementación permitirá fortalecer los controles existentes y avanzar hacia una arquitectura tecnológica más segura, resiliente y alineada con las necesidades actuales de protección de la información.

Actualmente se cuenta con el siguiente licenciamiento:

ITEM	SKU	Descripción	Vigencia de Garantía o Licenciamiento	Cantidad
1	CP-SASE-BROWSER-T2-Y	Licenciamiento de la solución avanzada de seguridad de acceso (Security Zero Trust Enterprise Browser) para usuarios y aplicaciones web, con componente de protección de fuga de datos junto con su respectiva suscripción de soporte de estas.	Un año a partir del 22 de dic de 2026	1800

Así mismo, se contratará la siguiente suscrición de servicios:

ITEM	SKU	Descripción	Vigencia	Cantidad
1	NA	Suscripción de soporte y mantenimiento por un año de mil (1800) licencias de ZTNA - Advanced Zero Trust Network	Un año a partir del 22 de dic de 2026	1

VERIFICACIÓN DE ACUERDOS MARCOS DE PRECIOS

De conformidad con lo establecido en los artículos 2.2.1.2.1.2.7 y siguientes del Decreto 1082 de 2015, y las disposiciones que los modifican, adicionan o complementan, las entidades estatales deben observar las reglas aplicables a la adquisición de bienes y servicios a través de los Acuerdos Marco de Precios e Instrumentos de Agregación de Demanda dispuestos por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente. En particular, el artículo 2.2.1.2.1.2.9 del citado decreto establece que, durante la etapa de planeación, las entidades estatales deben verificar la existencia de Acuerdos Marco de Precios vigentes que permitan satisfacer la necesidad identificada.

En cumplimiento de lo anterior, durante la etapa de estructuración del presente proceso de contratación, correspondiente a la vigencia 2026, la Oficina de Tecnologías de la

Información realizó la revisión de los instrumentos de agregación de demanda y Acuerdos Marco de Precios disponibles en la Tienda Virtual del Estado Colombiano, administrada por Colombia Compra Eficiente, con el propósito de identificar alternativas de adquisición que permitieran atender la necesidad institucional relacionada con la implementación de una solución tecnológica especializada para el control de acceso mediante el modelo Zero Trust Network Access (ZTNA) y la prevención de fuga de información (Data Loss Prevention – DLP).

Como resultado de la consulta efectuada, se identificó el siguiente instrumento contractual relacionado con el sector tecnológico:

Acuerdo Marco de Precios: Servicios de Nube Privada IV.

Identificador: CCE-308-AMP-2022.

Número del proceso: CCENEG-061-01-2022.

Vigencia reportada: Desde el 30 de diciembre de 2022 hasta el 28 de febrero de 2027.

Entidad administradora: Agencia Nacional de Contratación Pública – Colombia Compra Eficiente.

Una vez identificado el citado instrumento, la Oficina de Tecnologías de la Información procedió a analizar su objeto, alcance, condiciones técnicas, catálogo de bienes y servicios, componentes tecnológicos y posibilidades de adquisición, contrastándolos con los requerimientos funcionales, técnicos y operativos definidos para el presente proceso de contratación.

Como resultado de dicho análisis, se determinó que, aunque el Acuerdo Marco de Precios identificado contempla servicios y componentes tecnológicos asociados al entorno de nube privada y categorías relacionadas con software, su alcance y oferta disponible no permiten acreditar la correspondencia integral con las capacidades especializadas requeridas por la entidad para implementar una solución de seguridad basada en el modelo Zero Trust Network Access (ZTNA), complementada con mecanismos de prevención de fuga de información (DLP).

En consecuencia, desde la perspectiva técnica, funcional, económica y operativa, se identifican las siguientes razones que sustentan la necesidad de adelantar el presente

proceso de contratación mediante un mecanismo de selección diferente al Acuerdo Marco de Precios señalado:

1. Diferencia entre el objeto y alcance del Acuerdo Marco de Precios y la necesidad institucional identificada.

El Acuerdo Marco de Precios CCE-308-AMP-2022 tiene como objeto establecer las condiciones para la adquisición de servicios de nube privada. Sin embargo, la necesidad que pretende satisfacer la entidad no corresponde exclusivamente a la provisión de infraestructura o servicios de computación en la nube, sino a la adquisición de una solución especializada de ciberseguridad que permita establecer controles de acceso seguro a los recursos tecnológicos institucionales y prevenir la extracción, transferencia, divulgación o utilización no autorizada de información.

Por consiguiente, la necesidad institucional comprende capacidades funcionales específicas que deben operar de manera articulada, tales como la validación de identidad, el control de acceso contextual, la aplicación del principio de mínimo privilegio, la segmentación de aplicaciones y servicios, la supervisión de las actividades de los usuarios y la aplicación de políticas de protección de información.

Estas capacidades corresponden a un alcance funcional especializado que debe encontrarse expresamente contemplado en los bienes y servicios disponibles en el catálogo del instrumento de agregación de demanda para considerar que este satisface la necesidad institucional.

2. Necesidad de contar con capacidades especializadas de Zero Trust Network Access (ZTNA).

La entidad requiere implementar un modelo de acceso basado en el principio de confianza cero (Zero Trust), mediante el cual ninguna conexión sea considerada confiable por defecto y cada solicitud de acceso a los recursos tecnológicos sea evaluada conforme a la identidad del usuario, las condiciones de seguridad del dispositivo, el contexto de conexión y las políticas de acceso institucionales.

Para ello, se requiere una solución que permita establecer controles granulares de acceso a aplicaciones, sistemas de información, plataformas y demás recursos tecnológicos, independientemente de la ubicación física del usuario o de la red desde la cual se origine la conexión.

De igual manera, se requiere disponer de mecanismos de autenticación e integración con los servicios institucionales de identidad, validación de condiciones de acceso, segmentación lógica de recursos y administración centralizada de políticas de seguridad.

El análisis del instrumento identificado **no permitió establecer que su catálogo contemple, bajo las condiciones de adquisición allí definidas, una solución que satisfaga integralmente estas capacidades especializadas de ZTNA en los términos y alcance requeridos por la entidad.**

3. Requerimiento de capacidades específicas para la prevención de fuga de información (DLP).

Adicionalmente, la entidad requiere fortalecer sus mecanismos de protección de la información mediante capacidades de Data Loss Prevention (DLP), orientadas a identificar, controlar, monitorear y prevenir actividades que puedan ocasionar la divulgación, transferencia o extracción no autorizada de información institucional.

Para ello, se requiere una solución que permita establecer políticas de protección de acuerdo con la clasificación, sensibilidad y criticidad de la información, así como aplicar controles sobre las actividades de los usuarios y los diferentes canales de acceso, consulta, utilización y transferencia de información, de acuerdo con el alcance funcional y los componentes técnicos de la solución a adquirir.

Estas capacidades deben permitir, según las funcionalidades efectivamente contratadas, la identificación de información sensible, la aplicación de reglas de protección, la generación de alertas, el registro de eventos y la adopción de acciones preventivas o restrictivas frente a comportamientos que representen riesgos para la seguridad de la información.

En este sentido, los componentes tecnológicos asociados a la prestación de servicios de nube privada no pueden considerarse equivalentes a una solución especializada de prevención de fuga de información, en la medida en que responden a finalidades y necesidades funcionales diferentes.

4. Características particulares del licenciamiento y administración de la solución tecnológica.

La solución requerida contempla un esquema de licenciamiento y administración especializado, que debe responder a las condiciones de uso institucional, el número de usuarios objeto de protección, los recursos tecnológicos a los cuales acceden y las funcionalidades de seguridad requeridas.

En particular, se requiere que el modelo de licenciamiento permita administrar y controlar los usuarios cubiertos por las políticas de protección, de acuerdo con las condiciones técnicas y comerciales de la solución, evitando que la utilización de diferentes dispositivos por parte de un mismo usuario genere restricciones incompatibles con las necesidades operativas de la entidad.

Así mismo, se requiere disponer de una consola centralizada de administración y gestión de políticas de seguridad, con capacidades de supervisión, configuración, seguimiento y generación de reportes, que facilite la administración de los controles de acceso y protección de la información.

Estas condiciones deben estar articuladas con los requerimientos de implementación, parametrización, integración, soporte técnico y mantenimiento, de manera que la entidad pueda disponer de una solución funcionalmente integrada y administrable conforme a sus necesidades institucionales.

5. Necesidad de implementación, integración y puesta en funcionamiento de la solución.

La necesidad institucional no se limita a la adquisición de licencias de software**, sino que comprende los servicios especializados necesarios para su implementación, configuración, parametrización, integración con la**

infraestructura tecnológica y los servicios institucionales de identidad, definición de políticas de seguridad, pruebas funcionales, puesta en producción.

De igual manera, se requiere contar con servicios de soporte técnico y mantenimiento que permitan garantizar la operación de la solución, atender incidentes, gestionar actualizaciones y mantener las condiciones de funcionamiento y seguridad durante el periodo contractual.

Por lo tanto, se requiere una alternativa de contratación que permita articular integralmente los componentes tecnológicos y los servicios especializados necesarios para alcanzar los resultados esperados, conforme a las especificaciones técnicas y niveles de servicio definidos por la entidad.

6. Necesidad de garantizar la interoperabilidad y compatibilidad con la arquitectura tecnológica institucional.

La solución que se pretende adquirir debe contar con capacidades de integración e interoperabilidad con los sistemas, aplicaciones, servicios de identidad y demás componentes de la arquitectura tecnológica institucional, permitiendo implementar políticas homogéneas de acceso y protección de información.

Esta condición resulta fundamental para evitar la generación de controles aislados, duplicidad de herramientas, dificultades de administración o limitaciones en la visibilidad de los eventos de seguridad.

En consecuencia, la solución debe responder a los requerimientos específicos de la infraestructura tecnológica existente y permitir su articulación con los mecanismos institucionales de seguridad de la información, gestión de identidades, monitoreo y administración tecnológica.

7. Análisis de conveniencia económica, operativa y funcional.

Desde la perspectiva económica y operativa, la conveniencia de una alternativa de adquisición debe analizarse considerando no solamente el valor de las licencias, sino también el alcance funcional, la cobertura de usuarios, las capacidades de seguridad, los servicios de implementación, la integración tecnológica, el soporte, el mantenimiento y los niveles de servicio requeridos.

En este contexto, adelantar la contratación a través de un instrumento cuyo catálogo no permita satisfacer integralmente los requerimientos técnicos y funcionales identificados podría generar limitaciones en la cobertura de los controles de seguridad, la necesidad de adquirir componentes adicionales o la contratación de servicios complementarios, con posibles impactos en los costos totales, la interoperabilidad y la eficiencia de la operación tecnológica.

Por lo anterior, la Entidad requiere estructurar un proceso de contratación que permita obtener **una solución integral,** técnicamente compatible con su arquitectura tecnológica y acorde con las necesidades de protección de sus activos de información, bajo condiciones que permitan evaluar objetivamente la calidad, funcionalidad, cobertura, soporte y costo total de la solución.

Con fundamento en el análisis efectuado por la Oficina de Tecnologías de la Información, se concluye que el Acuerdo Marco de Precios **CCE-308-AMP-2022**, correspondiente a Servicios de Nube Privada IV**, no permite acreditar, con base en el alcance y los componentes revisados, la satisfacción integral de la necesidad institucional relacionada con la adquisición de una solución especializada de Zero Trust Network Access (ZTNA) y prevención de fuga de información (DLP).**

Lo anterior, teniendo en cuenta que la necesidad identificada requiere capacidades especializadas de ciberseguridad orientadas al control granular de acceso, validación contextual de usuarios y dispositivos, aplicación del principio de mínimo privilegio, segmentación de recursos tecnológicos, identificación y protección de información sensible, monitoreo de actividades y prevención de transferencias o divulgaciones no autorizadas de información institucional.

En consecuencia, **al no evidenciarse una correspondencia funcional y técnica integral entre los bienes y servicios disponibles en el Acuerdo Marco de Precios identificado y los requerimientos específicos que pretende satisfacer la entidad, se encuentra técnicamente justificado estructurar el presente proceso de contratación mediante**

el mecanismo de selección que jurídicamente corresponda, de acuerdo con la naturaleza del objeto, su cuantía, las condiciones del mercado y el régimen de contratación aplicable a la entidad.

Esta determinación no obedece a una preferencia por un mecanismo de selección particular ni a la intención de sustraerse de los instrumentos de agregación de demanda dispuestos por Colombia Compra Eficiente, **sino a la necesidad de garantizar que la modalidad de adquisición permita atender de manera efectiva, integral y verificable los requerimientos técnicos y funcionales institucionales.**

Por lo anterior, la Oficina de Tecnologías de la Información considera necesario adelantar la contratación de la solución tecnológica especializada de ZTNA / DLP (prevención de fuga de información), con el propósito de fortalecer la postura de ciberseguridad de la Entidad, mejorar el control sobre el acceso a los recursos tecnológicos, reducir la exposición a incidentes de seguridad y proteger la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

En virtud de lo expuesto, se deja constancia de la verificación realizada y de la justificación técnica y funcional que sustenta la **no utilización del Acuerdo Marco de Precios CCE-308-AMP-2022** para satisfacer la necesidad específica objeto del presente proceso contractual, sin perjuicio de las validaciones jurídicas y de las demás verificaciones que correspondan durante la estructuración del proceso.

Esta necesidad se encuentra contemplada dentro del Plan Anual de Adquisiciones (PAA) y el Plan de Acción Institucional (PAI) de la Entidad para la vigencia 2026.

1. DESCRIPCIÓN DEL OBJETO A CONTRATAR, CON SUS ESPECIFICACIONES Y LA IDENTIFICACIÓN DEL CONTRATO A CELEBRAR.

1.1 OBJETO DEL CONTRATO.

10-0-7-23 ADQUIRIR EL LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION) PARA USUARIOS, APLICACIONES Y REDES, ASÍ COMO SU IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO.

1.2 CLASIFICADOR DE BIENES Y SERVICIOS

El objeto contractual se clasifica en el siguiente código del Clasificador de Bienes y Servicios:

CÓDIGO	SEGMENTO	FAMILIA	CLASE
43222500	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
81112200	Servicios bajados en ingeniería, Investigación y tecnología	Servicios Informáticos	Mantenimiento y soporte de Software

Nota: Teniendo en cuenta que en el RUP el código solo se puede registrar hasta el tercer nivel, en el presente numeral solo se desagrega hasta nivel de clase.

1.3 OBLIGACIONES DEL CONTRATISTA

1.3.1 OBLIGACIONES ESPECÍFICAS

1. Cumplir con la totalidad de lineamientos, características técnicas y actividades a desarrollar durante la ejecución del contrato que se encuentren descritas en la ficha técnica del presente proceso, la cual hace parte integral del contrato que se suscriba.

2. Entregar al supervisor del contrato, dentro de los tres (3) días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, la carta de solicitud y requerimiento ante su proveedor nacional o extranjero (debidamente acreditado como proveedor especializado), de los bienes adquiridos, en el cual se exprese claramente que estos, serán entregados en los términos requeridos por la ANLA.
3. Entregar dentro de los tres (3) días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, un (1) documento que provenga del fabricante, en el cual se certifique la adquisición a nombre de la ANLA del Licenciamiento de la solución avanzada de seguridad de acceso (**Security Zero Trust Enterprise Browser**) para usuarios y aplicaciones web, con componente de protección de fuga de datos con vigencia de una año a partir de su activación, junto con su respectiva suscripción de soporte de estas en formato PDF en idioma (Español Colombia).
4. Realizar la activación del soporte 24 horas al día los 7 días de la semana por un año, y mantenimiento por un año de mil (1800) licencias de ZTNA - Advanced Zero Trust Network, por el término de un año, a partir del **22 de diciembre de 2026.**
5. El contratista/proveedor deberá garantizar que toda la documentación relacionada con la ejecución del contrato (Licencias, reportes, manuales, certificados, comunicaciones, etc.) se entregue en formato digital, evitando el uso de papel en línea con los lineamientos y programas ambientales de la ANLA.
6. El contratista/proveedor se compromete a que las actualizaciones de software, correcciones y mejoras se distribuyan y ejecuten mediante canales digitales, evitando el uso de soportes físicos o procesos que generen residuos tecnológicos innecesarios (CD y/o USB).
7. Garantizar el cumplimiento de las actividades establecidas entre las partes comprendiendo el afinamiento, puesta en producción, y monitoreo de los servicios contratados en los términos previstos en la ficha técnica, tras el cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.
8. Disponer de los recursos técnicos y humanos necesarios para ejecutar a satisfacción los lineamientos establecidos en la Ficha Técnica.
9. Presentar y mantener vigente durante la ejecución del contrato, los permisos, licencias y autorizaciones ambientales que correspondan, si a ellos hay lugar. Deberá cumplir con la normatividad ambiental vigente nacional, para reducir los aspectos e impactos ambientales asociados a su actividad.
10. Las demás obligaciones que, por naturaleza del contrato, el contratista este obligado a cumplir.

1.3.2 OBLIGACIONES GENERALES.

1. Ejecutar el contrato con plena autonomía técnica, administrativa, financiera y organizacional, bajo su exclusiva responsabilidad y utilizando sus propios medios personales y materiales. El personal que destine para la ejecución del contrato dependerá exclusivamente del contratista, quien ejercerá respecto de aquel todas las

facultades de dirección, coordinación, supervisión y control, sin que exista vínculo laboral, legal o reglamentario alguno entre dicho personal y la Autoridad Nacional de Licencias Ambientales –ANLA.

2. Presentar los informes de ejecución requeridos para el pago.
3. Asistir y participar en los comités, reuniones virtuales y/o presenciales y demás eventos que le indique el supervisor y se relacionen con el objeto del contrato.
4. Atender las instrucciones, que durante la ejecución del contrato impartan el supervisor del mismo, dentro del marco del objeto contractual.
5. No aceptar invitaciones, suministro de alimentación, transporte, refrigerios u otros estipendios que ofrezca el usuario o algún delegado de éste, sin previa autorización de la **ANLA.**
6. Salvaguardar la información confidencial que obtenga o conozca en el desarrollo de sus actividades, salvo requerimiento expreso de autoridad competente. Toda la información y/o documentos que se produzcan en desarrollo del presente contrato serán de uso exclusivo de la ANLA, obligándose desde ya el contratista a no utilizarlo para fines distintos a los previstos en este contrato, ni a divulgar la información que se le suministrare, ni los resultados de su trabajo, conservando la confidencialidad de los mismos, de conformidad con la Ley, so pena de las acciones civiles, administrativas o penales a que haya lugar.
7. Cumplir con lo señalado en el Código de Integridad adoptado por la Entidad.
8. Cumplir con lo señalado en el Protocolo para la prevención, atención y medidas de protección de todas las formas de violencia basadas en género y/o discriminación por razón de raza, etnia, religión, nacionalidad, ideología política o filosófica, sexo u orientación sexual o discapacidad y demás razones de discriminación en el lugar de trabajo de la Autoridad Nacional de Licencias Ambientales – ANLA adoptado mediante resolución No. 1423 del 6 de julio de 2023.
9. Informar de forma inmediata y por escrito a la **ANLA** respecto de cualquier situación referida al objeto del presente contrato que pudiere generar un conflicto de interés en la ejecución del mismo.
10. Hacer uso de los formatos establecidos en el Sistema Integrado de Gestión, ejecutar sus procedimientos y efectuar los registros, según corresponda a su actividad contractual.
11. Hacer uso de los sistemas operativos de información y demás herramientas implementadas y que en adelante sean adoptadas por la **ANLA** para el desarrollo de las actividades contractuales, garantizando la confidencialidad y debido uso de los usuarios y claves utilizados para tal fin.
12. Dar cumplimiento a la Política General de Privacidad y Seguridad de la Información establecida por la ANLA para los contratistas, así como a las directrices y controles establecidos en el Sistema de Gestión de Seguridad de la Información – SGSI, respecto de la información, sistemas, aplicaciones y recursos tecnológicos utilizados para la ejecución del objeto contractual. Para tal efecto, el contratista deberá adoptar las medidas de seguridad definidas por la Entidad y permitir las verificaciones que resulten necesarias para comprobar su cumplimiento, dentro del alcance de las obligaciones contractuales y respetando las disposiciones aplicables en materia de protección de datos personales, privacidad y seguridad de la información.
13. El contratista será el único responsable del cumplimiento de sus obligaciones fiscales y tributarias en los términos de Ley, en caso de que cambien las circunstancias bajo

las cuales se celebró el contrato tales como el régimen tributario, la modificación de los códigos de las actividades inscritas en el RUT, entre otras, se deberá dar aviso al supervisor del contrato.

