ESTUDIOS Y DOCUMENTOS PREVIOS

LICITACIÓN PÚBLICA

PROCESO TC-LP-26-01

OBJETO CONTRACTUAL:

PRESTACIÓN DE SERVICIO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, MONITOREO DE INICIDENTES DE SEGURIDAD Y ATENCIÓN CORRECTIVA A INCIDENTES DE LA GOBERNACIÓN DE SANTANDER, EN EL MARCO DEL PROYECTO DE IMPLEMENTACIÓN DE ACCIONES PARA EL ASEGURAMIENTO TECNOLÓGICO Y LA TRANSFORMACIÓN DIGITAL EN EL DEPARTAMENTO DE SANTANDER

VALOR ESTIMADO DEL CONTRATO

SEIS MIL OCHOCIENTOS SESENTA Y SIETE MILLONES TRESCIENTOS CINCUENTA Y NUEVE MIL CIENTO SESENTA Y SEIS PESOS ($6.867.359.166,00) INCLUIDO ESTAMPILLAS, IVA Y GASTOS DE LEGALIZACIÓN (3922,17smmlv)

PLAZO DEL CONTRATO:

El plazo estipulado para su ejecución es de ONCE (11) MESES Y VEINTISÉIS (26) DÍAS contados a partir de la suscripción del acta de inicio.

OFICINA GESTORA

SECRETARÍA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES TIC-

BUCARAMANGA, NOVIEMBRE DE 2026

INFORME DE CONVENIENCIA Y OPORTUNIDAD ESTUDIOS Y DOCUMENTOS PREVIOS

De conformidad con los lineamientos previstos en los numerales 7 y 12 del artículo 25 de la Ley 80 de 1993, el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, Decreto 399 de 2021 y demás normas que modifiquen, reglamenten o sustituyan, se
procede a realizar el análisis de conveniencia y oportunidad para establecer la necesidad y oportunidad de realizar la presente contratación.

El numeral 12 del artículo 25 de la Ley 80 de 1993 el cual fue modificado por el artículo 87 de la ley 1474 de 2011 establece que con la debida antelación a la apertura del procedimiento de selección o de la firma del contrato, según el caso, deberán elaborarse los estudios, diseños y proyectos requeridos y los pliegos de condiciones. Así mismo el numeral 7 artículo 25 de la Ley 80 de 1993 señala que la conveniencia o inconveniencia del objeto a contratar y las autorizaciones y aprobaciones para ello, se analizarán o impartirán con antelación al inicio del proceso de selección del contratista o al de la firma del contrato, según el caso.

A su vez el Decreto 1082 de 2015 en su artículo 2.2.1.1.2.1.1 modificado por el Decreto 399 de 2021 señala que los estudios y documentos previos son el soporte para elaborar el proyecto de pliegos, los pliegos de condiciones, y el contrato, igualmente establece los elementos que debe contener los estudios y documentos previos.

1. INVITACIÓN A LAS VEEDURÍAS CIUDADANAS.

El DEPARTAMENTO DE SANTANDER, en cumplimiento de lo dispuesto en el inciso 3 del artículo 66 de la Ley 80 de 1993, invita a todas las personas y organizaciones interesadas en hacer control social al contrato objeto del presente proceso, en cualquiera de sus fases o etapas, a que presenten las recomendaciones que consideren convenientes, intervengan en las audiencias y a que consulten los documentos del proceso en el SECOP.

2. DOCUMENTOS QUE SOPORTAN LA CONTRATACIÓN A REALIZAR

El presente proceso de selección y contratación se fundamenta en los siguientes documentos:

a. El Decreto Departamental No. 041 del 30 de enero de 2025, por el cual se delega en los Secretarios de Despacho y Jefes de Oficina del nivel central del Departamento de Santander la competencia para ordenar el gasto y ejercer la facultad de seleccionar, adjudicar, celebrar, ejecutar, adicionar, prorrogar, reanudar, modificar, aclarar, suspender, terminar y liquidar convenios o contratos a nombre del Departamento, con personas públicas o privadas. Igualmente, se delega la expedición de actos administrativos que se produzcan con motivo u ocasión de la actividad contractual, en cumplimiento de las funciones y misión asignadas a cada Secretaría u Oficina, con cargo al presupuesto de inversión o funcionamiento, según corresponda.
b. Resolución 9865 de julio 12 de 2012 – responsabilidad en la elaboración de estudios y documentos previos, proyectos, programas y sus respectivos presupuestos oficiales.
c. Decreto 651 del 21 de noviembre de 2022, por la cual se adopta el manual de contratación del Departamento de Santander.
d. Decreto 462 del 17 de septiembre de 2021 – “Por medio del cual se modifica el manual de funciones y/o actividades que deben cumplir los Interventores y/o Supervisores, para realizar en forma debida sus funciones como supervisor”
e. La ordenanza No. 007 del 30 de mayo de 2024 por la cual se adopta el Plan Desarrollo Departamental 2024-2027: “Es tiempo de Santander” Eje estratégico: PROSPERIDAD. Programa: Facilitar el acceso y uso de las Tecnologías de la Información y las Comunicaciones en todo el territorio nacional. Indicador Producto: Número de Herramienta Tecnológica de Gobierno Digital Implementada.
f. Certificado de banco de programas y proyectos del departamento de Santander No. 336 de fecha 31 de agosto de 2026 con SSEPI 20250680000079 y BPIN 202500000028652
g. Plan Anual de Adquisiciones del Departamento.

3. PLAN ANUAL DE ADQUISICIONES.

De conformidad con lo establecido en el artículo 2.2.1.1.1.4.1 del Decreto 1082 de 2015 el Departamento de Santander elaboró el plan anual de adquisiciones el cual contiene los bienes, obras y servicios que se pretenden adquirir durante la presente vigencia; encontrándose incluido el

objeto a contratar Dicho plan anual de adquisiciones ha sido publicado en la página web del Departamento de Santander y en el SECOP.

4. AVISO DE CONVOCATORIA.

En el proceso de selección de contratista, objeto del presente estudio, se expedirá y publicará el Aviso de Convocatoria, de conformidad con lo establecido en el artículo 2.2.1.1.2.1.2 del Decreto 1082 de 2015, el cual debe contener la información establecida en dicha norma.

5. AVISO DE LICITACIÓN.

En cumplimiento con lo dispuesto en el numeral 3 del artículo 30 de la Ley 80 de 1993, modificado por el artículo 224 del Decreto 019 de 2012, el Departamento de Santander, dentro de los diez (10) a veinte (20) días calendario anteriores a la apertura de la licitación publicará hasta un máximo de tres (3) avisos con intervalos entre dos (2) y cinco (5) días calendario según lo exija la naturaleza objeto y cuantía del contrato, en su página web y en el sistema electrónico para la contratación pública – SECOP-.

Los avisos contendrán información sobre el objeto y características esenciales de la respectiva licitación.

6. DOCUMENTOS DE COMPROMISOS DE TRANSPARENCIA Y ANTICORRUPCIÓN.

El proponente deberá anexar con la propuesta, los FORMATOS de COMPROMISO DE TRANSPARENCIA y de ANTICORRUPCIÓN (Anexo al pliego de condiciones), debidamente diligenciados y firmados.

En caso de Proponente plural, estos documentos deben ser diligenciados y firmados por cada uno de sus integrantes.

Si se comprueba el incumplimiento del Proponente, sus empleados, representantes, asesores o de cualquier otra persona que en el Proceso de Contratación actúe en su nombre, es causal suficiente para la terminación anticipada del contrato, si el incumplimiento ocurre con posterioridad a la adjudicación del mismo, sin perjuicio de que tal incumplimiento tenga consecuencias adicionales.

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

El panorama global y nacional de la ciberseguridad demanda una atención prioritaria y proactiva por parte de las organizaciones. A nivel mundial, los sistemas de información y redes son blanco constante de ciberataques sofisticados, capaces de comprometer la seguridad de la información y la continuidad operativa. Esta realidad se refleja de manera acentuada en Colombia, donde el entorno de ciberseguridad es complejo y está marcado por una creciente frecuencia y sofisticación de los incidentes.

El CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital, señala el objetivo de establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Los ciberataques están ampliando su rango de acción a partir del uso de nuevas tecnologías. Por ejemplo, los ataques a nivel global a dispositivos IoT (Internet of Things, por sus siglas en inglés) se incrementaron en un 300 % en el primer semestre de 2019 y si se tiene en cuenta que actualmente existen casi 21 billones de dichos dispositivos en el mundo, el riesgo de ataques es alarmante. Ahora bien, para 2025 y años subsiguientes se espera que la cifra de dichos dispositivos se duplique (Foro Económico Mundial, 2020), es evidente el incremento en el riesgo que implican los ataques cibernéticos. La aparición de ataques cibernéticos basados en nuevas tecnologías también conlleva costos para cualquier empresa o entidad pública, ya que el principal factor que incide en el aumento de los costos de contención de ataques cibernéticos es la creciente complejidad y sofisticación de estos. Teniendo en cuenta que el estudio Top 10 Strategic Technology Trends for 2020 (Gartner, 2020), determina las principales tendencias tecnológicas que generarán disrupciones digitales

significativas en los próximos años, se observa que hay un extenso panorama en el cual la complejidad y sofisticación tanto de la tecnología, como de los mismos ataques cibernéticos que pueden derivarse a partir de estas, supera hasta las más altas expectativas. Ante estos cambios derivados de la tecnología, la respuesta yace en la capacidad de investigación e innovación en materia de seguridad digital de cada entidad.

Durante el año 2023, Colombia fue escenario de ciberataques masivos que afectaron a más de 20 entidades públicas y 78 privadas, evidenciando la vulnerabilidad del ecosistema digital nacional. Cifras del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) revelaron 54.121 denuncias por ataques cibernéticos en 2023, un incremento del 79% respecto a 2021[1]. Eventos críticos como el ataque al Grupo Keralty en noviembre de 2022 y a IFX Networks en septiembre de 2023, que comprometió a cerca de 760 entidades, subrayan la urgencia de fortalecer las capacidades de defensa cibernética. Más recientemente, en 2024[2], se reportaron más de 20.000 millones de ciberataques en el país, y una encuesta sobre Seguridad Digital en Colombia[3] evidenció que el 78% de los encuestados ha sido víctima de un delito digital, lo que revela una baja percepción de riesgo y falta de autoprotección. Este contexto nacional exige la adopción de una postura proactiva, enfocada en la gestión integral de riesgos, la inversión en infraestructura tecnológica segura y el fortalecimiento de las capacidades institucionales.

Los objetivos específicos del modelo de seguridad de la información establecidos por el Ministerio de las TIC son:

- Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de las entidades.
- Orientar a las entidades en la transición de IPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
- Orientar a las entidades en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones

En este marco, la Gobernación de Santander ha identificado una necesidad imperante de fortalecer sus capacidades de monitoreo y respuesta ante incidentes de seguridad de la información para proteger integralmente sus activos críticos y garantizar la continuidad operativa de sus servicios tecnológicos. Aunque se han implementado algunos controles y políticas básicas de seguridad, la entidad carece de un sistema centralizado que permita una gestión proactiva y eficiente de los riesgos digitales. Actualmente, la mayoría de las actividades de seguridad se realizan de manera descentralizada, dificultando la detección temprana de amenazas y la respuesta coordinada a eventos e incidentes.

Un diagnóstico reciente, realizado durante el año 2024 y principios de 2025, evaluó el cumplimiento de 93 controles de la norma ISO 27001:2022 bajo el modelo MSPI. Esta evaluación reveló que, si bien la Gobernación de Santander ha avanzado en la implementación de controles de seguridad de la información, persisten importantes debilidades, principalmente en los controles Tecnológicos, Organizacionales y Físicos. Se identificaron deficiencias críticas en aspectos como el monitoreo proactivo de eventos y amenazas, la gestión efectiva de incidentes de seguridad y recopilación de evidencias, la protección de datos sensibles e infraestructura crítica, la resiliencia y continuidad operativa frente a ciberataques, y la capacidad limitada para coordinar respuestas entre áreas internas y proveedores TIC.