14. El contratista será responsable de actualizar su información tributaria, y en caso de encontrarse obligado a presentar Factura Electrónica conforme a lo señalado en el Decreto 358 del 5 de marzo de 2020, deberá realizar los trámites correspondientes en la plataforma que para tal fin se haya dispuesto. La validación de la factura electrónica por parte de la DIAN será requisito previo y obligatorio para gestionar el pago de la cuenta de cobro respectiva ante la **ANLA**.

15. Dar cumplimiento a las obligaciones con los sistemas de seguridad social integral, y presentar los documentos respectivos que así lo acrediten, conforme lo establecido en el artículo 50 de la Ley 789 de 2002, en concordancia con el artículo 23 de la Ley 1150 de 2007, en la Ley 828 de 2003, en la Ley 1122 de 2007, Decreto 1703 de 2002, Decreto 510 del 5 de marzo de 2003 y demás normas que las adicionen, complementen o modifiquen.

16. Cumplir con la matriz de roles y responsabilidades dentro del Sistema de Gestión de Seguridad y Salud en el Trabajo.

17. Realizar en términos de oportunidad los trámites de obligatorio cumplimiento como proveedor en la plataforma SECOP.

18. Cargar y publicar a través de la plataforma SECOP la garantía constituida para amparar el contrato en caso de ser solicitada, como requisito de ejecución del mismo, y en caso de modificaciones a la misma (según corresponda).

19. Al finalizar el contrato entregar toda la información que haya utilizado y/o producido durante la ejecución del mismo, mediante la herramienta establecida para el almacenamiento de la información y las actividades ejecutadas por el Contratista que disponga la Entidad.

20. Cumplir, durante la ejecución del contrato, las disposiciones legales aplicables en materia de prevención del lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva (LA/FT/FPADM). En consecuencia, el CONTRATISTA deberá abstenerse de utilizar en la ejecución contractual recursos de origen ilícito o de realizar operaciones contrarias a dichas disposiciones.

21. Mantener actualizada y veraz la información suministrada a la ANLA durante la etapa precontractual y la ejecución del contrato, relacionada con el origen lícito de sus recursos y la no inclusión del CONTRATISTA, su representante legal, administradores, socios, accionistas o beneficiarios finales, cuando corresponda, en listas internacionales vinculantes para Colombia, de conformidad con el artículo 20 de la Ley 1121 de 2006 y las demás normas aplicables.

22. Informar de manera inmediata y por escrito a la ANLA cualquier circunstancia sobreviniente de la que tenga conocimiento que afecte la veracidad o vigencia de las declaraciones e información suministradas en materia de origen de recursos, inclusión en listas internacionales vinculantes para Colombia o prevención de LA/FT/FPADM. Asimismo, deberá aportar las aclaraciones y los soportes que requiera la Entidad para evaluar los efectos de dicha circunstancia sobre la ejecución contractual y adoptar las medidas a que haya lugar.

Nota: Las presentes obligaciones se incorporan en cumplimiento de lo establecido en el Manual de Debida Diligencia a la Gestión Contractual GC-MN-08, versión 1, de la Autoridad Nacional de Licencias Ambientales (ANLA).

1.4 OBLIGACIONES DE LA ENTIDAD.

1. Pagar al CONTRATISTA el valor del contrato en las condiciones pactadas.
2. Ejercer la supervisión para verificar el cumplimiento del objeto contractual y las obligaciones a que se compromete EL CONTRATISTA.
3. Suministrar al CONTRATISTA, la información y documentos que requiera para desarrollar el objeto contractual.
4. Garantizar el acceso a las a las diferentes plataformas, servidores y consolas de administración para el cumplimiento del contrato, siempre y cuando sea necesario para el desarrollo del objeto contractual y sus obligaciones.
5. Ingresar las cartas de licenciamiento al almacén de la Entidad.

1.5 INFORMES Y PRODUCTOS

EL (LA) CONTRATISTA deberá entregar y suministrar a la ANLA:

- Documento que provenga del fabricante de cada una de las plataformas y/o servicios (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION), en el cual se certifique el licenciamiento y servicios adquiridos a nombre de la **ANLA**, incluyendo la vigencia de las licencias, la fecha de entrega de las mismas, que se debe presentar dentro de los tres (3) días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

- Los demás reportes o informes y entregables que se requieran en la ejecución del contrato acorde a la Ficha Técnica.

NOTA: La activación de las licencias será realizará por parte de la ANLA a partir del vencimiento del licenciamiento vigente, es decir a partir del **22 de diciembre de 2026.**

1.6 LUGAR DE EJECUCIÓN DEL CONTRATO

El lugar de ejecución del contrato será en la ciudad de **Bogotá D.C.** Se aclara que actualmente las instalaciones de la ANLA y sus servidores y servicios se encuentran ubicadas y alojados en la siguiente dirección:

- **Sede principal**: Carrera 13 a No. 34 – 72, Pisos 8 al 11, Bogotá D.C.

1.7 PLAZO DE EJECUCIÓN DEL CONTRATO

El plazo del contrato será hasta el **31 de diciembre de 2026**, contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución.

Nota 1: Vigencia de Licenciamiento que se adquiere: La vigencia del licenciamiento será de un (1) año, contado a partir del **22 de diciembre de 2026.**

Nota 2: La vigencia de la suscripción de soporte y mantenimiento de mil (1800) licencias de ZTNA - Advanced Zero Trust Network, será por el término de un año contado a partir del **22 de diciembre de 2026**.

Nota 3 La Garantía de fabrica (inherente a la licencia) comprende el periodo de la vigencia de la licencia.

Nota 4: El plazo de entrega de la carta del licenciamiento y de la suscripción del soporte y mantenimiento, será dentro de los 3 días hábiles, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución, en la cual debe constar la fecha de activación.

Nota 5: Los servicios previstos dentro de la garantía legal o de fábrica de las licencias (tales como soporte, acompañamiento, atención) serán por el período de vigencia de la licencia, a través de los canales virtuales.

1.8 SUPERVISIÓN Y CONTROL

La vigilancia y control del cumplimiento de las obligaciones a cargo del CONTRATISTA será ejercida por el **Profesional Especializado Código 2028 Grado 24 (Raúl Trujillo García) perteneciente a la oficina de Tecnologías de la Información de la ANLA**, o por quien designe el ordenador del gasto, quien será responsable de aprobar los pagos, los informes que presente el contratista, de proyectar el acta de liquidación definitiva del contrato, cuando sea el caso, y en general cumplir con lo previsto en el "Manual de Contratación, Supervisión e Interventoría" de la ANLA.

1.9 VALOR DEL CONTRATO Y FORMA DE PAGO.

1.9.1 VALOR DEL CONTRATO.

El valor del contrato será hasta por la suma de **TRESCIENTOS SESENTA Y UN MILLONES CUARENTA MIL PESOS M/CTE ($361.040.000)** incluido IVA y los demás impuestos, gastos, costos y erogaciones a que haya lugar, derivados de la adquisición del licenciamiento. Para lo cual se afectarán el Certificado de Disponibilidad Presupuestal No. **88726 del 14 de septiembre de 2026 por valor de $362.000.001,** expedido por el **Grupo de Gestión Financiera y Presupuestal de la AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES – ANLA.**

1.9.2 FORMA DE PAGO.

El **FONAM/ANLA** pagará al contratista el valor del contrato en los siguientes términos:

ÚNICO PAGO, correspondiente al valor establecido de las **1800 licencias a adquirir con la suscripción de soporte y mantenimiento**, una vez entregada la carta de licenciamiento y de suscripción del soporte y mantenimiento, lo cual deberá realizarse de conformidad con la cláusula plazo del contrato.

Recibido el documento que provenga del fabricante, en el cual se certifique la adquisición a nombre de la **AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES – ANLA** el licenciamiento antes señalado, incluyendo la vigencia de la licencia y la fecha de entrega, las mismas deben ser aprobadas y recibidas a satisfacción por parte del contratista y del supervisor del contrato, de lo cual se dejará constancia en Acta de entrega suscrita por las partes.

Por otra parte, el contratista para el pago deberá cumplir con los siguientes requisitos: la correcta presentación de la factura, informe de instalación, entrega del certificado de las suscripciones de soporte, carta de licenciamiento por parte de fabricante, garantía y el recibido a satisfacción por parte del supervisor del contrato de la ANLA para estos servicios. La factura deberá venir a nombre del **FONDO NACIONAL AMBIENTAL / AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES - FONAM/ANLA**.

Para efectos del pago, el contratista deberá adjuntar la factura correspondiente y en caso de estar obligado a facturar electrónicamente deberá dar cumplimiento a lo previsto en la Resolución No 165 del 1 de noviembre de 2023 expedida por la DIAN, y a lo dispuesto en los procedimientos internos los cuales les serán informados a través del supervisor; igualmente, deberá contar con el lleno de los requisitos legales, constancia de cumplimiento a satisfacción por parte del supervisor del contrato, acreditar mediante certificación firmada por revisor fiscal, cuando se esté obligado a tenerlo; o por el representante legal, donde manifieste estar al día en el pago de parafiscales y seguridad social como mínimo en los últimos seis meses. Cabe resaltar que el estar al día, es haber realizado los pagos pertinentes de acuerdo con los plazos fijados por la norma para tales fines. En caso de Consorcio o Uniones Temporales cada una de las partes deberán presentar este certificado.

De igual manera para este pago el contratista deberá presentar una factura con el cumplimiento de los siguientes requisitos legales y según el origen de los recursos utilizados, así:

Para el pago el proveedor deberá presentar factura con el cumplimiento de los requisitos legales y dirigirse a nombre del **FONDO NACIONAL AMBIENTAL / AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES – FONAM/ANLA** - **NIT 830.025.267-9**: Suscripción de soporte y mantenimiento por un año de mil (1800) licencias de ZTNA - Advanced Zero Trust Network Licenciamiento de Software para la Herramienta Especializada de Monitoreo.

Para efectos de los pagos, el contratista deberá adjuntar la factura correspondiente y en caso de estar obligado a facturar electrónicamente deberá dar cumplimiento a lo previsto en la Resolución No 165 del 1 de noviembre de 2023 expedida por la DIAN, y a lo dispuesto en los procedimientos internos los cuales les serán informados a través del supervisor; igualmente, deberá contar con el lleno de los requisitos legales, constancia de cumplimiento a satisfacción por parte del supervisor del contrato, acreditar mediante certificación firmada por revisor fiscal, cuando se esté obligado a tenerlo; o por el representante legal, donde manifieste estar al día en el pago de parafiscales y seguridad social como mínimo en los últimos seis meses.

Cabe resaltar que el estar al día, es haber realizado los pagos pertinentes de acuerdo con los plazos fijados por la norma para tales fines. En caso de Consorcio o Uniones Temporales cada una de las partes deberán presentar este certificado.

Para emitir la factura electrónica, el proveedor de servicios o bienes debe, en datos del adquiriente, registrar el correo electrónico: siifnacion.facturaelectronica@minhacienda.gov.co

Y en notas finales asegúrese de registrar únicamente:

Factura o documento electrónico a nombre de **FONAM/ANLA**:

#$32-04-01-200; CPS-F-XXX-20XX; PedroPerez@anla.gov.co#$

Nota: Los datos en rojo se registran de acuerdo con el número del contrato y supervisor, no se deben dejar espacios en blanco y los datos se separan por punto y coma.

Si el contrato establece pagos en el mes de diciembre, el proveedor de servicio o bienes debe atender lo contemplado en la Circular de Cierre que la Subdirección Administrativa y Financiera de esta Autoridad establezca.

Los pagos se realizarán por conducto del **Grupo de Gestión Financiera y Presupuestal**, previa presentación de los respectivos informes con el recibo a satisfacción por parte del Supervisor y de la constancia de estar al día con el pago de las obligaciones al Sistema de Seguridad Social Integral y ARL.

Nota 1: De acuerdo con el resultado del proceso de Subasta Inversa Electrónica y su respectiva adjudicación, los valores de los rubros serán ajustados.

Nota 2: Los pagos correspondientes serán consignados por el **FONAM/ANLA** al **CONTRATISTA** en la Cuenta Bancaria, certificada por la entidad financiera correspondiente y que hace parte integral del contrato.
Nota 3: FONAM/ANLA podrá retener las sumas correspondientes a los impuestos en los porcentajes establecidos en la ley.

Nota 4: No obstante, lo señalado en la forma de pago, los mismos están sujetos a las disponibilidades del Programa Anual Mensualizado de Caja – PAC y a la ubicación de fondos en la tesorería de la **ANLA.**
Nota 5: Para el pago de la última cuenta de cobro, el contratista deberá tener presente las fechas, requisitos y tramites establecidos en la Circular del Cierre Financiero que para tal fin expida la entidad, y deberá entregar toda la información que haya utilizado y/o producido durante la ejecución del mismo, mediante la herramienta establecida para el almacenamiento de la información y las actividades ejecutadas por el Contratista que disponga la Entidad.
Nota 6: Los bienes o servicios y que no sean aprobados previamente por el supervisor del contrato, ni recibidos a satisfacción no serán pagados por la entidad.

1.10 IDENTIFICACIÓN DEL CONTRATO A CELEBRAR.

El Estatuto General de Contratación de la Administración Pública (Ley 80 de 1993) establece en su artículo 32, de los contratos estatales, definiéndolos como "(…) todos los actos jurídicos generadores de obligaciones que celebren las entidades a que se refiere el presente estatuto, previstos en el derecho privado o en disposiciones especiales, o derivados del ejercicio de la autonomía de la voluntad (…)", procediendo a la enumeración de algunos de los tipos contractuales que pueden utilizar las entidades al celebrar contrataciones logrando así la consecución de sus fines.

El contrato por celebrar será de **compraventa**, teniendo en cuenta que, el componente principal del mismo lo constituye la adquisición del licenciamiento de una solución avanzada de seguridad para la prevención de **fuga de información y control de acceso (Zero Trust Network Access y Data Loss Prevention)** para usuarios, aplicaciones y redes y de la suscripción del soporte y mantenimiento.

Asimismo, atendiendo a la disposición normativa contenida en el artículo 13 de la Ley 80 de 1993 que establece: “DE LA NORMATIVIDAD APLICABLE A LOS CONTRATOS ESTATALES. Los contratos que celebren las entidades a que se refiere el artículo 2o. del presente estatuto se regirán por las disposiciones comerciales y civiles pertinentes, salvo en las materias particularmente reguladas en esta ley (…)” el contrato de compraventa se rige por las legislaciones, civil y comercial, las cuales no presentan diferencias en cuanto a la definición de dicho negocio jurídico.

1.11. INTERES DE LIMITAR LA CONVOCATORIA A MIPYMES

De conformidad con los requisitos señalados en el artículo 2.2.1.2.4.2.2. del Decreto 1082 de 2015, modificado por el artículo 5 del Decreto 1860 de 2021 los procesos de selección se podrán limitar a MiPymes, cuando el valor del Proceso de Contratación sea menor a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000), liquidados con la tasa de cambio que para el efecto determina cada dos años el Ministerio de Comercio, Industria y Turismo, que en la presente vigencia corresponde a **QUINIENTOS ONCE MILLONES SETECIENTOS OCHO MIL CUATROCIENTOS NOVENTA Y SIETE PESOS M/CTE ($511.708.497).**

En consecuencia, teniendo en cuenta que el presupuesto oficial del presente proceso de contratación asciende a La suma de **TRESCIENTOS SESENTA Y UN MILLONES CUARENTA MIL PESOS M/CTE ($361.040.000)**, valor inferior al umbral señalado, se concluye que el proceso **SÍ ES SUSCEPTIBLE DE SER LIMITADO A MIPYMES**, siempre que se cumplan los demás requisitos legales para ello.

2 MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO LOS FUNDAMENTOS JURÍDICOS.

Para el presente proceso se tendrá en cuenta lo dispuesto en la Ley 80 de 1993, en la Ley 1150 de 2007 y el Decreto 1082 de 2015, y se aplicarán los principios de economía, transparencia y responsabilidad contenidos en la primera norma citada.

De conformidad con lo establecido en el artículo 2° de la Ley 1150 de 2007, la escogencia del contratista se efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos, de mínima cuantía y contratación directa, con base en las reglas allí establecidas.

Por su parte, el numeral segundo del citado artículo expresa "(…)

2**. Selección abreviada**. La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que, por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.

(…)"

Así mismo, dentro de las causales de selección abreviada, se encuentra en el literal a) del numeral 2 del citado artículo (…) la *adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, definiendo como estos bienes y servicios, a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos.*"

Establece el mismo literal que para la adquisición de estos bienes y servicios, las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos.

El objeto del Proceso de Contratación corresponde a: **10-0-7-23 ADQUIRIR EL LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION) PARA USUARIOS, APLICACIONES Y REDES, ASÍ COMO SU IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO**, de tal manera que se trata de bienes y servicios de características técnicas uniformes y de común utilización, ofrecidos en el mercado en condiciones equivalentes por diferentes proveedores.

Así las cosas y de conformidad con lo establecido en el artículo 2.2.1.2.1.2.7 y subsiguientes el Decreto 1082 de 2015, las entidades estatales sometidas al Estatuto General de la Contratación se encuentran obligadas a realizar las adquisiciones de bienes y/o productos con características técnicas uniformes o no uniformes a través de los Acuerdos Marco de Precios disponibles y vigentes en la Tienda Virtual del Estado Colombiano. Igualmente, de conformidad con lo señalado en el artículo 2.2.1.2.1.2.9 del mencionado Decreto, las Entidades Públicas están obligadas a verificar la existencia de Acuerdos Marco de Precios que puedan satisfacer la necesidad identificada, la cual se pretende contratar.

Por lo anterior, durante la fase de estructuración del proceso para el año 2026, la Oficina de Tecnologías de la Información llevó a cabo una revisión exhaustiva de los Acuerdos Marco de Precios vigentes, los Instrumentos de Agregación de Demanda y los productos disponibles en la Tienda Virtual del Estado Colombiano, concluyendo que **el Acuerdo Marco de Precios** CCE-308-AMP-2022**, correspondiente a Servicios de Nube Privada IV, no permite acreditar, con base en el alcance y los componentes revisados, la satisfacción integral de la necesidad institucional relacionada con la adquisición de**

una solución especializada de Zero Trust Network Access (ZTNA) y prevención de fuga de información (DLP).

Lo anterior, teniendo en cuenta que la necesidad identificada requiere capacidades especializadas de ciberseguridad orientadas al control granular de acceso, validación contextual de usuarios y dispositivos, aplicación del principio de mínimo privilegio, segmentación de recursos tecnológicos, identificación y protección de información sensible, monitoreo de actividades y prevención de transferencias o divulgaciones no autorizadas de información institucional.