---

[1] Fuente https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-colombia-desafios-y-perspectivas/#_ftn1

[2] https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/396032:La-ciberseguridad-es-el-camino-para-crecer-y-fortalecer-los-entornos-digitales-del-pais-Ministro-Lizcano

[3] https://urosario.edu.co/periodico-nova-et-vetera/nuestra-u/seguridad-digital-en-colombia-reflexiones-y-desafios-para-proteger-el-futuro-digital.

Se tiene que, la infraestructura y sistema de ciberseguridad de la Gobernación presenta múltiples desafíos debido, por un lado, a la obsolescencia de algunos de sus componentes, incluyendo sistemas operativos desactualizados, servidores antiguos y equipos de red con limitaciones tecnológicas, así como a un sistema, protocolo y servicio moderno, eficaz y eficiente de monitoreo en tiempo real. Esta situación no solo genera riesgos de seguridad, rendimiento y compatibilidad, sino que también impacta negativamente la eficiencia operativa y la capacidad de adaptación a las tendencias modernas de TI. Un aspecto crítico es la falta de compatibilidad de ciertos programas con el protocolo IPv6, un problema a largo plazo que compromete la escalabilidad y seguridad de las redes.

Estas limitaciones comprometen significativamente la capacidad de la Gobernación para responder de manera oportuna y efectiva ante amenazas emergentes, y dificultan el cumplimiento de las mejores prácticas internacionales en ciberseguridad. Asimismo, la ausencia de un área de seguridad de la información consolidada restringe la gestión adecuada de las actividades necesarias para lograr un nivel aceptable de madurez en el sistema de gestión de seguridad de la información.

Como se ha indicado, la necesidad si bien contempla distintas actividades a desarrollar, se genera a partir del requerimiento institucional de una estrategia integral de monitoreo en ciberseguridad, orientada a proteger los activos digitales de la entidad. Esta estrategia debería comprender la adopción de una infraestructura, prácticas, procesos y tecnologías que permitan garantizar la protección, detección, respuesta oportuna y recuperación ante posibles ataques en el ciberespacio, con una planificación estratégica que contemple la capacitación del personal, procesos claros para la gestión de incidentes de seguridad, análisis de riesgos específico para identificar las amenazas más relevantes, así como definir los objetivos en términos de protección de datos, respuesta ante incidentes y monitoreo continuo de redes y sistemas de información. La adopción de normativas de ciberseguridad garantizará un enfoque integral y efectivo, además, es esencial fomentar la cultura de seguridad a través de programas de concienciación y capacitación regular sobre prácticas seguras en el entorno digital.

En este contexto, y con el fin de asegurar una gestión eficaz y continua del área de seguridad de la información, se identifica la necesidad de prestar servicios que desarrollen actividades asociadas al monitoreo, análisis y respuesta frente a incidentes de seguridad informática. Para ello, se contempla la integración de tecnologías avanzadas como inteligencia artificial y análisis de datos, que permitirán una mejor detección de anomalías y la automatización de respuestas ante incidentes.

La implementación exitosa de esta estrategia no solo protegerá la información sensible de la entidad, sino que también contribuirá a la confianza pública en la gestión gubernamental y el desarrollo sostenible de la región.

El alcance del servicio parte de la necesidad de proteger de manera integral los activos de información de la entidad frente a un entorno digital cada vez más complejo, interconectado y vulnerable a múltiples vectores de ataque. No se trata únicamente de implementar controles técnicos, sino de establecer un marco de gestión sólido, sostenible y alineado con estándares internacionales, que permita anticiparse, detectar, responder y recuperarse ante incidentes de seguridad.

En este sentido, el alcance propuesto trasciende las acciones reactivas y se orienta hacia la construcción de una capacidad institucional permanente en materia de seguridad digital. Por ello, contempla de manera articulada los siguientes componentes esenciales:

- En primer lugar, se aborda la gestión del Sistema de Seguridad de la Información (SGSI) como eje estructural del servicio. Esto implica no solo su implementación o actualización técnica, sino su integración transversal a los procesos institucionales mediante la definición del alcance, las políticas, la declaración de aplicabilidad, el tratamiento de riesgos y la planificación de auditorías internas. La madurez de un SGSI no se limita a la documentación: requiere revisión constante, auditorias, seguimiento y mejora continua.

- En segundo lugar, se incorpora la gestión proactiva de incidentes y la vigilancia activa sobre la infraestructura tecnológica mediante la implementación de herramientas de ciberseguridad que permiten el monitoreo, análisis, correlación de alertas en tiempo real, que en conjunto a la realización periódica de pruebas técnicas que permitan identificar vulnerabilidades y amenazas antes de que sean explotadas. La ejecución mensual de pruebas de vulnerabilidades, análisis de código (SAST y DAST), pruebas de ingeniería social y ejercicios de ethical hacking, permite

no solo evaluar el nivel de exposición institucional, sino atender de forma inmediata los riesgos detectados, incluyendo aquellos de tipo día cero.

Asimismo, se reconoce la importancia de gestionar el riesgo cibernético como una dimensión diferenciada dentro del riesgo organizacional, integrando metodologías basadas en la norma ISO 27000 o NIST (cybersecurity framework), que faciliten una comprensión real de los activos críticos, amenazas emergentes y escenarios de impacto. Esto no solo permite tomar decisiones informadas, sino diseñar estrategias de mitigación eficaces y priorizadas según el nivel de criticidad.

Otro aspecto fundamental del alcance es el componente humano, frecuentemente el eslabón más débil en la cadena de seguridad. Por ello, se requiere la implementación de un plan sistemático de concientización y formación. A través de talleres, simulaciones y campañas, se busca generar una cultura organizacional orientada a la prevención, la corresponsabilidad y la actuación segura frente a posibles amenazas.

Con el fin de lograr una de ejecución efectiva, el servicio requiere contar con personal profesional especializado, con el fin de lograr la continuidad operativa, trazabilidad de las acciones, articulación con las áreas técnicas de la entidad, y liderazgo constante en la implementación de controles y tratamiento de incidentes. De igual forma, el personal vinculado al servicio de monitoreo deberá tener los más altos estándares nacionales e internacionales de acreditación de capacidades profesionales, técnicas y de formación en normas y/o certificados de acreditación que los ubican en los más altos niveles de capacidades frente a la seguridad cibernética. Lo anterior, resulta consecuente bajo el entendido real de la generación de incidentes o ciberataques, los cuales son desarrollados en su mayoría a un nivel externo y luego replicados a nivel local. Hecho que amerita que el personal se encuentre a la vanguardia de las más recientes actualizaciones en la materia.

En conclusión, el alcance del servicio se define bajo una visión integral, que entiende la seguridad de la información no como un producto o un software, sino como un proceso institucional estratégico, dinámico y continuo. Su cobertura incluye todos los sistemas, procesos, actores y activos digitales de la organización, con el firme propósito de fortalecer la resiliencia institucional y garantizar la confianza digital de cara a la ciudadanía y los entes de control.

A su vez, es conveniente mencionar, que la presente necesidad, se encuentra ligada y enmarcada en un proyecto de mayor envergadura. El Departamento de Santander adelantó los procesos contractuales que tenían por objetivo adquirir y adecuar las capacidades cibernéticas para la concreción de un modelo integral de defensa a esta escala. Por ello adquirió los equipos de data center, puestos de monitoreo y un sistema de climatización que garantice la funcionalidad de estos. Esta adquisición está llamada a servir como insumo para la implementación material del sistema de ciberseguridad, dado que los equipos e instalaciones con las que se contaba, limitaban la modernización e integralidad del sistema.