En consecuencia, **al no evidenciarse una correspondencia funcional y técnica integral entre los bienes y servicios disponibles en el Acuerdo Marco de Precios identificado y los requerimientos específicos que pretende satisfacer la Entidad, se encuentra técnicamente justificado estructurar el presente proceso de contratación mediante el mecanismo de selección que jurídicamente corresponda, de acuerdo con la naturaleza del objeto, su cuantía, las condiciones del mercado y el régimen de contratación aplicable a la entidad.**

Así las cosas, el procedimiento se llevará a cabo según lo establecido en la Ley 80 de 1993, la Ley 1150 de 2007, el artículo 2.2.1.2.1.2.2. del Decreto 1082 de 2015, modificado por el artículo 6 del Decreto 1860 de 2021 que establecen todo lo relacionado al **Procedimiento para la Subasta Inversa.**

La uniformidad técnica se fundamenta en los siguientes aspectos:

De conformidad con el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015, los bienes y servicios de características técnicas uniformes en concordancia con el literal (a) del numeral 2 del artículo 2 de la Ley 1150 de 2007 corresponden a aquellos de común utilización que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos, así:

Estandarización del licenciamiento y las cantidades requeridas. La ficha técnica identifica el licenciamiento establece una cantidad determinada de 1.800 licencias y define su vigencia. En consecuencia, los oferentes deben cotizar un mismo componente de licenciamiento, bajo condiciones equivalentes de cantidad, funcionalidad y duración, sin que existan diferencias en el alcance exigido por la Entidad.

Funcionalidades mínimas de seguridad previamente definidas. La ficha técnica establece requerimientos específicos relacionados con acceso de confianza cero, autenticación y autorización de usuarios, control granular de aplicaciones, segmentación de red, protección de información, administración de políticas de seguridad y verificación de la postura de los dispositivos. Estas funcionalidades constituyen condiciones técnicas mínimas de obligatorio cumplimiento y permiten verificar objetivamente la conformidad de las soluciones ofrecidas.

Condiciones de interoperabilidad y compatibilidad tecnológica. Se establecen requerimientos de integración con plataformas de gestión de identidades, entre ellas Active Directory, Azure Active Directory, Okta y Google Workspace, así como capacidades de integración con herramientas de gestión de eventos de seguridad (SIEM), incluyendo FortiSIEM, Microsoft Sentinel y Splunk. Estas condiciones buscan garantizar la interoperabilidad de la solución con la infraestructura tecnológica institucional y se encuentran previamente definidas como requisitos técnicos verificables, sin constituir factores adicionales de puntuación.

Parámetros comunes de desempeño y seguridad. La ficha técnica contempla condiciones relacionadas con monitoreo de sesiones, registros de actividad, gestión de certificados, inventario de dispositivos, comprobaciones de seguridad, compatibilidad con sistemas operativos, administración mediante API y disponibilidad de infraestructura de conectividad global. Estos requerimientos permiten establecer patrones mínimos de funcionamiento, desempeño y calidad que deberán cumplir los oferentes.

Homogeneidad de los servicios complementarios. Los servicios de soporte y mantenimiento se encuentran asociados al licenciamiento requerido y comprenden actividades de configuración, actualización, migración y atención de necesidades técnicas durante su vigencia. En consecuencia, dichos servicios forman parte del alcance contractual previamente determinado y no constituyen prestaciones abiertas cuya valoración dependa de criterios subjetivos de calidad.

Comparabilidad objetiva de las ofertas económicas. La definición de cantidades, vigencias, funcionalidades y servicios mínimos permite estructurar una matriz económica homogénea, en la cual los proponentes presentan sus precios sobre componentes previamente determinados. Una vez verificado el cumplimiento de los requisitos habilitantes y técnicos, la comparación económica puede realizarse sobre una misma base, utilizando el menor precio como factor de selección.

Por lo anterior, la ANLA considera técnicamente procedente estructurar la contratación mediante selección abreviada por subasta inversa, conforme al artículo 2, numeral 2, literal a), de la Ley 1150 de 2007 y las disposiciones reglamentarias del Decreto 1082 de 2015, teniendo en cuenta que las especificaciones mínimas, cantidades y condiciones de prestación se encuentran previamente determinadas y permiten efectuar una comparación económica objetiva entre ofertas que cumplan integralmente los requerimientos exigidos.

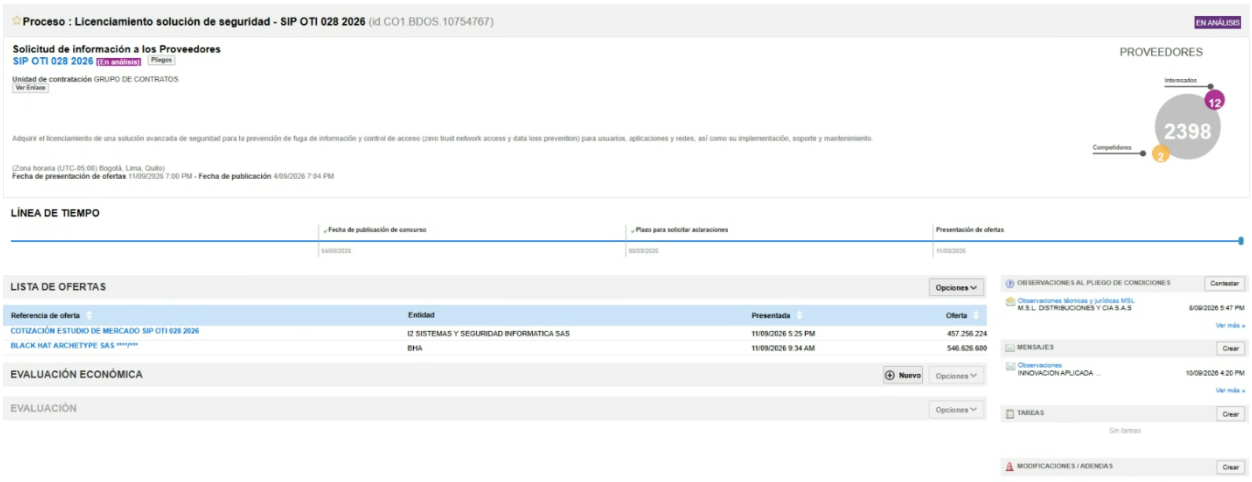
En este contexto, la competencia no se fundamentará en la asignación de puntajes por funcionalidades adicionales, características superiores o propuestas técnicas alternativas, sino en la presentación de ofertas económicas sobre una solución que satisfaga las condiciones mínimas establecidas por la Entidad.

En consecuencia, la modalidad de **Subasta Inversa** resulta coherente con la naturaleza del objeto contractual, siempre que se garantice que los requisitos técnicos definidos permitan la participación de proveedores en condiciones de competencia efectiva y que la verificación de su cumplimiento se efectúe mediante criterios objetivos y previamente establecidos.

3 VALOR ESTIMADO DEL CONTRATO Y LA JUSTIFICACIÓN DEL MISMO.

3.1. Con el fin de establecer el presupuesto para el proceso cuyo objeto es: "**10-0-7-23 ADQUIRIR EL LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION) PARA USUARIOS, APLICACIONES Y REDES, ASÍ COMO SU IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO**", la **Oficina de Tecnología de la Información** solicitó cotización por la plataforma Secop II con el **código SIP OTI 028 2026,** y mediante correo electrónico a posibles proveedores, obteniendo cotización de las siguientes empresas:

En la plataforma Secop II están relacionadas **2398 empresas** con los códigos solicitados a los cuales se les remitió solicitud de cotización, sin embargo, solo se interesaron 12 empresas y **cotizaron 2**, de acuerdo con el siguiente registro de SECOP II.



Link de consulta:
https://community.secop.gov.co/Public/Tendering/ContractNoticePhases/View?PPI=CO1.PPI.49619595&isFromPublicArea=True&isModal=False

Se presenta cuadro cotizaciones recibidas tanto por SECOP II, como a través de solicitudes directas a través de Correo Electrónico, así:

EMPRESAS COTIZANTES SIP OTI 028-2026 Y CORREO ELECTRONICO		
Entidad	**NIT**	**Medio**
Black Hat Archetype SAS	900034395	SECOP II
I2 Sistemas y Seguridad informática SAS	830036992	SECOP II
Globaltek Security SAS	830001516	Correo Electrónico
Safety IN Deep SAS	900443044	Correo Electrónico
Network & Accesories SAS	901159165	Correo Electrónico

Por su tamaño empresarial las cinco empresas están clasificadas en el segmento MiPyme, así:

TAMAÑO EMPRESARIAL			
Entidad	**NIT**	**Tamaño**	**Mi Pyme**

Black Hat Archetype SAS	900034395	Mediana Empresa	SI
I2 Sistemas y Seguridad informática SAS	830036992	Mediana Empresa	SI
Globaltek Security SAS	830001516	Mediana Empresa	SI
Safety IN Deep SAS	900443044	Mediana Empresa	SI
Network & Accesories SAS	901159165	Microempresa	SI

El Valor Total de cada cotización es el siguiente:

VALOR TOTAL EN COP$ COTIZACIÓN		
Entidad	**NIT**	**Valor COP$**
Black Hat Archetype SAS	900034395	546.626.600
I2 Sistemas y Seguridad informática SAS	830036992	457.256.224
Globaltek Security SAS	830001516	318.450.000
Safety IN Deep SAS	900443044	305.865.000
Network & Accesories SAS	901159165	313.660.000

Para determinar el presupuesto se analizó el precio unitario de cada ítem cotizado antes de IVA, obteniendo el Promedio, la Media Geométrica, la Mediana, la Desviación Estándar, los Límites Superior e Inferior, y los Valores Máximo y Mínimo, así:

ITEM 1

ANÁLISIS PRECIOS UNITARIOS EN COP$	
ÍTEM 1	
Licenciamiento de la solución avanzada de seguridad de acceso (Security Zero Trust EnterpriseBrowser) para usuarios y aplicaciones web, con componente de protección de fuga de datos junto con su respectiva suscripción de soporte de estas.	
Empresa	**Valor Unitario antes de IVA**
Black Hat Archetype SAS	289.137

I2 Sistemas y Seguridad informática SAS	215.555
Globaltek Security SAS	167.000
Safety IN Deep SAS	161.000
Network & Accesories SAS	165.000
INDICADORES	
Promedio	199.538
Media Geométrica	194.239
Mediana	167.000
Desviación Estándar	49.033
Límite Superior (Máximo Precio Razonable)	216.033
Límite Inferior (Mínimo Precio Razonable)	117.967
Valor Máximo	289.137
Valor Mínimo	161.000
Se escoge	Media geométrica
Valor COP$	194.239
Valor Para presupuesto ajustado	190.000

Para la determinación del valor unitario de referencia del ítem 1, la Autoridad Nacional de Licencias Ambientales (ANLA) efectuó un análisis estadístico de las cinco (5) cotizaciones recibidas durante el sondeo de mercado, presentadas por las empresas Black Hat Archetype S.A.S., I2 Sistemas y Seguridad Informática S.A.S., Globaltek Security S.A.S., Safety IN Deep S.A.S. y Network & Accesories S.A.S., con valores unitarios de $289.137, $215.555, $167.000, $161.000 y $165.000, respectivamente.

El análisis permitió identificar diferencias entre los precios ofertados, con un valor mínimo de $161.000 y un máximo de $289.137, lo que representa una diferencia absoluta de $128.137.

Estas variaciones pueden estar relacionadas con las condiciones comerciales, estructuras de costos, canales de distribución y márgenes de comercialización de los proveedores consultados, razón por la cual resulta pertinente utilizar herramientas estadísticas que permitan establecer un valor de referencia representativo del comportamiento del mercado.

Como resultado del análisis se obtuvo un promedio aritmético de $199.538, una media geométrica de $194.239, una mediana de $167.000 y una desviación estándar poblacional de $49.033.

Asimismo, tomando como referencia la mediana y adicionando y restando una desviación estándar, se estableció un intervalo de precios entre $117.967 y $216.033, dentro del cual se encuentran cuatro (4) de las cinco (5) cotizaciones recibidas.

La cotización de mayor valor, correspondiente a $289.137, supera el límite superior establecido, evidenciando una diferencia significativa frente al comportamiento predominante de los precios consultados.

Para establecer el valor unitario de referencia se seleccionó la media geométrica, equivalente a $194.239, por considerarse una medida estadística apropiada para el análisis de precios positivos que presentan diferencias proporcionales.

A diferencia del promedio aritmético, esta medida reduce la influencia relativa de los valores más elevados, sin excluir ninguna de las cotizaciones válidas, permitiendo obtener una estimación que incorpora la totalidad de la información económica suministrada por los proveedores.

La selección de la media geométrica resulta especialmente pertinente considerando que la cotización de mayor valor supera considerablemente las restantes y puede incrementar el promedio aritmético. Por su parte, la utilización de la mediana de $167.000 conduciría a adoptar una referencia cercana a los menores precios identificados, sin reflejar suficientemente las diferencias comerciales de la muestra.

En consecuencia, la media geométrica constituye una alternativa intermedia que permite equilibrar estas condiciones y establecer una estimación económicamente razonable, sin depender exclusivamente de los valores extremos.

Adicionalmente, el resultado de la media geométrica se encuentra dentro del intervalo de referencia establecido, lo cual constituye un elemento complementario para sustentar su selección. Su aplicación permite mantener la objetividad y trazabilidad del análisis

económico, al utilizar una metodología estadística uniforme sobre las cinco cotizaciones recibidas.

Una vez seleccionada la media geométrica, se determinó adoptar un valor unitario ajustado de **$190.000** para efectos de la estructuración del presupuesto oficial. Este ajuste corresponde a una aproximación conservadora a la decena de mil pesos inferior, que representa una disminución de $4.239 respecto del resultado estadístico seleccionado, equivalente aproximadamente al 2,18 %. La decisión permite establecer una cifra presupuestal de fácil aplicación y consolidación, sin generar incrementos sobre el valor obtenido mediante el análisis estadístico.

El ajuste efectuado mantiene la razonabilidad económica de la estimación, toda vez que el valor adoptado permanece dentro del intervalo de referencia y supera los precios presentados por tres (3) de los cinco (5) proveedores consultados. Esta circunstancia evidencia la existencia de alternativas comerciales cuyos precios se encuentran por debajo del valor presupuestado, favoreciendo la posibilidad de obtener condiciones económicas competitivas, siempre que se garantice el cumplimiento integral de las especificaciones técnicas y demás obligaciones contractuales.

En relación con el tratamiento tributario del ítem 1, el numeral 21 del artículo 476 del Estatuto Tributario establece la **exclusión del impuesto sobre las ventas (IVA)** para los servicios de suministro de páginas web, servidores (hosting) y computación en la nube (cloud computing). En concordancia con esta disposición, la Dirección de Impuestos y Aduanas Nacionales (DIAN), mediante el Concepto Unificado 017056 del 25 de agosto de 2017 y su doctrina complementaria, ha señalado que la exclusión resulta aplicable a los servicios de computación en la nube que cumplan las características, los modelos de servicio y los modelos de implementación definidos para esta modalidad tecnológica.

Para el presente proceso de contratación, las cinco (5) cotizaciones recibidas durante el sondeo de mercado coinciden en presentar los valores del ítem 1 sin incluir el impuesto sobre las ventas (IVA), lo que evidencia uniformidad en el tratamiento tributario aplicado por los proveedores consultados. En consecuencia, para efectos de la estructuración del presupuesto oficial, **se adopta el valor unitario de $190.000** sin adicionar IVA, de conformidad con las condiciones económicas reportadas por el mercado. Este tratamiento se sustenta en la exclusión prevista en el numeral 21 del artículo 476 del Estatuto Tributario, en la medida en que la solución contratada corresponda efectivamente a un servicio de computación en la nube que cumpla los requisitos técnicos y jurídicos establecidos para su aplicación. Por tanto, las cotizaciones constituyen el soporte económico de la estimación

presupuestal, mientras que la procedencia de la exclusión tributaria se fundamenta en el cumplimiento de los presupuestos establecidos en la citada disposición legal.

En conclusión, la selección de la media geométrica como referente estadístico se encuentra justificada por su capacidad para incorporar la totalidad de las cotizaciones recibidas y moderar la influencia relativa de los precios más elevados. Asimismo, el ajuste del resultado de $194.239 a $190.000 representa una reducción moderada que mantiene la estimación dentro del intervalo de referencia y responde a criterios de prudencia presupuestal, razonabilidad económica y eficiencia en la utilización de los recursos públicos.

Por lo anterior, se considera procedente adoptar el valor unitario de $190.000 para el ítem 1, como base para la estructuración del presupuesto oficial del proceso, sujeto a la validación del tratamiento tributario correspondiente.

ITEM 2

ANÁLISIS PRECIOS UNITARIOS EN COP$	
ÍTEM 2	
Suscripción de soporte y mantenimiento por un año de mil (1800) licencias de Security Zero Trust Enterprise Browser	
Empresa	**Valor Unitario antes de IVA**
Black Hat Archetype SAS	22.000.000
I2 Sistemas y Seguridad Informática S:A.S	58.199.774
Globaltek Security SAS	15.000.000
Safety IN Deep SAS	13.500.000
Network & Accesories SAS	14.000.000
INDICADORES	
Promedio	24.539.955
Media Geométrica	20.510.649
Mediana	15.000.000
Desviación Estándar	17.107.991
Límite Superior (Máximo Precio Razonable)	32.107.991

Límite Inferior (Mínimo Precio Razonable)	-2.107.991

Para el análisis económico del ítem 2, la Autoridad Nacional de Licencias Ambientales (ANLA) tomó como referencia las cinco (5) cotizaciones recibidas durante el sondeo de mercado, presentadas por las empresas Black Hat Archetype S.A.S., I2 Sistemas y Seguridad Informática S.A.S., Globaltek Security S.A.S., Safety IN Deep S.A.S. y Network & Accesories S.A.S., cuyos valores fueron de $22.000.000, $58.199.774, $15.000.000, $13.500.000 y $14.000.000, respectivamente.

Del análisis inicial se obtuvo un promedio aritmético de $24.539.955, una media geométrica de $20.510.649, una mediana de $15.000.000 y una desviación estándar poblacional de $17.107.991. Asimismo, tomando como referencia la mediana y adicionando y restando una desviación estándar, se estableció un intervalo de precios entre -$2.107.991 y $32.107.991.

Los resultados evidencian una dispersión significativa entre los valores ofertados, particularmente por la cotización presentada por I2 Sistemas y Seguridad Informática S.A.S., por valor de $58.199.774, que supera en $36.199.774 la segunda cotización más elevada, correspondiente a $22.000.000.

Adicionalmente, este valor equivale aproximadamente a 3,88 veces la mediana de las cinco cotizaciones y supera ampliamente el límite superior de referencia de $32.107.991.

La inclusión de esta cotización incrementa considerablemente el promedio aritmético, la media geométrica y la desviación estándar, generando una mayor dispersión estadística y afectando la representatividad de los indicadores utilizados para la determinación del presupuesto.

Esta situación se evidencia especialmente en el límite inferior calculado, que presenta un resultado negativo de -$2.107.991, carente de interpretación económica para la adquisición de servicios de soporte y mantenimiento, cuyos precios necesariamente deben ser positivos.

Por lo anterior, y con el propósito de establecer una referencia presupuestal que refleje de manera más adecuada el comportamiento predominante de los precios observados en el mercado, se considera técnicamente justificado **excluir** del cálculo de los indicadores estadísticos la cotización presentada por I2 Sistemas y Seguridad Informática S.A.S., al constituir un valor atípico superior que introduce una distorsión significativa en la estimación económica.

Es importante precisar que esta exclusión se realiza exclusivamente para efectos del análisis estadístico y la determinación del valor de referencia presupuestal, sin desconocer la participación de la empresa en el sondeo de mercado ni cuestionar la validez de su cotización. La decisión se fundamenta en criterios objetivos de dispersión, proporcionalidad y representatividad de los precios, y no en una valoración subjetiva del proveedor.

De acuerdo con lo expuesto los cálculos son los siguientes:

ANÁLISIS PRECIOS UNITARIOS EN COP$	
ÍTEM 2	
Suscripción de soporte y mantenimiento por un año de mil (1800) licencias de Security Zero Trust Enterprise Browser	
Empresa	**Valor Unitario antes de IVA**
Black Hat Archetype SAS	22.000.000
Globaltek Security SAS	15.000.000
Safety IN Deep SAS	13.500.000
Network & Accesories SAS	14.000.000
INDICADORES	
Promedio	24.539.955
Media Geométrica	20.510.649
Mediana	15.000.000
Desviación Estándar	17.107.991
Límite Superior (Máximo Precio Razonable)	32.107.991
Límite Inferior (Mínimo Precio Razonable)	-2.107.991
Valor Máximo	58.199.774

Valor Mínimo	13.500.000
Se escoge	Promedio
Valor COP$	24.539.955
Valor Para presupuesto ajustado	16.000.000

Para la determinación del valor de referencia del ítem 2, una vez depurada la muestra y excluida del análisis estadístico la cotización presentada por I2 Sistemas y Seguridad Informática S.A.S., se seleccionó el promedio aritmético como medida de tendencia central, considerando que los cuatro (4) valores restantes presentan una menor dispersión y permiten obtener una estimación más representativa de las condiciones económicas identificadas en el mercado.

La selección del promedio aritmético se fundamenta en que esta medida incorpora de manera proporcional la totalidad de las cotizaciones consideradas válidas para el análisis, asignando igual participación a cada una de ellas.

A diferencia de la muestra inicial, en la cual un valor considerablemente superior afectaba los resultados estadísticos, la muestra depurada presenta una distribución de precios más homogénea, circunstancia que favorece la utilización del promedio como referente para la estructuración presupuestal.

En efecto, las cuatro (4) cotizaciones consideradas corresponden a $22.000.000, $15.000.000, $13.500.000 y $14.000.000, obteniéndose un promedio aritmético de $16.125.000. Este resultado se encuentra dentro del rango de precios efectivamente observado y refleja el comportamiento conjunto de los proveedores, sin depender exclusivamente de la cotización de menor valor ni adoptar como referencia el precio más elevado de la muestra depurada.

Adicionalmente, la selección del promedio permite reconocer las diferencias comerciales existentes entre los proveedores, manteniendo una estimación equilibrada frente a las condiciones de oferta identificadas.

Si bien la cotización de $22.000.000 es superior a las otras tres, su incidencia sobre el resultado es considerablemente menor que la generada por el valor excluido de

$58.199.774, lo que permite obtener una referencia presupuestal más moderada y consistente con la información disponible.

En consecuencia, se considera técnicamente justificada la selección del promedio aritmético de $16.125.000 antes de IVA, como valor de referencia para el ítem 2, toda vez que su cálculo se fundamenta en cuatro (4) cotizaciones comparables y permite establecer una estimación económica sustentada en criterios de objetividad, razonabilidad y representatividad del mercado. Esta metodología contribuye a la adecuada estructuración del presupuesto oficial de la ANLA y favorece la utilización eficiente de los recursos públicos.

Aplicando los valores unitarios seleccionados a las cantidades requeridas y adicionando el IVA al ítem 2, se tiene el siguiente presupuesto:

Ítem	SKU	Descripción del Producto	Desde	Hasta	Cantidad	Valor unitario antes de IVA	Valor Unitario IVA Incluido	Valor Total IVA Incluido PRECIO TECHO
1	CP-SASE-BROWSER-T2-Y	Licenciamiento de la solución avanzada de seguridad de acceso (Security Zero Trust Enterprise Browser) para usuarios y aplicaciones web, con componente de protección de fuga de datos junto con su respectiva suscripción de soporte de estas.	22/12/2026	21/12/2027	1.800	190.000	190.000	342.000.000
2	No Aplica	Suscripción de soporte y mantenimiento por un año de mil (1800) licencias de Security Zero Trust Enterprise Browser	22/12/2026	21/12/2027	1	16.000.000	19.040.000	19.040.000
PRESUPUESTO EN COP$								**$ 361.040.000**

En consecuencia se tiene un presupuesto para el proceso con el "**10-0-7-23 ADQUIRIR EL LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION) PARA USUARIOS, APLICACIONES Y REDES, ASÍ COMO SU IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO**", por valor

de **TRESCIENTOS SESENTA Y UN MILLONES CUARENTA MIL PESOS M/CTE ($361.040.000)** incluido IVA contribuciones, impuestos, gastos, costos y erogaciones a que haya lugar, derivados de la prestación del objeto de este proceso.

Nota. El ítem 1, "Licenciamiento de la solución avanzada de seguridad de acceso (Security Zero Trust Enterprise Browser) para usuarios y aplicaciones web, con componente de protección de fuga de datos junto con su respectiva suscripción de soporte de estas" está exento del IVA.

Análisis de razonabilidad del precio de mercado y variación del presupuesto

Con el propósito de evaluar la razonabilidad económica del presupuesto estimado para la vigencia 2026, la Autoridad Nacional de Licencias Ambientales (ANLA) efectuó un análisis comparativo frente a los valores presupuestados en la vigencia 2025, considerando las cantidades requeridas, los precios unitarios y el valor total de los componentes que integran la solución tecnológica.

Para la vigencia 2025, el presupuesto ascendió a $309.465.000, mientras que para 2026 se estableció un valor de $361.040.000, lo que representa un incremento absoluto de $61.065.000, equivalente al 16.7 %.

En relación con el ítem 2, correspondiente a la suscripción anual de soporte y mantenimiento, el presupuesto pasó de $13.500.000 en 2025 a $16.000.000 en 2026, lo que representa un incremento absoluto de $2.500.000, equivalente al 18.5 %.

En consecuencia, se considera económicamente razonable el valor presupuestado para el ítem 2, teniendo en cuenta que su incremento absoluto responde a una ampliación significativa de la cobertura del soporte y mantenimiento.

Este resultado, sumado al respaldo obtenido mediante el sondeo de mercado, permite sustentar la estimación presupuestal bajo criterios de razonabilidad, eficiencia económica y adecuada utilización de los recursos públicos.

3.2 ANÁLISIS DEL SECTOR

Para la presente contratación la Oficina de Tecnologías de la Información de la Autoridad Nacional de Licencias Ambientales – ANLA realizó el correspondiente documento denominado "Análisis del Sector" el cual se encuentra en documento anexo al presente Estudio Previo y hace parte integral de este documento.

4 CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

De conformidad con lo establecido en el numeral 3° del artículo 5 de la Ley 1150 de 2007, en los procesos de selección cuyo objeto sea la adquisición o suministro de servicios de características técnicas uniformes y de común utilización, las entidades estatales incluirán como único factor de evaluación el **menor precio ofrecido**, a través de la modalidad de **SUBASTA INVERSA ELECTRÓNICA**.

En la fecha y hora establecidas en el cronograma de la convocatoria, se llevará a cabo la subasta inversa electrónica y adjudicación del contrato, la misma se realizará de conformidad con lo establecido en el artículo 2.2.1.2.1.2.2 y subsiguientes del Decreto 1082 de 2015, y especialmente con lo establecidos en el artículo 2.2.1.2.1.2.5. y con las reglas establecidas en el pliego de condiciones, así como también las guías establecidas por Colombia Compra Eficiente relacionadas con el Proceso de Selección Abreviada por Subasta Inversa.

El contrato se adjudicará al proponente que presente la oferta, mediante lance valido, más favorable para la entidad, es decir, la de **menor valor**.

El **margen mínimo de mejora** corresponde al **tres por ciento** (**3%**) [14]del valor de la mejor oferta inicial o del lance inmediatamente anterior. ***Si el lance está por debajo del Margen Mínimo de mejora, éste será un lance no válido.*** El porcentaje de cada lance aplica al valor total de la oferta.

Nota 1: El valor total ofertado **NO PODRÁ superar en ningún caso el Valor Total (Incluido IVA) PRECIO TECHO establecido por ítem, NI EL DEL PRESUPUESTO**

[14] **El margen mínimo de mejora** se calculó de conformidad con los lineamientos contenidos en el documento denominado "sondeo de mercado para determinar el porcentaje mínimo de lances", documento que hace parte integral del presente proceso

OFICIAL ESTIMADO y que no armonice con lo solicitado en el anexo **FICHA TÉCNICA** que para el presente proceso en la suma **TRESCIENTOS SESENTA Y UN MILLONES CUARENTA MIL PESOS M/CTE ($361.040.000)** incluido IVA y los demás impuestos, gastos, costos y erogaciones a que haya lugar, derivados de la prestación del servicio. caso en el cual **SE RECHAZARÁ LA OFERTA.**

NOTA 2: Si sólo un oferente resultare habilitado, la Entidad adjudicará el contrato a este, siempre que su oferta no exceda el monto establecido de acuerdo con el presupuesto oficial estimado para el presente proceso de contratación, en este caso **no habrá SUBASTA**., conforme a lo establecido en el Artículo 2.2.1.2.1.2.2. del Decreto 1082 de 2015, numeral 5.

4.1 OFERTA ECONÓMICA

El proponente deberá ofertar la totalidad de los bienes y/o servicios con todas las características y especificaciones señaladas en el anexo **FICHA TÉCNICA**, registrando el valor total de su oferta económica incluido IVA, y demás impuestos, costos y gastos relacionados directa o indirectamente con la ejecución del objeto, **sin que en ningún caso el valor de su oferta económica supere el valor del presupuesto oficial estimado para el presente proceso en la suma TRESCIENTOS SESENTA Y UN MILLONES CUARENTA MIL PESOS M/CTE ($361.040.000)** incluido IVA y los demás impuestos, gastos, costos y erogaciones a que haya lugar, derivados de la prestación del servicio. **En ningún caso el valor ofertado por los proponentes podrá superar el presupuesto oficial, ni el Valor Total (Incluido IVA) PRECIO TECHO, establecido por ítem** y que no armonice con lo solicitado en el anexo **FICHA TÉCNICA** caso en el cual **SE RECHAZARÁ LA OFERTA.**

El proponente presentará su oferta económica en el sobre digital denominado **SOBRE ECONÓMICO** que se encuentra en la sección **CUESTIONARIO**, establecido en la Plataforma SECOP II para tal fin, el cual es diferente al sobre digital que contiene los documentos que soportan los requisitos habilitantes jurídicos, técnicos y financieros.

La **OFERTA ECONÓMICA** deberá incluir el valor expresado en pesos colombianos, **sin decimales**, el cual, **no podrá modificarse** a parte del resultado de la subasta, desde la fecha de presentación de la propuesta, hasta el recibo definitivo de los servicios por parte de ANLA.

Serán de exclusiva responsabilidad del oferente, los errores u omisiones en que incurra al indicar el valor de su oferta económica, debiendo asumir los mayores costos y/o pérdidas que se deriven de dichos errores u omisiones, sin que por esta razón haya lugar a alegar ruptura del equilibrio económico del contrato.

Para efecto del señalamiento de la oferta económica, el oferente debe tener en cuenta todos los costos, gastos, impuestos, seguros, pago de salarios, prestaciones sociales y demás emolumentos (directos e indirectos) que considere necesarios para la fijación de la oferta económica. Serán de cargo de los oferentes todos los costos asociados con la preparación y presentación de su oferta, por tal motivo la ANLA en ningún caso será responsable de los mismos.

Para la presentación de la oferta económica, se debe tener en cuenta lo siguiente:

1. El ofrecimiento económico deberá realizarse en pesos colombianos que es la moneda oficial.

2. El proponente deberá proyectar el valor de la oferta de forma responsable, con el lleno de los requisitos técnicos exigidos en el Pliego de Condiciones.

3. Los valores unitarios y totales se deben presentar **sin decimales**, estos valores deberán aproximarse por exceso o por defecto al entero más cercano así: si es superior a 50 centavos, se aproxima al entero siguiente; si es inferior a 50 centavos se baja al entero anterior). **Nota:** Para evitar inconvenientes de decimales, se sugiere aplicar la fórmula de **REDONDEAR**.

4. El valor ofertado **no podrá ser superior al valor del presupuesto oficial ni superior al Valor Total (Incluido IVA) PRECIO TECHO establecido por ítem**, **so pena de rechazo.**

Téngase en cuenta los siguientes Valores Totales (Incluido IVA) PRECIO TECHO:

Ítem	SKU	Descripción del Producto	Desde	Hasta	Cantidad	Valor unitario antes de IVA	Valor Unitario IVA Incluido	Valor Total IVA Incluido PRECIO TECHO

1	CP-SASE-BROWSER-T2-Y	Licenciamiento de la solución avanzada de seguridad de acceso (Security Zero Trust Enterprise Browser) para usuarios y aplicaciones web, con componente de protección de fuga de datos junto con su respectiva suscripción de soporte de estas.	22/12/2026	21/12/2027	1.800	190.000	No Aplica	342.000.000
2	No Aplica	Suscripción de soporte y mantenimiento por un año de mil (1800) licencias de Security Zero Trust Enterprise Browser	22/12/2026	21/12/2027	1	16.000.000	19.040.000	19.040.000
PRESUPUESTO EN COP$								**$ 361.040.000**

5. Son de cargo del adjudicatario el pago de los derechos, impuestos, tasas y otros conceptos que genere el contrato.

6.Los valores producto del evento de Subasta, se mantendrán durante la vigencia del contrato sin reajustes.

7. Si como resultado de la verificación aritmética, el valor total de la propuesta económica señalado en la sección Propuesta Económica (Incluido IVA y demás impuestos que aplique) es superior al presupuesto oficial establecido para el presente proceso la propuesta **SERÁ RECHAZADA**.

NOTAS APLICABLES A LA OFERTA ECONOMICA:

Nota 1: Para efectos de la celebración de la Subasta, para establecer el valor inicial de la misma se tendrá en cuenta el valor total de la oferta económica de menor precio válidamente presentada.

Nota 2: Los precios contenidos en la **OFERTA ECONÓMICA** presentada mediante la Plataforma SECOP II, **NO** estarán sujetos a ajuste alguno durante el desarrollo del contrato.

Nota 3: Es obligación para la habilitación del proponente presentar la propuesta económica debidamente diligenciada.

Nota 4: Serán de exclusiva responsabilidad del oferente, los errores u omisiones en que incurra al indicar el valor de su oferta económica, debiendo asumir los mayores costos y/o pérdidas que se deriven de dichos errores u omisiones, sin que por esta razón haya lugar a alegar ruptura del equilibrio económico del contrato.

Nota 5: Para efecto del señalamiento de la oferta económica, el oferente debe tener en cuenta todos los costos, gastos, impuestos, seguros, pago de salarios, prestaciones

sociales y demás emolumentos (directos e indirectos) que considere necesarios para la fijación de la oferta económica. Serán de cargo de los oferentes todos los costos asociados con la preparación y presentación de su oferta, por tal motivo la ANLA en ningún caso será responsable de los mismos.

Nota 6: En caso de no diligenciar en el SECOP II la totalidad de los ítems que componen la propuesta económica, esto tendrá como consecuencia el **RECHAZO de la oferta**.

Nota 7: En cumplimiento del artículo 2.2.1.1.2.2.4. del Decreto 1082 de 2015 y en concordancia con lo establecido en la **Guía de Colombia Compra Eficiente para el Manejo de Ofertas Artificialmente Bajas para Procesos de Contratación**, en el evento que LA ANLA estime que el valor de una oferta resulta artificialmente bajo, requerirá al proponente para que explique las razones que sustenten el valor por él ofertado. allegadas las explicaciones, la Entidad procederá al rechazo o a permitir la continuidad de la oferta presentada en el proceso, cuando el valor de la misma responda a circunstancias objetivas que no pongan en riesgo el proceso, ni el cumplimiento de las obligaciones del contrato a celebrar, en caso de que este se adjudique a dicho proponente.

Por tratarse de un proceso mediante subasta inversa, de conformidad con lo establecido en el inciso tercero del artículo en mención, esta disposición es aplicable sobre el precio obtenido al final de la subasta.

Nota 8: Si sólo un oferente resultare habilitado, la entidad adjudicará el contrato a este, siempre que su oferta no exceda el monto establecido de acuerdo con el presupuesto oficial estimado para el presente proceso de contratación, en este caso no habrá SUBASTA, conforme a lo establecido en el Artículo 2.2.1.2.1.2.2. del Decreto 1082 de 2015, numeral 5.

Nota 9: La adquisición de bienes amigables con el medio ambiente, como estrategia para el fortalecimiento y el avance positivo de la gestión ambiental, en el sentido de contribuir al desarrollo sostenible del país y la implementación de buenas prácticas que reduzcan al mínimo los efectos o daños al medio ambiente (Emisión de gases de efecto invernadero, generación de residuos, uso de agua, energía y materias primas).

Acorde con lo anterior, la entidad puede sumarse al ejercicio de incluir en la selección y evaluación, aspectos ambientales acorde a sus necesidades, y considerar realizar el análisis de ciclo de vida del bien o servicio desde la producción hasta la posibilidad de contribución a la protección del medio ambiente (Reciclaje o reutilización), y que, a su vez, sume beneficios a nivel económico y social, sin anteponerse a las normas específicas de la contratación.

En definitiva, la adquisición de bienes amigables contribuye al Consumo Sostenible que, desde el Gobierno Nacional y los entes regulatorios, promueven por medio de políticas y planes de desarrollo, mediante cambios progresivos en la producción y consumo, logrando la integridad del medio ambiente con la competencia empresarial y la solidez de los procesos.

4.2 REQUISITOS HABILITANTES OBJETO DE VERIFICACIÓN

El proceso de verificación y evaluación se realizará de conformidad con la tabla que se especifica a continuación, en donde se relacionan los factores que serán objeto de verificación en las propuestas.

Los proponentes deberán acreditar el cumplimiento de todos y cada uno de los requisitos jurídicos, técnicos y financieros y de capacidad de organización que se establecen a continuación, de conformidad con lo dispuesto en la Ley 1150 de 2007, en el artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015 y demás normas concordantes, son objeto de verificación de cumplimiento para la participación en el proceso de selección y **no otorgarán puntaje**, así:

NUMERO	CRITERIO	CONDICIÓN
1	Requisitos jurídicos	Habilitante o descalificará la propuesta (**CUMPLE O NO CUMPLE).**
2	Requisitos mínimos de capacidad financiera y organizacional	Habilitante o descalificará la propuesta (**CUMPLE O NO CUMPLE).**
3	Requerimientos Técnicos Mínimos	Habilitante o descalificará la propuesta (**CUMPLE O NO CUMPLE).**

Tabla: Criterios de Selección

5 REQUISITOS HABILITANTES TÉCNICOS

5.1 FICHA TÉCNICA

El proponente acreditará que cumple con las condiciones y especificaciones técnicas establecidas en el presente proceso de contratación, mediante la suscripción clara, inequívoca e incondicional de la **FICHA TÉCNICA** por parte del representante legal. La **FICHA TÉCNICA** será presentada junto con la propuesta a través de la plataforma SECOP II, con la suscripción de la **FICHA TÉCNICA** el contratista acepta y se obliga a cumplir con las especificaciones técnicas establecidas por la entidad.

NOTA 1: El proponente futuro contratista podrá presentar la información y documentación adicional que estime conveniente para precisar, aclarar o concretar los ofrecimientos hechos, en ningún caso se admitirá información o documentos tendientes a mejorar la oferta, **SO PENA DE RECHAZO.**

NOTA 2: El proponente futuro contratista se compromete a no adicionar, suprimir, cambiar o modificar los ítems, la descripción, las especificaciones, el detalle, de acuerdo con lo exigido por la Entidad **SO PENA DE CONSIDERARLO COMO RECHAZO DE LA PROPUESTA.**

5.2 EXPERIENCIA MÍNIMA DEL PROPONENTE

En el presente proceso podrán participar las personas naturales o jurídicas, nacionales o extranjeros constituidos legalmente, así como aquellas que conforman consorcios o uniones temporales, consideradas legalmente capaces de conformidad con las disposiciones legales colombianas.