La población objetivo del presente proyecto, son 2.340.657 personas beneficiadas. El objetivo Fortalecer la infraestructura tecnológica que permita desarrollar estrategias integrales (incluyendo políticas, protocolos y procedimientos) alineadas con estándares nacionales e internacionales.

El Departamento de Santander cuenta con un proyecto denominado “IMPLEMENTACIÓN DE ACCIONES PARA EL ASEGURAMIENTO TECNOLÓGICO Y LA TRANSFORMACIÓN DIGITAL EN EL DEPARTAMENTO DE SANTANDER.” Con certificado del banco de proyectos del Departamento de Santander No. No. 336 de fecha 31 de agosto de 2026 con SSEPI 20250680000079 y BPIN 202500000028652.

Por lo expuesto, se encuentra necesario, conveniente y oportuno iniciar el proceso de contratación bajo la modalidad correspondiente, con el fin de dar cumplimiento con lo propuesto Plan Desarrollo Departamental 2024- 2027: “Es tiempo de Santander” Eje estratégico: PROSPERIDAD. Programa: Fomento del desarrollo de aplicaciones, software y contenidos para impulsar la apropiación de las Tecnologías de la Información y las Comunicaciones (TIC).

Así, gracias a la evaluación realizada por el Departamento de Santander, identificados los riesgos asociados a la plataforma de tecnología (TI), a los procesos de gestión de Tecnologías y Sistemas de Información del Departamento de Santander (Gobernación de Santander) y a los recursos requeridos, se requiere la implementación de controles para minimizar y mitigar los riesgos inherentes identificados, lo que conduce a que se lleve el riesgo a niveles aceptables o asumibles por la entidad.

De lo anterior se definen claramente los objetivos específicos a satisfacer:

1. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
2. Incluir en la estrategia todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.
3. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de seguridad que se presenten.
4. Gestionar las vulnerabilidades de aquellas infraestructuras criticas o plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
5. Realizar un monitoreo continuo a la plataforma tecnológica e infraestructura critica con el propósito de identificar y predecir comportamientos inusuales que puedan evidenciar ataques contra la entidad.
6. Implementar tecnologías que permitan a la Entidad identificar el origen de los ataques, tipos de ataques, comportamientos y la detección predictiva de amenazas.
7. Integrar infraestructura moderna y adaptada para que los equipos y sistemas se complementen en integren en virtud de la prestación de un servicio en optimas condiciones de funcionalidad y calidad.

Objetivos que se resumen en la finalidad del servicio, el cual corresponde a adoptar medidas técnicas, humanas y administrativas para garantizar la gobernanza de la seguridad digital, la gestión de riesgos de seguridad digital, la identificación y reporte de infraestructuras críticas cibernéticas y servicios esenciales, y la gestión y respuesta a incidentes de seguridad digital

8. OBJETO A CONTRATAR, CON SUS ESPECIFICACIONES, LAS AUTORIZACIONES, PERMISOS Y LICENCIAS REQUERIDOS PARA SU EJECUCIÓN.

La ENTIDAD contratará de conformidad con la ley 80 de 1993, la ley 1150 de 2007 y el Decreto 1082 de 2015, el siguiente objeto contractual:

8.1. OBJETO A CONTRATAR.

PRESTACIÓN DE SERVICIO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, MONITOREO DE INCIDENTES DE SEGURIDAD Y ATENCIÓN CORRECTIVA A INCIDENTES DE LA GOBERNACIÓN DE SANTANDER, EN EL MARCO DEL PROYECTO DE IMPLEMENTACIÓN DE ACCIONES PARA EL ASEGURAMIENTO TECNOLÓGICO Y LA TRANSFORMACIÓN DIGITAL EN EL DEPARTAMENTO DE SANTANDER.