Igualmente, podrán participar las demás que se encuentren establecidas en el artículo 6 de la Ley 80 de1993, modificado por el artículo 1 de la Ley 2160 de 2021:

a) **Cabildos indígenas:** Para acreditar esta condición el proponente deberá aportar certificación expedida por el Ministerio del Interior, EXPEDIDO CON UNA ANTELACIÓN **MÁXIMA DE SESENTA (60)** DÍAS A LA FECHA DE CIERRE DEL PRESENTE PROCESO.
b) **Consejos comunitarios de las comunidades negras; formas de expresiones organizativas; Organizaciones de Base de Comunidades Negras, Afrocolombianas, Raizales y Palenqueras; Organizaciones de Segundo Nivel,**

Asociaciones de Autoridades Tradicionales Indígenas: Para acreditar cualquiera de las anteriores formas de organización, deberá aportar una certificación expedida por el Ministerio del Interior, **CON UNA ANTELACIÓN MÁXIMA DE SESENTA (60) DÍAS A LA FECHA DE CIERRE DEL PRESENTE PROCESO**. Estas organizaciones deberán contar con diez (10) años o más de haber sido incorporados por el Ministerio del Interior en el correspondiente Registro Público Único Nacional y que hayan cumplido con el deber de actualización de información en el mismo registro; aplica para los consorcios y uniones temporales.

El proponente debe acreditar hasta tres (3) certificaciones de contratos ejecutados y finalizados con empresas públicas o privadas dentro de los cinco (5)[15] años anteriores al cierre del proceso de selección, que reúnan las siguientes condiciones:

1. El objeto de los contratos u obligaciones deberá estar relacionado con lo siguiente: **VENTA O INSTALACIÓN DE SOLUCIONES DE HERRAMIENTAS DE SEGURIDAD INFORMATICA O SOFTWARE DE PREVENCIÓN DE PERDIDA DE INFORMACIÓN.**
2. La sumatoria de los contratos acreditados expresada en SMMLV debe ser igual o superior al 100% del presupuesto oficial estimado, esto es **206,2** SMLMV.
3. Los contratos deben estar ejecutados y terminados
4. Cada contrato debe estar registrado en el Registro Único de Proponentes RUP, acorde con el Clasificador de Bienes y Servicios de Naciones Unidas, mínimo hasta el tercer nivel y deberá estar inscritos en al menos **uno (1)** de los códigos UNSPSC descritos en el cuadro relacionado.

CÓDIGO	SEGMENTO	FAMILIA	CLASE
43222500	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
81112200	Servicios bajados en ingeniería, Investigación y tecnología	Servicios Informáticos	Mantenimiento y soporte de Software

[15] Se precisa que para efectos de acreditar la experiencia los oferentes deben presentar certificaciones de contratos ejecutados en los últimos 5 años , atendiendo a la obsolescencia tecnológica, es decir, para evitar la devaluación de un bien debido al progreso tecnológico, lo cual sucede usualmente cuando una nueva tecnología o un nuevo producto sustituyen a otro más antiguo, situación está que se presenta específicamente en lo que respecta al software y la tecnología

Nota: Teniendo en cuenta que en el RUP el código solo se puede registrar hasta el tercer nivel, en el presente numeral solo se desagrega hasta nivel de clase.

Las certificaciones cargadas en la Plataforma SECOP II, deberán cumplir mínimo con los siguientes requisitos:

a. Nombre de la entidad y/o empresa contratante
b. Persona o empresa a la que certifican.
c. Objeto y/o descripción de las actividades realizadas en el contrato
d. Fecha de inicio del contrato
e. Fecha de terminación del contrato
f. Valor del contrato (incluido IVA de ser el caso)
g. Porcentaje de participación en caso de unión temporal o consorcio
h. Estar debidamente suscrita por quien la expida.

Adicionalmente, y con el fin de verificar y validar la información de la experiencia que se certifica, el oferente deberá diligenciar y cargar a través de la plataforma SECOP II, el Anexo - "Verificación de Experiencia Proponentes" del pliego de condiciones, indicando la relación de la experiencia relacionada y el registro en el mencionado RUP.

NOTAS APLICABLES:

Nota 1: En el caso de propuestas presentadas por proponentes plurales se deberá adjuntar y cargar en el SECOP II, un documento con la tabla del anexo citado para cada uno de los integrantes. La experiencia y el valor, será la sumatoria de la experiencia y valor que acrediten cada uno de los integrantes, por lo menos uno de los integrantes del proponente plural debe acreditar la experiencia requerida en este numeral. Es decir, para efectos de acreditar la experiencia requerida, el proponente plural podrá hacerlo mediante la sumatoria de la experiencia y los valores acreditados por sus integrantes. Así mismo, se entenderá acreditado el requisito cuando uno solo de los integrantes acredite, por sí mismo, la totalidad de la experiencia y el valor mínimo exigidos en el presente numeral. En consecuencia, no será necesario que cada uno de los integrantes acredite individualmente la totalidad de la experiencia y el valor requeridos, siempre que, en conjunto, se cumpla con los requisitos establecidos o que uno de los integrantes los acredite en su totalidad.

Nota 2: No podrá acumularse a la vez, la experiencia de los socios y la de la persona jurídica cuando éstos se asocien entre sí para presentar propuesta bajo alguna de las modalidades previstas en el artículo 7 de la Ley 80 de 1993.

Nota 3: En el evento de proponente extranjero no obligado a estar inscrito en el RUP, el mismo deberá adjuntar igualmente el anexo EXPERIENCIA MÍNIMA DEL PROPONENTE adjuntando las respectivas certificaciones las cuales deberán contener la información mínima previamente indicada.

Nota 4: Cuando las certificaciones expresen su valor en dólares, se tendrá en cuenta la TRM a la fecha en que se celebró el contrato certificado, la cual será la certificada por el Banco de la Republica.

Nota 5: En el evento en que las certificaciones de contratos suscritos con **entidades estatales**, en las que se incluya la fecha de terminación o la anotación de que el contrato ha sido ejecutado, no contengan la información prevista de forma precedente, la misma podrá ser complementada aportando copia del contrato **y/o** acta de liquidación.

Nota 6: En caso de que la certificación de contratos suscritos con **entidades estatales** no establezca que el contrato se encuentra debidamente ejecutado o la fecha de terminación del mismo y si esta certificación carece de algunos de los requerimientos establecidos de forma precedente, los mismos podrán ser complementados anexando contrato **y** acta de liquidación. No se aceptará uno u otro documento, sino que necesariamente debe remitirse ambos.

Nota 7: De igual manera, si los contratos certificados son suscritos con **entidades privadas**, las certificaciones aportadas que no incluyan cualquiera de los datos anteriormente descritos podrá aportarse para complementar la información copia del contrato **o** cualquier documento en el cual se constate la ejecución del contrato.

Nota 8: Cuando el proponente individual o integrante de un consorcio o unión temporal sea una filial o subordinada de una sociedad controlante, se tendrá en cuanta SOLAMENTE la experiencia propia y no la de la controlante, ni viceversa.

Nota 9: De acuerdo con el literal 2.5 del artículo 2.2.1.1.1.5.2. del Decreto 1082 de 2015: "Si la constitución del interesado es menor a tres (3) años, puede acreditar la experiencia de sus accionistas, socios o constituyentes.".

Nota 10: Para efectos de lo establecido en el presente numeral, la ANLA se reserva el derecho a verificar directamente, cuando lo considere necesario, la información que suministren los oferentes sobre su experiencia.

Nota 11: Conforme a la CIRCULAR EXTERNA ÚNICA Código: CCE-EICP-MA-06 del 27 de diciembre de 2023 expedida por la Agencia Nacional de Contratación Pública, para que los documentos en un idioma distinto al castellano puedan ser apreciados en el Proceso de Contratación deben ser presentados en su lengua original junto con la traducción oficial al castellano. El proponente puede presentar con la oferta documentos con una traducción simple y entregar la traducción oficial al castellano dentro del plazo previsto para la subsanación. La traducción oficial debe ser el mismo texto presentado. Debe tenerse en cuenta que, cuando un documento es presentado en un idioma distinto al castellano, debe ser traducido y, para tales fines, se aplicarán las siguientes reglas: (i) si es un documento

privado que requiere de traducción, no será indispensable que sea traducción oficial, de acuerdo con el numeral 15 del artículo 25 de la Ley 80 de 1993; (ii) si es un documento público que requiere de apostilla o legalización, y estos trámites se van a realizar ante las autoridades colombianas, se requerirá la autenticación ante notario público de la firma del traductor del documento, en los términos del artículo 6 de la Resolución 1959 de 2020; y (iii) si es un documento público que requiere de apostilla o legalización, y ésta ya se realizó ante autoridades diferentes a las colombianas, se requerirá traducción siempre que el idioma sea diferente al castellano, sin que sea necesario traducción oficial ni autenticación ante notario público, en aplicación del numeral 15 del artículo 25 de la Ley 80 de 1993, y del numeral 5 del artículo 9 de la Ley 1437 de 2011, según se explicó antes.

Nota 12: No podrá acumularse a la vez, la experiencia de los socios y la de la persona jurídica cuando éstos se asocien entre sí para presentar propuesta bajo alguna de las modalidades previstas en el artículo 7 de la Ley 80 de 1993.

Nota 13: En el evento en que las certificaciones no incluyan cualquiera de los datos solicitados, podrá aportarse para complementar la información copia del contrato acompañado de su respectiva acta de liquidación debidamente suscrita, siempre y cuando el contrato sea sujeto de liquidación de lo contrario se aportará copia simple del mismo.

Nota 14: Para verificar el valor de los contratos certificados, la ANLA hará la conversión al valor del SMMLV del año de celebración del respectivo contrato

.

5.2.1. ACREDITACION DE EXPERIENCIA PARA PROPONENTES EXTRANJEROS SIN SUCURSAL EN COLOMBIA

Los proponentes extranjeros no obligados para registrarse en el RUP, para acreditar su experiencia, deberán diligenciar el Anexo dispuesto en el pliego de condiciones **Anexo - "Verificación de Experiencia Proponentes"** para cada una de las experiencias, el cual debe estar suscrito por el Representante Legal y cargado a través de la plataforma SECOP II.

Igualmente, se debe adjuntar hasta tres **(3) certificaciones** de contratos ejecutados en donde se evidencie que la experiencia reportada sea directamente relacionada con contratos que cumplan con las condiciones de experiencia habilitante requeridas, junto con el acta de liquidación o cualquier documento idóneo donde se pueda verificar que el objeto y alcance tenga relación igual a similar con el objeto señalado, y el valor de la sumatoria de los contratos deberá ser igual o superior **206.2 SMMLV.**

Los objetos de los contratos que se reporten en el **Anexo - "Verificación de Experiencia Proponentes"** dispuesto por la entidad deben corresponder con el objeto del presente proceso de selección.

En caso de que alguna información referente a la acreditación de experiencia obtenida en un país extranjero no esté acreditada de la manera que se exige en la presente convocatoria, se deberá aportar el documento o documentos equivalentes, de los cuales se pueda obtener la información requerida, debidamente apostillados o legalizados de conformidad con las reglas establecidas en la Convención de la Haya.

APLICACIÓN CRITERIOS DE SEGURIDAD Y SALUD EN EL TRABAJO Y DE GESTIÓN AMBIENTAL

Para efectos de la implementación de criterios de sostenibilidad, se validó en el instructivo GC-MN-01 Guía de Criterios en Seguridad, Salud y Ambiente para la Selección y Evaluación de Contratistas y Proveedores, de acuerdo con el proceso contractual a ejecutar, para lo cual se remitió correo electrónico al Grupo de Gestión Administrativa y al Grupo de Gestión Humana, los cuales hacen parte del presente documento.

En cuanto a los **CRITERIOS DE GESTIÓN AMBIENTAL,** el Grupo de Gestión Administrativa precisó que, cuando el objeto contractual corresponda **exclusivamente a la adquisición de bienes, NO se requiere diligenciar el anexo de Cumplimiento Ambiental para Proveedores, código GA-FO-83.** En consecuencia, dicho documento **NO SE EXIGE** como requisito habilitante en el presente proceso de contratación, considerando la naturaleza de su objeto contractual. Esta determinación se encuentra debidamente sustentada y justificada en el documento **Análisis del Sector**.

En relación con los **CRITERIOS DE SEGURIDAD Y SALUD EN EL TRABAJO – SST,** EL Grupo de Gestin Humana establece lo siguiente:

5.3 CERTIFICADO DE CUMPLIMIENTO DE LAS DISPOSICIONES CONTENIDAS EN EL DECRETO 1072 DE 2015 Y LA RESOLUCIÓN 0312 DE 2019 DEL MINISTERIO DEL TRABAJO

En aplicación a lo contenido en el Manual de Criterios en Seguridad, Salud y Ambiente para la Selección y Evaluación de Contratistas y Proveedores, el oferente se compromete a dar estricto cumplimiento a todas las disposiciones contenidas en el Decreto 1072 de 2015 y la Resolución 0312 de 2019 del Ministerio del Trabajo, sobre los aspectos mínimos que el empleador debe tener en cuenta en materia de seguridad y salud el trabajo en las contrataciones de personal que haga, para lo cual diligenciará y suscribirá el **"ANEXO - CERTIFICADO DE CUMPLIMIENTO DE LAS DISPOSICIONES CONTENIDAS EN EL DECRETO 1072 DE 2015 Y EN LA RESOLUCIÓN 0312 DE 2019 DEL MINISTERIO DE TRABAJO"** o el documento que haga sus veces.

5.4 CRITERIOS DIFERENCIADORES PARA MIPYMES

En aplicación al artículo 2.2.1.2.4.2.18 del Decreto 1860 de 2021, se definió por parte de la Entidad un criterio diferenciador para las empresas Mipyme, así:

El proponente que sea Mipyme debe acreditar **hasta cuatro (4) certificaciones de contratos ejecutados** con empresas públicas o privadas que reúnan las condiciones anteriormente relacionadas en la experiencia mínima del proponente.

Para la acreditación de la condición de Mipyme, el proponente deberá aportar una certificación, que se entenderá presentada bajo la gravedad de juramento, suscrita por el Revisor Fiscal en los casos en que la sociedad este obligada a tenerlo, o un Contador Público y el Representante Legal de la empresa, junto con los siguientes documentos:

Las personas naturales: Mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil.

Las personas jurídicas: Mediante certificación expedida por el representante legal y el contador o por el revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación.

Para la acreditación deberán observarse los rangos de clasificación empresarial establecidos de conformidad con la Ley 590 de 2000 y el Decreto 1074 de 2015, o las normas que lo modifiquen, sustituyan o complemente.

En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación.

Los proponentes plurales: Por lo menos uno de los integrantes deberá acreditar la calidad de Mipyme y deberá tener una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

5.5 CRITERIOS DIFERENCIALES A FAVOR DE LOS EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD:

En aplicación a lo contenido en el Artículo 2.2.1.2.4.2.7.3 del Decreto 1082 de 2015, modificado por el Artículo 1 del Decreto 287 de 2026, se definió por parte de la Entidad un criterio diferenciador para los emprendimientos y empresas de personas con discapacidad, así:

El proponente que reúna las condiciones establecidas en el Artículo 1 del Decreto 287 de 2026 debe acreditar **hasta (4) certificaciones** que acredite:

- ✓ **Personas naturales con discapacidad que hayan realizado actividades comerciales a través un establecimiento de comercio, durante al menos el año anterior al cierre del proceso de selección:**

  La circunstancia se acreditará mediante la copia de la cédula de ciudadanía, la cédula de extranjería o el pasaporte, el certificado de discapacidad expedido de acuerdo a la normativa del Ministerio de Salud y Protección Social, así como la copia del registro mercantil.

- ✓ **Personas jurídicas donde más del 50% de sus acciones, partes de interés o cuotas de participación pertenezcan a personas con discapacidad y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del proceso de selección**. La circunstancia de propiedad de la persona jurídica se acreditará mediante certificación expedida por el representante legal y el revisor fiscal cuando exista, de acuerdo con los requerimientos de ley o, el contador donde conste la distribución los derechos en la sociedad y el tiempo en el que personas con discapacidad han mantenido su participación Adicionalmente se debe adjuntar la copia de la cédula de ciudadanía, extranjería o el pasaporte, el certificado de

discapacidad expedido la normativa del Ministerio de Salud y Protección Social, así como la copia del certificado de existencia y representación legal.

- ✓ **Personas jurídicas que tengan vinculadas laboralmente al menos una persona con discapacidad en empleos del nivel directivo de la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel**. Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde se señale de manera detallada las personas con discapacidad que ocupan cargos de nivel directivo del proponente y el tiempo de vinculación.

La certificación deberá relacionar el nombre completo y el número de documento de identidad de las personas con discapacidad que ocupan cargos de nivel directivo del proponente. Como soporte, se anexará copia de los respectivos documentos de identidad, copia de los contratos de trabajo o certificación laboral con las funciones, así como el certificado de aportes a seguridad social del último año en el que se demuestren los pagos realizados por el empleador, y el certificado de discapacidad expedido de acuerdo con la normativa del Ministerio de Salud y Protección Social.

Respecto de los incentivos contractuales para los emprendimientos y empresas de personas con discapacidad, las certificaciones de que trata el presente artículo deben expedirse bajo la gravedad de juramento con una fecha de máximo treinta (30) días calendario anteriores a la prevista para el cierre del proceso de selección.

Proponentes Plurales: Tratándose de proponentes plurales, estas condiciones solo se aplicarán cuando al menos uno de los integrantes cumpla con los criterios previstos en el artículo 2.2.1.2.4.2.6. del Decreto 1082 del 2015, modificado por el decreto 287 de 2026, y acredite una participación no inferior al diez por ciento (10%) en el consorcio o la unión temporal, aportando la experiencia requerida, como mínimo, en una proporción equivalente a su participación en la conformación del proponente plural.

5.6. CERTIFICACIONES ADICIONALES

Teniendo en cuenta las características técnicas del objeto a contratar, el proponente junto con su propuesta deberá anexar.

- Certificación expedida por el fabricante CHECK POINT dirigida a la **AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES – ANLA cuya fecha de expedición no podrá ser mayor a treinta (30) días calendario anteriores al cierre del proceso**, en la que conste que el proponente cuenta con la calidad de canal oficial autorizado y que certifique venta y distribución de soluciones de CHECK POINT 3 Estrellas o superior

Nota 1: Para proponentes plurales, es suficiente con que uno de sus miembros acredite la certificación anteriormente mencionada, siempre que por parte del proponente se cumpla con todos y cada uno de los anteriores requisitos.

Nota 2: Conforme a la CIRCULAR EXTERNA ÚNICA Código: CCE-EICP-MA-06 del 27 de diciembre de 2023 expedida por la Agencia Nacional de Contratación Pública, para que los documentos en un idioma distinto al castellano puedan ser apreciados en el Proceso de Contratación deben ser presentados en su lengua original junto con la traducción oficial al castellano. El proponente puede presentar con la oferta documentos con una traducción simple y entregar la traducción oficial al castellano dentro del plazo previsto para la subsanación. La traducción oficial debe ser el mismo texto presentado.

Nota 3: Debe tenerse en cuenta que, cuando un documento es presentado en un idioma distinto al castellano, debe ser traducido y, para tales fines, se aplicarán las siguientes reglas: (i) si es un documento privado que requiere de traducción, no será indispensable que sea traducción oficial, de acuerdo con el numeral 15 del artículo 25 de la Ley 80 de 1993; (ii) si es un documento público que requiere de apostilla o legalización, y estos trámites se van a realizar ante las autoridades colombianas, se requerirá la autenticación ante notario público de la firma del traductor del documento, en los términos del artículo 6 de la Resolución 1959 de 2020; y (iii) si es un documento público que requiere de apostilla o legalización, y ésta ya se realizó ante autoridades diferentes a las colombianas, se requerirá traducción siempre que el idioma sea diferente al castellano, sin que sea necesario traducción oficial ni autenticación ante notario público, en aplicación del numeral 15 del artículo 25 de la Ley 80 de 1993, y del numeral 5 del artículo 9 de la Ley 1437 de 2011, según se explicó antes.

NO CONFIGURACIÓN DE TERCERIZACIÓN LABORAL DEL PROCESO EN LOS TÉRMINOS DEL DECRETO 0581 DEL 5 DE JUNIO DE 2026

Del análisis efectuado sobre la naturaleza, el objeto y las condiciones de ejecución del presente proceso de contratación, se concluye que este no configura una modalidad de tercerización laboral en los términos previstos en el Decreto 0581 del 5 de junio de 2026. Lo anterior, teniendo en cuenta que la **naturaleza jurídica del negocio corresponde a un contrato de compraventa**, cuyo objeto está orientado a la adquisición de bienes y no a la provisión de personal o al desarrollo de actividades mediante esquemas de intermediación o tercerización laboral.

Así mismo, la ejecución del objeto contractual estará a cargo del contratista, quien actuará con autonomía técnica, administrativa, financiera y operativa, y asumirá bajo su propia responsabilidad la organización y ejecución de las actividades necesarias para el cumplimiento de las obligaciones pactadas, sin que ello implique la configuración de una relación de naturaleza laboral con la Entidad.

En consecuencia, al no evidenciarse los presupuestos fácticos y jurídicos que permitan identificar la configuración de tercerización laboral en el presente proceso, se determina que este riesgo no resulta aplicable y, por tanto, no se incorpora en la matriz de riesgos. Esta decisión atiende a los principios de pertinencia, proporcionalidad y razonabilidad en la gestión del riesgo, procurando que la matriz contemple aquellos eventos que, de acuerdo con la naturaleza, el alcance y las condiciones de ejecución del contrato, puedan materializarse e incidir en el cumplimiento de las obligaciones contractuales.

6. REQUISITOS HABILITANTES JURÍDICOS

Este ítem no dará puntaje, habilitará o descalificará la propuesta. **(CUMPLE O NO CUMPLE)**.

6.1 CARTA DE PRESENTACIÓN DE LA OFERTA (Ver Anexo del Pliego de Condiciones)

El proponente debe dirigir una comunicación a ANLA, mediante la cual de forma expresa hace entrega de una propuesta para participar en el presente proceso de selección y se compromete a suscribir el contrato y a ejecutarlo en el evento que le sea adjudicado.

Esta carta deberá estar firmada por la persona natural oferente o por el representante legal de la persona jurídica, o por la persona designada para representar al consorcio o unión temporal, cuando de ello se trate.

Los oferentes podrán tomar y suscribir el modelo suministrado en el formato anexo al Pliego de Condiciones. En todo caso, si los oferentes utilizan otro modelo, este deberá contener mínimo la información solicitada en dicho formato del Pliego de Condiciones.

Nota: En el evento que la oferta se presente a través de apoderado, éste debe encontrarse debidamente facultado para participar en el proceso de contratación y suscribir el contrato que se derive de éste.

Cuando se trate de personas naturales o jurídicas extranjeras sin domicilio o sucursal en Colombia, deberán además acreditar un apoderado domiciliado en Colombia debidamente facultado para realizar el ofrecimiento, de ser necesario presentar la propuesta, participar y comprometer a su representado en las diferentes instancias del proceso de selección, suscribir los documentos y declaraciones que se requieran, así como el contrato, suministrar la información que le sea solicitada, y demás actos necesarios de acuerdo con la convocatoria, y representarlo judicial o extrajudicialmente.

Dicho apoderado podrá ser el mismo apoderado único para el caso de personas extranjeras que participen en consorcio o unión temporal, y en tal caso, bastará para todos los efectos, la presentación del poder común otorgado por todos los integrantes del consorcio o unión temporal con los requisitos relacionados con la autenticación, consularización y traducción; particularmente con lo exigido en el Código de Comercio de Colombia.

El poder a que se refiere este párrafo podrá otorgarse en el mismo acto de constitución del consorcio o unión temporal.

La carta de presentación deberá cumplir los siguientes requisitos: 1) Debe contener todas las manifestaciones y declaraciones que contiene el anexo correspondiente del pliego de condiciones; 2) El proponente NO podrá señalar condiciones diferentes a las establecidas en el pliego de condiciones. 3) Será rechazada la propuesta sometida a condiciones para celebrar el contrato.

6.2 CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL O SU EQUIVALENTE

En el presente proceso se podrán presentar personas jurídicas, uniones temporales o consorcios. Las personas jurídicas nacionales y extranjeras deberán acreditar que su duración es como mínimo, igual a la del plazo de ejecución del contrato que se derive y un (1) año más contado a partir de la fecha del cierre del proceso de selección.

Igualmente, podrán participar las demás que se encuentren establecidas en el artículo 6 de la Ley 80 de 1993, modificado por el artículo 1 de la Ley 2160 de 2021.

El objeto social del proponente o de los miembros del proponente si acuden bajo cualquiera de las figuras asociativas autorizadas por la Ley 80 de 1993, **debe ser acorde con el objeto de la presente convocatoria**.

a) Para Proponentes Nacionales:

Certificado de Existencia y Representación legal de la Cámara de Comercio: Para las personas jurídicas o su equivalente, **EXPEDIDO CON UNA ANTELACIÓN MÁXIMA DE SESENTA (60) DÍAS CONTADOS DESDE LA FECHA DE CIERRE DEL PRESENTE PROCESO**, en el que se pueda verificar que el objeto social sea acorde con el de la presente contratación y que su duración no sea inferior al plazo de ejecución del contrato y por lo menos un (1) año más.

Cuando sea una persona natural comerciante, Registro Mercantil expedido por la Cámara de Comercio o por la entidad competente, en el que se pueda verificar que las actividades sean acordes con el objeto de la presente contratación, **CON UNA ANTELACIÓN MÁXIMA DE SESENTA (60) DÍAS CONTADOS DESDE LA FECHA DE CIERRE DE LA CONVOCATORIA.**

En el caso de que se encuentre desarrollando actividades como actos no mercantiles descritos en el artículo 23 del Código de Comercio cómo, por ejemplo, la prestación de servicios inherentes a las profesiones liberales no está obligado a inscribirse en el registro mercantil, razón por la cual podrá aportar el Registro Único Tributario – RUT

b) Para Proponentes Extranjeros:

Para sucursales de sociedades extranjeras establecidas en Colombia el certificado de Existencia y Representación legal de la Cámara de Comercio, **EXPEDIDO CON UNA ANTELACIÓN MÁXIMA DE SESENTA (60) DÍAS A LA FECHA DE CIERRE DEL PRESENTE PROCESO**, en el que se pueda verificar el objeto social y que su constitución es de por lo menos de un (1) año antes a la fecha de cierre del presente proceso; así mismo, que su duración no sea inferior al plazo de ejecución del contrato y por lo menos un (1) año

más.

Para personas jurídicas extranjeras sin sucursal en Colombia, deberá aportar los documentos previstos por la legislación del país de origen para acreditar su capacidad jurídica, existencia y representación, expedidos por el funcionario competente, el cual deberá contener como mínimo lo siguiente: razón social, representante legal y facultades del mismo, objeto social y domicilio social, duración de la sociedad no inferior al plazo de ejecución del contrato y un (1) año más.

Cuando se trate de personas naturales extranjeras sin domicilio en el país o de personas jurídicas privadas extranjeras que no tengan establecida sucursal en Colombia, deberá acreditar la constitución de un apoderado (Poder Especial), domiciliado y residente en Colombia, debidamente facultado para presentar la propuesta y celebrar el contrato, así como para representarla administrativa, judicial o extrajudicialmente.

NOTA 1: En el evento de resultar favorecido con la adjudicación un proponente extranjero sin domicilio, ni sucursal en Colombia, para efectos de poder ejecutar el contrato deberá previamente constituir una sucursal en Colombia en los términos del Código de Comercio, de acuerdo con lo señalado en los Artículos 471 y 474.

c) Para Consorcios o Uniones Temporales: Modelo Acuerdo de Consorcio o Unión Temporal (ver Anexo del Pliego de Condiciones)

En caso de consorcios o uniones temporales conformados por personas jurídicas, se debe cargar a través de la plataforma de SECOP II, el documento que acredite la existencia y representación legal de cada uno de sus integrantes, **EXPEDIDOS CON UNA ANTELACIÓN MÁXIMA DE SESENTA (60) DÍAS A LA FECHA DE CIERRE DEL PRESENTE PROCESO.**

Igualmente, deberá cargar a través de la plataforma de SECOP II, el acta de constitución según el formato establecido como anexo del Pliego de Condiciones (Ver formato anexo “modelo de acuerdo de consorcio o unión temporal”). En caso de utilizar otro formato, el proponente plural debe garantizar que incluirá la información establecida en el anexo “modelo de acuerdo de consorcio o unión temporal”, y donde conste por lo menos lo siguiente:

1. Identificación de los integrantes del consorcio o unión temporal.

2. Indicación de la participación a título de CONSORCIO o UNIÓN TEMPORAL
3. Designación de la persona, que, para todos los efectos, representará al consorcio o la unión temporal, así como su suplente.
4. Indicación de las reglas básicas que regulen las relaciones entre los miembros del consorcio o la unión temporal y sus respectivas responsabilidades.
5. Precisar cuál es el porcentaje de participación de cada uno de los integrantes.
6. Si se trata de una UNIÓN TEMPORAL, señalar los términos y extensión de la participación de cada uno de los integrantes en la propuesta y en su ejecución, los cuales no podrán ser modificados sin el consentimiento de la Entidad.
7. Señalar el término de duración del CONSORCIO o de la UNION TEMPORAL, el cual no puede ser inferior al término de ejecución del contrato y por tres (3) años más. En todo caso, se debe indicar que durante el término de ejecución del contrato y hasta el año siguiente a la expiración del plazo contractual o de su prórroga si la hubiere, el consorcio o la unión temporal no podrá ser disuelto o liquidado. De igual forma, la fecha de constitución del consorcio o unión temporal debe ser anterior al plazo para presentar oferta.
8. El objeto social de las personas jurídicas integrantes de un proponente plural les debe permitir adelantar las actividades del proceso de contratación, sea como parte de su objeto social o ser una actividad conexa a éste. Los representantes legales de las personas jurídicas integrantes del proponente plural deben estar plenamente facultados para comprometer a la persona jurídica en el cumplimiento de la totalidad del objeto del contrato, puesto que la responsabilidad es solidaria frente a la Entidad Estatal.
9. En caso de **resultar favorecidos con la adjudicación para la suscripción del contrato, deberá tramitar** y presentar el respectivo Registro Único Tributario – RUT del consorcio o unión temporal ante la entidad competente para ello y posteriormente presentarlo ante la Entidad Estatal.
10. Los integrantes del consorcio o unión temporal no podrán ceder parcial, ni totalmente sus derechos a terceros, sin obtener la autorización previa, expresa y escrita de la ANLA. En ningún, caso podrá haber cesión parcial o total del contrato, entre quienes integran el consorcio o unión temporal.

Nota 1: Es indispensable señalar la duración del Consorcio o Unión Temporal, la cual no podrá ser inferior a la del plazo de ejecución y liquidación del contrato y tres (3) años más.

En caso de requerirse aclaraciones sobre los términos consignados en el documento de conformación del consorcio o unión temporal, la Entidad requerirá al proponente y le fijará el plazo dentro del cual deba presentarlas. En el caso de no entregar las aclaraciones dentro del plazo establecido, la oferta será **rechazada**.

En atención a lo dispuesto en el artículo 11 del Decreto 3050 de 1997, los integrantes del Consorcio o Unión Temporal en el documento de constitución y para efectos del pago, en relación con la facturación deben manifestar:

1. Si la va a efectuar en representación del consorcio o la unión temporal uno de sus integrantes, caso en el cual debe informar el número del NIT de quien factura.
2. Si la facturación la van a presentar en forma separada cada uno de los integrantes del consorcio o la unión temporal, caso en el cual deben informar el número de NIT de cada uno de ellos y la participación de cada uno en el valor del contrato.
3. Si la va realizar el consorcio o unión temporal con su propio NIT, caso en el cual se debe indicar el número. Además, se debe señalar el porcentaje o valor del contrato que corresponda a cada uno de los integrantes, el nombre o razón social y el NIT de cada uno de ellos.

Celebrado el contrato, queda convenido que no podrá haber cesión del mismo entre los miembros que integren el consorcio. Cuando se trate de cesión a terceros, se requerirá de la autorización previa, expresa y escrita de la Entidad.

d) Cabildos indígenas: Para acreditar esta condición el proponente deberá aportar certificación expedida por el Ministerio del Interior, **EXPEDIDO CON UNA ANTELACIÓN MÁXIMA DE SESENTA (60) DIAS CONTADOS DESDE LA FECHA DE CIERRE DE LA CONVOCORIA**.

e) Consejos comunitarios de las comunidades negras; formas de expresiones organizativas; Organizaciones de Base de Comunidades Negras, Afrocolombianas, Raizales y Palenqueras; Organizaciones de Segundo Nivel, Asociaciones de Autoridades Tradicionales Indígenas: Para acreditar cualquiera de las anteriores formas de organización, deberá aportar una certificación expedida por el Ministerio del Interior, **CON UNA ANTELACIÓN MÁXIMA DE SESENTA (60) DIAS CONTADOS DESDE LA FECHA DE CIERRE DE LA CONVOCATORIA.** Estas organizaciones deberán contar con diez (10) años o más de haber sido incorporados por el Ministerio del Interior en el correspondiente Registro Público Único Nacional y que hayan cumplido con el deber de actualización de información en el mismo registro; aplica para los consorcios y uniones temporales.

6.3. AUTORIZACIÓN DE LA JUNTA DIRECTIVA DE SOCIOS O ASAMBLEA GENERAL

El representante legal del proponente persona jurídica debe estar autorizado para presentar la propuesta y suscribir el contrato.

Si del certificado de Cámara de Comercio se desprende que las facultades del

representante legal se encuentran limitadas para presentar la propuesta o para firmar el respectivo contrato, se deberán anexar los estatutos y la correspondiente autorización de la Junta Directiva, de Socios o Asamblea General, que lo faculte específicamente para presentar la propuesta en este proceso de selección y celebrar el contrato respectivo, en caso de resultar seleccionado.

En el caso de Consorcios o Uniones Temporales o Promesa de Sociedad Futura, todos sus integrantes en forma individual deberán cumplir con este requisito.

6.4. REGISTRO ÚNICO DE PROPONENTES

Por disposición del artículo 6 de la Ley 1150 de 2007, modificado por el artículo 221 del Decreto Ley 019 de 2012 y en concordancia con el artículo 2.2.1.1.1.5.1. del Decreto 1082 de 2015, todas las personas naturales o jurídicas nacionales o extranjeras con domicilio en Colombia que aspiren a celebrar contratos con las entidades estatales deberán estar inscritas en el Registro Único de Proponentes.

Para tal efecto, el interesado deberá presentar el documento correspondiente expedido por la Cámara de Comercio de su jurisdicción, con fecha de expedición **NO MAYOR A SESENTA (60) DÍAS DE ANTERIORIDAD AL CIERRE DEL PRESENTE PROCESO,** en el cual conste su inscripción en el Registro Único de Proponentes (RUP).

Para la fecha de cierre del proceso el proponente **deberá estar inscrito en el Registro Único de proponentes, esté deberá estar vigente y en firme**, salvo las excepciones establecidas en la Ley.

Cuando el proponente sea un Consorcio o Unión Temporal, para la verificación de cumplimiento de los requisitos exigidos por la Entidad en el RUP, todos los miembros deberán acreditar la inscripción en el Registro Único de Proponentes.

El artículo 2.2.1.1.1.5.1. del Decreto Reglamentario 1082 de 2015 establece que las personas inscritas en el RUP deben presentar la información para renovar su registro a más tardar el quinto día hábil del mes de abril de cada año, pues de lo contrario cesan los efectos del RUP.

Al cierre del procedimiento de selección, es decir, hasta el plazo para presentar ofertas, el **RUP debe encontrarse vigente y en firme, esto es, que el proponente haya presentado la información para renovar el registro en el término legal establecido**.

Tratándose del trámite de renovación, la persona que haya presentado la información para renovar su registro a más tardar el quinto día hábil del mes de abril, cumpliendo con el requisito exigido en el artículo 2.2.1.1.1.5.1. del Decreto Reglamentario 1082 de 2015, puede participar en los procedimientos de selección, debiéndose tener en cuenta la información antigua, esto es, la información que estuviera en firme antes del cierre del proceso.

Para verificar que los efectos del RUP no han cesado, en los eventos que el proponente presentó la información para renovar su registro, es necesario que el certificado contenga la anotación de que el inscrito, a más tardar el quinto día hábil de abril de cada año, radicó ante la cámara de comercio los documentos para su renovación.

En todo caso, si tal circunstancia no estuviese inscrita en el certificado, podrá acreditarse mediante el medio documental expedido por la cámara de comercio correspondiente. De este modo, al no existir tarifa legal que permita establecer la forma de acreditar el trámite de renovación, la entidad estatal debe verificar que el documento aportado por el proponente ofrezca certeza sobre el estado del trámite[16].

6.5. CERTIFICACIÓN DE CUMPLIMIENTO DE APORTES AL SISTEMA GENERAL DE SEGURIDAD SOCIAL INTEGRAL Y PARAFISCALES (VER ANEXO DEL PLIEGO)

El proponente persona jurídica debe presentar certificación expedida por el representante legal o por el revisor fiscal si por ley está obligado a tenerlo, mediante la cual deje constancia de que se encuentra al día en el pago de sus obligaciones al Sistema de Seguridad Social en Salud, Pensión y Riesgos Laborales, así como en lo que atañe a aportes parafiscales (Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar – ICBF y Servicio Nacional de Aprendizaje –SENA).

El término respecto del cual se debe expedir y presentar la certificación mencionada, debe ser el siguiente:

[16] Circular_externa_única_versión_3_vf49.pdf

a) Si se trata de una **persona jurídica**, durante el lapso equivalente al exigido para que se hubiere constituido la sociedad, el cual en todo caso no puede ser inferior a los **seis (6) meses anteriores al cierre del proceso**.

b) En el evento en que la sociedad **no tenga más de seis (6) meses de constituida**, deberá acreditar los pagos a partir de la fecha de su constitución.

Si el proponente es un consorcio o una unión temporal, cada uno de sus integrantes deberá presentar esta certificación.

Si el proponente es persona natural, deberá allegar la certificación de encontrarse afiliado y activo en los Sistemas de Salud, Pensiones, Riesgos Laborales, Cajas de Compensación Familiar, ICBF y SENA, éstos últimos cuando a ello hubiere lugar, y la constancia de pago del mes anterior al del cierre del proceso de selección. Dicha certificación debe tener fecha de expedición **no mayor** a **cinco (5) días hábiles anteriores** a la fecha de cierre de este proceso.

La obligación de presentar las certificaciones de cumplimiento del artículo 50 de la Ley 789 de 2002 no aplica para personas jurídicas extranjeras, salvo que participen sucursales de éstas legalmente constituidas en Colombia, caso en el cual deberán presentar la certificación mencionada en el segundo párrafo de este numeral o una certificación del Revisor Fiscal en la que manifieste que la sucursal no tiene empleados y, por lo tanto, no deben cumplir con lo señalado en la Ley 789 de 2002.