8.2. ALCANCE DEL OBJETO Y ESPECIFICACIONES TECNICAS:

El proponente adjudicatario deberá prestar el servicio de gestión de monitoreo de acuerdo con lo establecido en el documento de estudios previos, pliego de condiciones y el contrato, atendiendo a las indicaciones dadas por el supervisor del contrato así:

ítems	Actividad	Alcance
1	Apoyo en el seguimiento a auditorías internas (bimestrales) y externas. Evidenciar cumplimiento, preparar hallazgos y atender requerimientos de entes de control.	Cobertura del SGSI de la Gobernación de Santander.
2	Apoyo en la evaluación, mitigación y monitoreo de riesgos de seguridad. Incluye gestión continua de indicadores y actualización conforme a nuevas amenazas y tecnologías.	Evaluación de riesgos a nivel de sistemas, usuarios y activos de información.
3	Apoyo en el desarrollo e implementación de políticas institucionales basados en ISO 27001:2022 (contraseñas, proveedores, uso aceptable, privacidad, aseguramiento, mantenimiento, desarrollo de software seguro, gestión de cambios, DRP y POA anual).	Cobertura del SGSI de la Gobernación de Santander.
4	Apoyo en la documentación de procedimientos como respaldo, continuidad, seguimiento a incidentes, control de cumplimiento y mitigación de vulnerabilidades.	Aplicación a todos los sistemas informáticos de la Gobernación de Santander.

5	Asistencia técnica en la elaboración y ejecución del Plan de sensibilización y capacitación del personal de las secretarías sobre el SGSI y pruebas de Phishing	Diseño y ejecución de campañas de sensibilización (Una mensual), Capacitación en Seguridad de la Información (Una (1) por semestre), y una (1) prueba de ingeniería social semestral (phishing) para 1000 buzones de correo.
6	Realizar pruebas de vulnerabilidades de la infraestructura tecnológica en la Gobernación de Santander.	Realizar un análisis de vulnerabilidades cuatrimestral a 80 servidores y 800 computadores de la Gobernación de Santander.
7	Aplicar pruebas de seguridad (SAST y DAST) antes del despliegue de software.	Realizar un set de 5 revisiones de código fuente estático (SAST) y 5 revisiones de análisis de aplicaciones DAST
8	Ejecutar pruebas de Ethical Hacking semestrales	Realizar 1 prueba de Ethical Hacking semestral a 30 (Servidores físicos, Servidores virtuales, UTM y aplicaciones)
9	Implementar soluciones de seguridad Threat Hunting (EDR, herramientas de protección de amenazas de red)	Protección de amenazas persistentes avanzadas , que permita la interrupción de ataques en curso para 40 Servidores y 800 computadores durante la ejecución del contrato
10	Implementar herramientas avanzadas de detección, análisis y respuesta en tiempo real para identificar y mitigar amenazas persistentes y avanzadas	Servicios de inteligencia de amenazas en red con IA para la defensa de amenazas persistentes para la interrupción de ataques en curso de hasta 840 dispositivos y/o IP
11	Puesta en marcha de herramientas para detección y respuesta automática de ataques a través de correo electrónico	300 buzones de correo a proteger
12	Implementación de SIEM de nueva generación con monitoreo 24/7, capacidades SOAR y UEBA, y operación desde centro de monitoreo con CSIRT.	Capacidad de 3000 EPS y (1) un año de retención de logs
13	Implementar herramientas de monitoreo de red para detectar anomalías y prever fallos de infraestructura.	Servicio de monitoreo e infraestructura y disponibilidad NOC 7*24 para 100 dispositivos
14	Implementación de herramientas de seguridad de portales web	Protección WAF, DDoS, CDN, Bots y 300 Gigabytes mensuales para tres (3) sitios web públicos de la gobernación de Santander.
15	Implementar monitoreo de marca con tecnología de vigilancia digital y detección en Deep/Dark Web	Aplica para dos dominios institucionales y redes sociales de la gobernación de Santander

Nota 1. En documento anexo denominado ANEXO TÉCNICO se detallan las actividades, alcance y obligaciones sobre el cumplimiento de los ítems descritos anteriormente para la implementación del servicio especializado en el Centro de Operaciones de Seguridad (SOC – Security Operations Center) y de Control de Red (NOC - Network Operations Center) del Departamento para el monitoreo de las redes y los servicios tecnológicos que hacen parte de la infraestructura.