La Entidad se reserva el derecho de verificar con las respectivas Entidades la información que suministran los proponentes. Si se advierten discrepancias entre la información suministrada y lo establecido por la Entidad, se solicitarán las aclaraciones de rigor.

Nota 1: La certificación debe estar suscrita por quien corresponda, en caso de ser el revisor fiscal deberá allegar la fotocopia legible de la cédula de ciudadanía en el formato vigente, según la Registraduría Nacional del Estado Civil, la cual es amarilla de hologramas y/o Cedula de Ciudadanía Digital, la cual se aceptará como documento válido el archivo PDF que se descarga desde la página web de la Registraduría Nacional del Estado Civil y/o copia de la cédula de ciudadanía de seguridad física personalizada en policarbonato. así como la copia de la tarjeta profesional y el certificado de antecedentes emitido por la Junta Central de Contadores.

Lo anterior aplica la persona jurídica que se presente como proponente, y cada uno de los miembros del consorcio o unión temporal que se constituya para el efecto.

Nota 2: En caso de que el proponente no tenga personal a cargo y, por ende, no esté obligado a efectuar el pago de seguridad social y aportes parafiscales en relación con personal, debe así indicarlo en la certificación expedida por el Revisor Fiscal o por el Representante Legal o por el proponente persona natural, según el caso; éstos últimos bajo la gravedad del juramento, el cual se entiende prestado con la presentación de la oferta.

6.6. FOTOCOPIA DEL DOCUMENTO DE IDENTIFICACIÓN DEL PROPONENTE O DEL REPRESENTANTE DE LA PERSONA JURÍDICA, CONSORCIO O UNIÓN TEMPORAL.

Toda persona natural que funja como oferente en el presente proceso de contratación, deberá cargar a través de la plataforma del SECOP II, una copia legible de su cédula de cédula de ciudadanía en el formato vigente, según la Registraduría Nacional del Estado Civil, la cual es amarilla de hologramas y/o Cedula de Ciudadanía Digital, en archivo PDF. Igualmente, lo deberá hacer el representante legal de la persona jurídica que se presente como proponente y su apoderado de ser el caso, y cada uno de los miembros del consorcio o unión temporal que se constituya para el efecto.

Para personas extranjeras sin domicilio en Colombia, acreditará su existencia mediante una copia de su pasaporte vigente.

Para personas extranjeras domiciliadas en Colombia, deberán cargar a través de la plataforma del SECOP II, una copia de su cédula de extranjería del proponente persona natural y/o apoderado o del representante legal, sí es persona jurídica.

6.7. CERTIFICADO DIGITAL DE DEFINICIÓN DE LA SITUACIÓN MILITAR.

Cuando el oferente sea una **persona natural** propietaria de establecimiento de comercio, la Entidad validará en la Página del Comando de Reclutamiento y Control Reservas el certificado de definición de la situación militar.

NOTA: En caso de que la Libreta Militar haya sido expedida con número de tarjeta de identidad, la proponente persona natural, deberá aportar copia de la libreta militar, con el fin de validar la situación militar.

6.8. DECLARACIÓN JURAMENTADA DE NO INCLUSIÓN EN LISTAS VINCULANTES Y RESTRICTIVAS DE LAVADO DE ACTIVOS, FINANCIACIÓN DEL TERRORISMO Y PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA (LA *(Lavado de Activos)* /FT *(Financiación del Terrorismo)* / FPADM *(Financiamiento de la Proliferación de Armas de Destrucción Masiva).* (VER ANEXO DEL PLIEGO DE CONDICIONES).

Toda persona natural que funja como oferente en el presente proceso de contratación, así como el representante legal de la persona jurídica, o de consorcio o unión temporal, deberá cargar a través de la plataforma del SECOP II, una declaración expresa, bajo la gravedad del juramento, que ni la empresa, ni él, se encuentran incluidos en listas VINCULANTES Y RESTRICTIVAS DE LAVADO DE ACTIVOS, FINANCIACIÓN DEL TERRORISMO Y PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA (LA *(Lavado de Activos)* /FT *(Financiación del Terrorismo)* / FPADM *(Financiamiento de la Proliferación de Armas de Destrucción Masiva.*

6.9. COMPROMISO DE TRANSPARENCIA (VER ANEXO DEL PLIEGO DE CONDICIONES)

Los proponentes deberán cargar a través de la plataforma del SECOP II, debidamente diligenciado y firmado, el formato denominado Anexo - Compromiso de Transparencia del presente proceso.

En caso de consorcio o unión temporal esta declaración deberá ser, además, suscrita por el representante legal de cada uno de los integrantes que lo conforman.

6.10. ANTECEDENTES DISCIPLINARIOS, FISCALES Y JUDICIALES Y CONSULTA EN EL REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS.

La Entidad verificará los antecedentes fiscales, disciplinarios y judiciales, a través de los certificados expedidos por la Contraloría General de la República, la Procuraduría General de la Nación y la Policía Nacional.

Igualmente, y de acuerdo con el artículo 183 de la Ley 1801 de 2016, la Entidad realizará la consulta de medidas correctivas a través del portal ofrecido por la Policía Nacional a la fecha de la evaluación del presente proceso de selección.

En el caso de consorcios o uniones temporales, se realizarán las mismas verificaciones para cada uno de sus integrantes.

6.11. GARANTIA DE SERIEDAD DE LA PROPUESTA

EL PROPONENTE para la presentación de la propuesta deberá constituir garantía de seriedad del ofrecimiento a favor del **FONDO NACIONAL AMBIENTAL / AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES – FONAM/ANLA**, **identificado con NIT 830.025.267-9,** en cualquiera de las modalidades contenidas el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, con el objeto de amparar el ofrecimiento hecho en el presente proceso de selección.

El valor de esta garantía será equivalente **al DIEZ (10%)** por ciento del valor del presupuesto oficial del proceso de contratación que corresponde a la suma de **TRESCIENTOS SESENTA Y UN MILLONES CUARENTA MIL PESOS M/CTE ($361.040.000),** La garantía debe estar vigente desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato y en todo caso se extenderá hasta la aprobación de la garantía que ampara los riesgos propios de la etapa contractual, en cualquiera de las modalidades contenidas en el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015.

El proponente debe allegar con su propuesta la garantía de seriedad de la propuesta.

Si la oferta se **presenta en forma conjunta**, es decir, bajo la modalidad de CONSORCIO O UNIÓN TEMPORAL, la garantía **debe ser otorgada por todos sus integrantes.**

Si el proponente es **persona natural y tiene establecimiento de comercio**, el tomador debe ser la persona natural y no su establecimiento de comercio.

En caso de que la fecha de cierre del proceso se selección se amplíe, debe tenerse en cuenta la nueva fecha para efecto de la vigencia de la póliza.

La garantía de seriedad de la oferta cubrirá los perjuicios derivados del incumplimiento del ofrecimiento, en los siguientes eventos:

- ✓ La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el plazo para la adjudicación o para suscribir el contrato es prorrogado, siempre que tal prorroga sea inferior a tres (3) meses.
- ✓ El retiro de la oferta después de vencido el plazo fijado para la presentación de las ofertas.
- ✓ La no suscripción del contrato sin justa causa por parte del proponente seleccionado.
- ✓ La falta de otorgamiento por parte del proponente seleccionado, de la garantía de cumplimiento del contrato.

6.12. CERTIFICADO DE REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS - REDAM

De conformidad con lo dispuesto en la Ley 2097 de 2021, La persona natural propietaria de establecimiento de comercio y/o el representante legal de la persona jurídica que se presente como proponente **deberá aportar el Certificado Registro de Deudores Alimentarios Morosos (REDAM), el cual debe estar vigente al momento de presentación de la oferta** y del cual la Entidad realizará la verificación en la Plataforma.

6.13. ACUERDO DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN PARA COLABORADORES DE LA ANLA (VER ANEXO DEL PLIEGO DE CONDICIONES)

Lo proponentes deberán cargar a través de la plataforma del SECOP II, debidamente diligenciado y firmado, el formato denominado Anexo - **Acuerdo de Confidencialidad y Seguridad de la Información para Colaboradores de la ANLA**.

En caso de consorcio o unión temporal esta declaración deberá ser, **además**, suscrita por el representante legal de cada uno de los integrantes que lo conforman.

NOTAS APLICABLES A LOS DOCUMENTOS DE LA PROPUESTA:

1. Conforme a la CIRCULAR EXTERNA ÚNICA Código: CCE-EICP-MA-06 del 27 de diciembre de 2023, expedida por la Agencia Nacional de Contratación Pública, para que los documentos en un idioma distinto al castellano puedan ser apreciados en el Proceso de Contratación deben ser presentados en su lengua original junto con la traducción oficial al castellano. El proponente puede presentar con la oferta documentos con una traducción simple y entregar la traducción oficial al castellano dentro del plazo previsto para la subsanación. La traducción oficial debe ser el mismo texto presentado.

2. La Entidad se reserva el derecho a verificar, cuando lo considere necesario, la información que suministren los oferentes sobre su experiencia.

3. Todos los documentos expedidos en el exterior por un funcionario público en ejercicio de sus funciones o por un particular en el ejercicio de funciones públicas, deben ser apostillados o legalizados por la Entidad competente desde el país de origen, para que puedan surtir efectos legales en Colombia. En armonía con lo anterior, los documentos públicos expedidos en el exterior por un país signatario de la Convención de La Haya de 1961, sobre la abolición del requisito de legalización, deben apostillarse; por su parte, los documentos públicos expedidos en países respecto de los cuales no resulte aplicable el Convenio de la Haya de 1961 deberán surtir el trámite de legalización correspondiente de conformidad con la normatividad aplicable.

4. Para el trámite de la apostilla o legalización de dichos documentos, debe tenerse en cuenta lo establecido en la Resolución No. 1959 del 3 de agosto de 2020, “Por la cual se dictan disposiciones en materia de apostilla y de legalización de documentos y se deroga la Resolución 10547 del 14 de diciembre de 2018”, expedida por el Ministerio de Relaciones Exteriores de la República de Colombia, o la norma que la adicione, modifique o sustituya.

5. Por otro lado, los documentos privados expedidos en el exterior no requieren ser apostillados o legalizados. Sin perjuicio de lo anterior, de acuerdo con la Resolución del párrafo precedente, para efectos de la apostilla o legalización, los documentos privados deberán contener certificación oficial de un servidor público o de un particular en ejercicio de funciones públicas, que avale la firma o la entidad que lo emite

7. REQUISITOS DE CAPACIDAD FINANCIERA Y ORGANIZACIONAL (HABILITANTES)

De conformidad con el artículo 2.2.1.1.1.6.1. del Decreto 1082 del 26 de mayo de 2015, las Entidades Estatales deben hacer, durante la etapa de planeación, el análisis necesario para conocer el sector relativo al objeto del Proceso de Contratación desde la perspectiva legal,

comercial, **financiera, organizacional,** técnica, y de análisis de riesgo, los cuales deben constar en los documentos del proceso contractual.

Así mismo, el artículo 2.2.1.1.1.6.2 del Decreto 1082 del 26 de mayo de 2015, adicionado parcialmente en el Parágrafo Transitorio por el artículo 6 del Decreto 399 de 2021 y sustituido en el Parágrafo Transitorio por el artículo 3 del Decreto 579 de 2021, prevé la manera como las Entidades Estatales deben establecer los requisitos habilitantes, así:

"(…)

ARTÍCULO 2.2.1.1.1.6.2. Determinación de los Requisitos Habilitantes. *La Entidad Estatal debe establecer los requisitos habilitantes en los pliegos de condiciones o en la invitación, teniendo en cuenta: (a) el Riesgo del Proceso de Contratación; (b) el valor del contrato objeto del Proceso de Contratación; (c) el análisis del sector económico respectivo; y (d) el conocimiento de fondo de los posibles oferentes desde la perspectiva comercial. La Entidad Estatal no debe limitarse a la aplicación mecánica de fórmulas financieras para verificar los requisitos habilitantes.*

"PARÁGRAFO TRANSITORIO: *De conformidad con los parágrafos transitorios de los artículos 2.2.1.1.1.5.2. y 2.2.1.1.1.5.6., y en desarrollo del deber de análisis de las Entidades Estatales, de que trata el artículo 2.2.1.1.1.6.1. de este Decreto, a partir del 1 de julio de 2021 las Entidades Estatales establecerán y evaluarán los requisitos habilitantes de capacidad financiera y organizacional teniendo en cuenta la información que conste en el Registro Único de Proponentes. En todo caso, se establecerán indicadores proporcionales al procedimiento de contratación.*

Para ello, atendiendo a las condiciones aludidas, en relación con los indicadores de la capacidad financiera y organizacional, de los procesos de selección cuyo acto administrativo de apertura o invitación se publique a partir del 1 de julio de 2021, se tendrá en cuenta la información vigente y en firme en el RUP, por lo que las Entidades Estatales evaluarán estos

(…)"

Teniendo en cuenta que las Entidades Estatales deben evaluar los requisitos habilitantes de capacidad financiera y organizacional en atención al Registro Único de Proponentes -RUP-, el Decreto 1082 de 2015 prevé en su artículo 2.2.1.1.1.5.3. que las cámaras de comercio en Colombia deben verificar y certificar, entre otros requisitos habilitantes, los siguientes:

"(…)

3. Capacidad Financiera *- los siguientes indicadores miden la fortaleza financiera del interesado:*

3.1. Índice de liquidez: activo corriente dividido por el pasivo corriente.
3.2. Índice de endeudamiento: pasivo total dividido por el activo total.

3.3. Razón de cobertura de intereses: utilidad operacional dividida por los gastos de intereses.

***4. Capacidad Organizacional** - los siguientes indicadores miden el rendimiento de las inversiones y la eficiencia en el uso de activos del interesado:*
4.1. Rentabilidad del patrimonio: utilidad operacional dividida por el patrimonio.
4.2. Rentabilidad del activo: utilidad operacional dividida por el activo total. (Decreto 1510de 2013, artículo 10)

(…)"

Así pues, conforme a los presupuestos legales antes expuestos, el GGFP procederá a establecer los indicadores de capacidad financiera y organizacional del Proceso de Selección Abreviada de Subasta Inversa cuyo objeto es: "*10-0-7-26 - Fortalecer el sistema de gestión de seguridad de la información SGSI para la Autoridad Nacional de Licencias Ambientales ANLA a través de las herramientas especializadas (licenciamiento de software y soporte) de monitoreo FORTISIEM, de monitoreo de red SOLARWINDS, de mesa de ayuda ARANDA; así como la contratación de servicios especializados de un centro de operación de seguridad (SOC)",* a partir de la información que consta en los Registros Únicos de Proponentes – RUP- de treinta y dos (32) empresas relativas al sector -remitidas por la Oficina de Tecnologías de la información y a las cuales se realiza la verificación de los indicadores idóneos para el proceso. Dicha información fue extraída del portal web del Registro Único Empresarial y Social -RUES-En cuanto a los indicadores de capacidad financiera y organizacional, se tendrá en cuenta el último año fiscal anterior a la inscripción o renovación del RUP y la verificación de este se hará tal como lo establece la metodología previamente dispuesta por Colombia Compra Eficiente, para las propuestas presentadas por consorcios o uniones temporales la verificación de los indicadores de Capacidad Financiera y Capacidad Organizacional se hará respecto al porcentaje de participación de cada integrante dentro del proponente plural y la metodología utilizada será la establecida por Colombia Compra Eficiente. (Todos los integrantes deberán adjuntar los estados financieros para realizar la verificación correspondiente). Para este caso la ANLA medirá los índices de capacidad financiera y organizacional que resulta del análisis conjunto de las empresas que integran la Unión temporal y no de manera individual.

Bajo esta metodología y de acuerdo con la solicitud que radicó la Oficina de Tecnologías de la Información, a través del Memorando interno identificado con radicado ANLA No.20261305419773 del 10 de septiembre de 2026, el GGFP procede a establecer los indicadores de capacidad financiera y organizacional del Proceso de Selección Abreviada de Subasta Inversa cuyo objeto es: *"10-0-7-26 - Fortalecer el sistema de gestión de seguridad de la información SGSI para la Autoridad Nacional de Licencias Ambientales ANLA a través de las herramientas especializadas (licenciamiento de software y soporte) de monitoreo FORTISIEM, de monitoreo de red SOLARWINDS, de mesa de ayuda ARANDA; así como la contratación de servicios especializados de un centro de operación de seguridad (SOC)*", así:

CAPACIDAD FINANCIERA

ÍNDICE DE LIQUIDEZ:

IL = Activo Corriente / Pasivo Corriente (Decreto 1082 de 2015)

Permite establecer la cuantía del activo disponible que soporta las obligaciones a corto plazo.
Se determinará dividiendo el activo corriente, sobre el pasivo corriente.

Es la razón más utilizada para medir la solvencia a corto plazo, e indica el grado en el cual los derechos de los acreedores a corto plazo se encuentran cubiertos por activos que se espera que se conviertan en efectivo en un periodo más o menos igual al del vencimiento de las obligaciones.

El análisis de liquidez permite estimar la capacidad de la empresa para atender sus obligaciones en el corto plazo. Es decir, el dinero en efectivo de que dispone, para cancelar las deudas.

Cuanto mayor sea el valor de esta razón, mayor será la capacidad de la empresa de pagar sus deudas.

Por lo general, el resultado de la razón circulante debe estar entre los valores 1 y 2 para considerarse aceptable. Un valor de este índice menor que 1 indica que la empresa puede declararse en suspensión de pagos y deberá hacer frente a sus deudas a corto plazo teniendo que tomar parte del Activo Fijo.

De acuerdo con el estudio realizado se propone solicitar un índice de liquidez mayor o igual a **1.39**

El cual garantiza una solvencia suficiente del oferente participante para atender sus obligaciones en el corto plazo

ÍNDICE DE ENDEUDAMIENTO:

IE = (Pasivo Total / Activo Total) (Decreto 1082 de 2015)

Define el porcentaje que representa el compromiso con terceros, garantizado en el activo total. Se determina el nivel de endeudamiento tomando el pasivo total y se divide entre el activo total.

El índice de endeudamiento mide el riesgo financiero de la empresa e indica su capacidad de endeudamiento. (Ideal <1)

Su valor será inferior (lo más recomendable) o a lo sumo igual a 1, por encima de este valor aumentará el riesgo de la empresa.

Los indicadores de endeudamiento tienen por objeto medir en qué grado y de qué forma participan los acreedores dentro del financiamiento de la empresa. De la misma manera, se

trata de establecer el riesgo que corren tales acreedores, el riesgo de los dueños y la conveniencia o inconveniencia de un determinado nivel de endeudamiento para la empresa.

Se propone solicitar un índice de endeudamiento menor o igual a **0.70** que es el valor promedio de endeudamiento de la muestra seleccionada.

Consideramos que este valor es adecuado y no pone en riesgo la capacidad de ejecución del contrato, manteniendo el equilibrio entre la sana participación y la garantía en la ejecución del objeto contractual.

RAZÓN DE COBERTURA DE INTERESES:

RCI = Utilidad Operacional / Gastos de Intereses (Decreto 1082 de 2015)

Es el número de veces que la utilidad operacional cubre los gastos financieros. Establece la incidencia que tienen los gastos financieros sobre las utilidades operacionales de la empresa.

Esta razón es muy útil para determinar si un prestatario será capaz de dar servicio a los pagos de intereses sobre un préstamo. Indica cuantas veces podemos pagar los intereses generados en el periodo. Mide la capacidad de una compañía para dar servicio a la deuda.

Se propone solicitar una razón de cobertura de intereses mayor o igual a **1.00**

Para aquellos casos en que los proponentes no presenten gastos de intereses se tendrá en cuenta como resultado del indicador, el mínimo índice requerido por la entidad, siempre y cuando este indicador se establezca en el RUP como INDETERMINADO. En los eventos en que no se señale así en dicho documento, el proponente deberá adjuntar una certificación emitida por el Revisor Fiscal en la cual certifique que efectivamente la empresa no presenta gastos de intereses con anterioridad a un periodo contable.

CAPACIDAD ORGANIZACIONAL

RENTABILIDAD DEL PATRIMONIO:

RP = Utilidad Operacional / Patrimonio (Decreto 1082 de 2015)

Quiere decir esto que los socios o dueños de la empresa obtuvieron un rendimiento sobre su inversión de X.

Este indicador señala, como su nombre lo indica, la tasa de rendimiento que obtienen los propietarios de la empresa, respecto de su inversión representada en el patrimonio registrado contablemente:

Maximizar este ratio es el principal objetivo de cualquier firma ya que expresa el porcentaje de remuneración que puede ofrecerse a los capitales propios (representados por el patrimonio), mostrando el lucro que los accionistas están obteniendo por su inversión.

Se propone solicitar una rentabilidad del patrimonio mayor o igual a **0.13**

RENTABILIDAD DEL ACTIVO:

RA = Utilidad Operacional / Activo Total (Decreto 1082 de 2015)

El retorno sobre activos mide la capacidad efectiva de la firma para remunerar a todos los capitales puestos a su disposición, sean propios (patrimonio) o ajenos (pasivos), que la conforman. Ésta es una medida más adecuada de rentabilidad, ya que muestra su retorno operativo por cada peso de capital invertido en ella.

Se propone solicitar una rentabilidad del activo mayor o igual a **0.06**

CAPACIDAD FINANCIERA

FACTORES DE VERIFICACIÓN	CONDICIÓN HABILITANTE
Índice de liquidez	MAYOR O IGUAL A 1.39
Índice de endeudamiento	MENOR O IGUAL A 0.70
Razón de cobertura de intereses	MAYOR O IGUAL A 1.00

CAPACIDAD ORGANIZACIONAL

FACTORES DE VERIFICACIÓN	CONDICIÓN HABILITANTE
Rentabilidad del patrimonio	MAYOR O IGUAL A 0.13
Rentabilidad del activo	MAYOR O IGUAL A 0.06

NOTAS APLICABLES A LA VERIFICACIÓN FINANCIERA Y ORGANIZACIONAL:

NOTA 1: Para el caso de las propuestas presentadas por consorcios o uniones temporales, la verificación de los indicadores de Capacidad Financiera y Capacidad Organizacional se hará respecto al porcentaje de participación de cada integrante dentro del proponente plural (Todos los integrantes deberán adjuntar el Registro Único de Proponentes (RUP) para realizar la verificación correspondiente).

NOTA 2: La propuesta será aceptada siempre que al aplicar cada uno de los indicadores anteriormente enunciados, su resultado cumpla la condición de aceptada, es decir que de su verificación se halla obtenido como resultado: **HABILITADA**.

NOTA 3: Cuando el proponente no cumpla con alguno de los índices en la verificación financiera, esta será considerada como **NO HABILITADA**, por lo tanto, no continua en el proceso de selección.

NOTA 4: Las personas naturales o jurídicas extranjeras sin domicilio o sucursal en Colombia, no están obligadas a estar inscritas en el Registro Único de Proponentes (RUP), por lo cual, la ANLA verificará directamente el cumplimiento de los requisitos habilitantes, para el efecto deberán diligenciar, suscribir y cargar en la plataforma del SECOP II, el Anexo denominado "VERIFICACIÓN DE CAPACIDAD FINANCIERA Y ORGANIZACIONAL PARA PROPONENTES EXTRANJEROS NO OBLIGADOS A ESTAR INSCRITOS EN EL RUP" del pliego de condiciones.

NOTA 5: Los oferentes extranjeros no obligados a tener Registro Único de Proponentes (RUP) deben cargar a través de la plataforma del SECOP II, sus estados financieros a la fecha de corte establecida en los países de origen o en sus estatutos sociales. Los mismos deberán estar en la moneda legal del país en el cual fueron emitidos y adicionalmente en pesos colombianos. El proponente y la Entidad para efectos de acreditar y verificar los requisitos habilitantes tendrán en cuenta la tasa representativa del mercado vigente en la fecha en la cual los estados financieros fueron expedidos. Para el efecto, el proponente y la Entidad tendrán en cuenta las tasas de cambio certificadas por la Superintendencia Financiera.

8. ANÁLISIS DE RIESGO Y LA FORMA DE MITIGARLO.

Con arreglo a lo establecido en el artículo 4º de la Ley 1150 de 2007, el artículo 2.2.1.1.1.6.3 del Decreto 1082 de 2015 y en los lineamientos del Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación expedido por Colombia Compra Eficiente, respecto del presente proceso de selección, La Autoridad Nacional de Licencias Ambientales - **ANLA** ha tipificado, estimado y asignado los siguientes riesgos previsibles desde su planeación hasta la liquidación del contrato:

Valoración del Riesgo

			Impacto			
	Categoría	Valoración	Insignificante	Menor	Moderado	Mayor	Catastrófico
			1	2	3	4	5
Probabilidad	Raro (puede ocurrir excepcionalmente)	1	2	3	4	5	6
	Improbable (puede ocurrir ocasionalmente)	2	3	4	5	6	7
	Posible (puede ocurrir en cualquier momento futuro)	3	4	5	6	7	8
	Probable (probablemente va a ocurrir)	4	5	6	7	8	9
	Casi cierto (ocurre en la mayoría de circunstancias)	5	6	7	8	9	10

Categoría del Riesgo

Valoración del Riesgo	Categoría
8, 9 y 10	Riesgo extremo
6 y 7	Riesgo alto
5	Riesgo medio
2, 3 y 4	Riesgo bajo

Fuente: Manual para la identificación y Cobertura del Riesgo en los Procesos de Contratación- Colombia Compra Eficiente[17].

MATRIZ DE RIESGOS

[17] https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documents/cce_manual_cobertura_riesgo.pdf

No.	Clase	Fuente	Etapa	Tipo	DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Calificación Total	Categoría
1	General	Especifico	Selección	Jurídico	Riesgo derivado de la declaratoria de desierto.	Retrasa la adjudicación del contrato objeto de selección, se retrasa la satisfacción de la necesidad, lo que a su vez provoca la no disponibilidad oportuna del licenciamiento requerido para la operación de la solución de seguridad, comprometiendo la continuidad de las medidas de protección de acceso y control de la información, incrementando la posibilidad de fuga de la información. Adicionalmente, podría impactar la eficiencia de los servicios tecnológicos de la Entidad y generar afectaciones en el cumplimiento de las políticas de seguridad de la información establecidas.	3	4	7	Alto
2	Especifico	Interno	Planeación	Operacional	Adjudicar el contrato a empresas no idóneas	No cumplimiento de las actividades técnicas requeridas en el ANEXO - FICHA	2	2	4	Bajo

No.	Clase	Fuente	Etapa	Tipo	DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Calificación Total	Categoría
						TÉCNICA del estudio previo.				
3	Especifico	Interno	Ejecución	Operacional	Ocurrencia de errores de funcionamiento de software especializado adquirido no reportados previamente	Comportamiento errado del software, resultados inesperados.	3	5	8	Alto
4	Específico	Interno	Ejecución	Operacional	Que el licenciamiento adquirido y su soporte no cumplan con las especificaciones técnicas requeridas.	No cumplimiento de las actividades técnicas requeridas en la ficha técnica del estudio previo	3	4	7	Bajo
5	Especifico	Externo	Ejecución	Operacional	Incumplimiento de las obligaciones generales y especificas del contrato y del ANEXO - FICHA TÉCNICA.	Manipulación o pérdida de información vital de la ANLA Sanciones disciplinarias. Parálisis en el normal funcionamiento de las dependencias	3	3	6	Alto
6	General	Interno	Planeación	Operacional	Que el presupuesto asignado para el proceso no sea suficiente de acuerdo con el estudio de mercado	Que el proceso de contratación no se pueda realizar.	3	5	8	Medio
7	General	Interno	Planeación	Operacional	Que los estudios previos y el pliego de condiciones sean confusos y	Que no se presenten oferentes.	3	5	8	Medio

No.	Clase	Fuente	Etapa	Tipo	DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Calificación Total	Categoría
					no esté soportado técnicamente					

La siguiente es la forma de mitigación de los riesgos anteriores:

MATRIZ DE MITIGACIÓN DE RIESGOS

No.	¿A quién se le asigna?	Tratamiento/ Controles a ser implementados	Impacto después del tratamiento			¿Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Monitoreo y revisión	
			Probabilidad	Impacto	Calificación Total			¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
1	ANLA	Aclarar los requisitos, requerimientos y especificaciones y productos del contrato para establecer adecuadamente el presupuesto oficial a partir del análisis del el estudio de mercado	2	4	6	SI	Área solicitante	Verificación de los Requerimientos técnicos de la entidad definidos en la Ficha Técnico	Desde la etapa de planeación del proceso hasta la publicación del mismo.
2	ANLA	Definir claramente los requisitos habilitantes (jurídicos, financieros y técnicos) en los pliegos de condiciones, conforme a la normatividad vigente.	1	4	4	NO	Designados para la evaluación de ofertas.	Verificación de las actividades relacionadas con la evaluación de los oferentes, con el fin de que las mismas, se desarrollen conforme a lo establecido en los pliegos de	Desde la etapa precontractual y durante la evaluación de las ofertas.

No.	¿A quién se le asigna?	Tratamiento/ Controles a ser implementados	Impacto después del tratamiento			¿Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Monitoreo y revisión	
			Probabilidad	Impacto	Calificación Total			¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
		Verificar el cumplimiento documental de los requisitos de experiencia, capacidad técnica y respaldo del fabricante o distribuidor autorizado, según corresponda. Aplicar criterios de evaluación objetivos y verificables, asegurando que la adjudicación se realice únicamente a oferentes que cumplan la totalidad de los requerimientos establecidos.						condiciones y la normatividad vigente.	
3	Contratista	Utilizar la última versión estable. Ejecutar las actualizaciones indicadas por el fabricante.	2	4	6	NO	Área Solicitante	Supervisor del contrato	Inicio del plazo de ejecución del contrato
4	ANLA	Establecer de Manera clara desde el estudio de mercado y en los Estudios Previos los requerimientos técnicos con los que debe contar la garantía y soporte	2	4	6	SI	Área solicitante	Identificar de manera exacta el problema que quiere solucionar la entidad a través de la adquisición de software especializado	Desde la etapa de planeación del proceso
5	Contratista	Se acepta el riesgo y por ende se incluye	2	3	5	SI	Supervisor	El supervisor del contrato hace seguimiento a	Desde la etapa de planeación del proceso

No.	¿A quién se le asigna?	Tratamiento/ Controles a ser implementados	Impacto después del tratamiento			¿Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Monitoreo y revisión	
			Probabilidad	Impacto	Calificación Total			¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
		garantías dentro del proceso.						la ejecución y entrega del software especializado	
6	Contratista	Las cotizaciones que se solicitan para el estudio de mercado deben ser claras para permitir contar con valores acordes con el servicio que se va a contratar	2	4	6	SI	Área Solicitante	Se solicitan la mayor cantidad de cotizaciones para establecer los valores del mercado	Desde que la dependencia inicia el sondeo de mercado
7	ANLA	Analizar al detalle los bienes que se pretender contratar para construir los documentos previos con rigurosidad y claridad que requiere el proceso	2	4	6	SI	Área Solicitante	Servidor público de la ANLA competente de realizar la revisión	Desde que la dependencia solicitante de la contratación identifica la necesidad a satisfacer.

No obstante lo anterior, durante el termino de observaciones, los posibles oferentes o interesados en participar en el proceso deberán manifestar a la entidad, teniendo en cuenta el conocimiento que tienen como expertos en su actividad ordinaria, la existencia de posibles riesgos asociados a la ejecución del contrato que puedan afectar el equilibrio económico del mismo de conformidad con lo expresado por el artículo 863 del Código de Comercio, según el cual, las partes deberán proceder de buena fe exenta de culpa en el periodo precontractual, so pena de indemnizar los perjuicios que se causen.

En consecuencia, la entidad no aceptará reclamaciones relacionadas con circunstancias previsibles por el contratista que afecten dicho equilibrio económico y que no hayan sido manifestadas por el mismo.

9. ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS.

Para asegurar el cumplimiento de las obligaciones adquiridas en virtud del contrato, el Contratista deberá constituir garantía a favor del **FONDO NACIONAL AMBIENTAL /AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES - FONAM/ANLA**, identificado con **NIT 830.025.267-9** conforme lo establecido en los artículos 2.2.1.2.3.1.1 y siguientes del Decreto 1082 de 2015. Igualmente, debe tenerse en cuenta que los contratistas prestarán garantía única para el cumplimiento de las obligaciones surgidas del contrato de acuerdo con lo siguiente:

- **Cumplimiento del Contrato:** En cuantía equivalente al veinte por ciento (20%) del valor del mismo, con una vigencia igual al término de ejecución del contrato, y un (1) año más.
- **Calidad de los servicios:** Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato, con una vigencia igual al término de ejecución del mismo y un (1) año más.
- **Calidad y correcto funcionamiento de los bienes:** Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato, con una vigencia igual al término de ejecución del mismo y un (1) año más contado a partir del recibo a satisfacción de los bienes.

Notas aplicables a las Garantías:

1. El contratista deberá restablecer el valor de las garantías cuando este se haya visto reducido por razón de las reclamaciones efectuadas por la entidad contratante. De igual manera, en cualquier evento en que se aumente o adicione el valor del contrato o se prorrogue su término de ejecución, el contratista deberá ampliar el valor de la garantía otorgada o ampliar su vigencia, según el caso.

2. Si resultare como contratista, un **CONSORCIO O UNIÓN TEMPORAL**, la garantía debe ser otorgada por todos los integrantes.

10. INDICACIÓN DE SI LA CONTRATACIÓN ESTÁ COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE PARA EL ESTADO COLOMBIANO

De acuerdo a lo establecido en el artículo 2.2.1.1.2.1.1 numeral 8 del Decreto 1082 de 2015 y siguiendo los lineamientos fijados por el Ministerio de Comercio, Industria y Turismo y el Departamento Nacional de Planeación en el documento “Manual para el Manejo de Acuerdos Comerciales”, se logra concluir que el presente proceso está cobijado por varios

Acuerdos Internacionales o Tratados de Libre Comercio vigentes, de conformidad con las siguientes verificaciones:

ACUERDO COMERCIAL		Entidad Estatal Incluida	Presupuesto del Proceso de Contratación superior al valor del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
Alianza Pacifico	Chile	SI	SI	NO	SI
	Perú	SI	NO	NO	NO
	México	SI	SI	NO	SI
Canadá		SI	NO	NO	NO
Chile		SI	SI	NO	SI
Costa Rica		SI	NO	NO	NO
Estados AELC		SI	NO	NO	NO
Estados Unidos		SI	NO	NO	NO
Unión Europea		SI	NO	NO	NO
Israel		SI	NO	NO	NO
Corea		SI	NO	NO	NO
Estados Unidos Mexicanos		SI	SI	NO	SI
Triángulo Norte	El Salvador	SI	SI	NO	SI
	Guatemala	SI	SI	NO	SI
	Honduras	SI	SI	NO	SI
Comunidad Andina de Naciones		SI	SI	NO	SI
Reino Unido de Gran Bretaña e Irlanda		SI	NO	NO	NO

Al presente proceso le es aplicable el Acuerdo con la Comunidad Andina de Naciones, toda vez que la Decisión 439 de 1998 de la Comisión de la CAN es aplicable a todos los Procesos de Contratación de las Entidades Estatales del nivel nacional, independientemente del valor del Proceso de Contratación.

No está cubierto por los Acuerdos Comerciales con Canadá, toda vez que no se supera el umbral establecido, es decir, la suma de **$433.332.253.**

No está cubierto por los Acuerdos Comerciales entre Costa Rica y Colombia, toda vez que no se supera el umbral, es decir la suma de **$432.974.981**, estando el presupuesto oficial, correspondiente a la suma de **$361.040.000** por debajo del valor de dicho umbral.

No está cubierto por los Acuerdos Comerciales entre Estados Unidos y Colombia, toda vez que no se supera el umbral, es decir la suma de **$439.974.981**, estando el

presupuesto oficial, correspondiente a la suma de **$361.040.000** por debajo del valor de dicho umbral.

Si está cubierto por el Acuerdo Comercial con los Estados Unidos Mexicanos, toda vez que calculado el valor del umbral, establecido para la aplicación de este acuerdo es a partir de la suma **$ 341.973.443**, estando el presupuesto oficial, es decir la suma de **$361.040.000,** por encima del umbral.

No está cubierto por el Acuerdo Comercial con Corea, toda vez que el umbral establecido para este acuerdo está por la suma de **$382.000.000,** mientras que el presupuesto oficial para este proceso corresponde a suma de **$361.040.000.**

Si está cubierto por el Acuerdo Comercial con Chile, porque el presupuesto oficial para este proceso, que corresponde a la suma de **$361.040.000,** supera el umbral establecido en la suma de $**272.764.794**.

Si está cubierto por los Acuerdos de Libre Comercio del Triángulo Norte (Salvador, Guatemala y Honduras), toda vez que el presupuesto oficial del presente proceso, que corresponde a la suma de **$361.040.000,** supera el límite inferior de la menor cuantía de la Entidad, esto es, la suma de **$78.790.726.**

No está cobijado por el Acuerdo Comercial con la Unión Europea, toda vez que el presupuesto oficial del presente proceso, que corresponde a la suma de **$361.040.000**, está por debajo del umbral establecido en la suma de **$ 735.297.922.**

No está cobijado por el Acuerdo Comercial con AELC, toda vez que el presupuesto oficial del presente proceso, que corresponde a la suma de **$361.040.000,** está por debajo del umbral establecido para dicho acuerdo en la suma de **$735.297.922**.

No está cobijado por el Acuerdo Comercial con Reino Unido de Gran Bretaña e Irlanda, toda vez que el presupuesto oficial del presente proceso, que corresponde a la suma de **$361.040.000,** está por debajo del umbral para este acuerdo, establecido en la suma de **$ $709.188.464.**

Si está cubierto por Alianza del Pacífico - Chile, toda vez que el presupuesto oficial del presente proceso, que corresponde a la suma de **$361.040.000,** supera el umbral establecido para dicho acuerdo en la suma de **$272.951.066.**

No está cubierto por Alianza del Pacífico Perú, toda vez que el presupuesto oficial, establecido en la suma de **$361.040.000**, no supera el umbral para este acuerdo, es decir la suma de **$518.607.026**.

Si está cobijado por el Acuerdo Alianza del Pacífico México, toda vez que el presupuesto oficial del presente proceso, que corresponde a la suma de **$361.040.000,** supera el umbral establecido para este acuerdo en la suma de **$272.951.066**.

No está cubierto por el Acuerdo Comercial con Israel, toda vez que el presupuesto oficial que corresponde a la suma de **$361.040.000,** no supera el umbral establecido para este Acuerdo en la fecha de estos Estudios Previos, el cual corresponde a **$595.313.867,08**.



MAURICIO ALEJANDRO GARCIA CORREDOR
JEFE DE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Anexos: (Escriba aquí los anexos. Si no los hay borrar este renglón)

ElaborÃ³:
MAURICIO ALEJANDRO GARCIA CORREDOR (JEFE DE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN)

Revisó:

Aprobó (Escriba aquí quien aprueba. Si no lo hay borrar este renglón