Nota 2. La implementación del servicio de monitoreo se debe prestar con altos estándares de control a partir de matrices y estándares internacionales que garanticen no solo la estabilidad de los sistemas sino encontrarse a la vanguardia internacional. Los ciber ataques adicional a su constancia son cada vez más modernos y adaptados a los distintos niveles de seguridad que las entidades e instituciones aplican, por lo que es menester establecer criterios avanzados, actualizados y novedosos para afrontar estos ataques.

Nota 3. La solución tecnológica propuesta para la prestación del servicio deberá cumplir con los siguientes criterios de liderazgo según el Cuadrante Mágico de Gartner y otros criterios de calidad:

- Plataforma SIEM: La herramienta de correlación y análisis utilizada debe estar relacionada y mencionada en el Cuadrante Mágico de Gartner para plataformas SIEM.
- EDR (Endpoint Detection and Response): La solución de seguridad para Threat Hunting y protección de endpoints debe estar clasificada como líder en el Cuadrante Mágico de Gartner para plataformas de seguridad en endpoints.
- NDR (Network Detection and Response): La solución de inteligencia de amenazas en red, basada en inteligencia artificial para la detección y defensa frente a amenazas, debe figurar como líder en el Cuadrante Mágico de Gartner para plataformas NDR (Network Detection and Response).
- Criterios de un marco de gestión basado en el Sistema de Gestión de Seguridad de la Información (SGSI) acreditado por entidad correspondiente a nivel nacional, acreditación que permite proteger de manera efectiva la confidencialidad, integridad y disponibilidad de la información.

Nota 4. El servicio se encuentra estructurado en servicio global a todo costo con una forma de pago mensual durante la prestación efectiva del servicio y un primer pago que asegura la adquisición de las tecnologías necesarias para la prestación del servicio, los cuales se integran al mismo y son propiedad del contratante. Este valor incluye, infraestructura, configuraciones, personal, capacitaciones, apoyos estratégicos en auditorias, generación de reportes, implementación de herramientas, ejecución de pruebas, apoyo en la generación documental de planes y programas de gestión en seguridad.

Nota 5. El proponente dispondrá del personal profesional requerido en sitio, en las estaciones de monitoreo dispuestas por el Departamento de Santander, ubicadas en la ciudad de Bucaramanga.

Nota 6. La entidad requerirá para le ejecución del servicio contratado que los perfiles cumplan con la exigencia de criterios de altas capacidades técnicas y propias del personal que se ha considerado idóneo. Los mismos, obedecen a un análisis técnico de cada uno de los ítems de la ficha técnica en los que se engloba el servicio, la puesta en marcha del servicio y a la complejidad que pesa sobre la necesidad a satisfacer, dado que corresponde un sistema que busca garantizar la protección de los sistemas de información bajo estándares internacionales, por lo anterior se han considerado tales perfiles como mínimos requeridos para una correcta implementación de las herramientas, procesos o servicios necesarios.

8.3 CLASIFICACIÓN UNSPSC

Los servicios objeto del presente Proceso de Contratación está codificada en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC), como se indica en el siguiente cuadro:

CLASIFICACION	DESCRIPCION
80101500	Servicios de consultoría de negocios y administración corporativa
80101600	Gerencia de Proyectos
80111500	Desarrollo de recursos humanos
80111700	Servicios de contratación
81111500	Ingeniería de software o hardware
81111700	Sistema de manejo de información MIS
81111800	Servicios de sistemas y administración de componentes de sistemas
81111900	Sistema de recuperación de información
81112000	Servicios de datos
81112200	Mantenimiento y soporte de software
81112300	Mantenimiento de soporte de hardware de computador
81161700	Servicios de telecomunicaciones
81161800	Servicios de alquiler o arrendamiento de equipos o plataformas de voz y datos o multimedia
72151200	Servicios de instalación y mantenimiento de sistemas de climatización

72151500	Servicios de instalación y mantenimiento de sistemas eléctricos
26121600	Cables de telecomunicaciones
32101500	Circuitos integrados
32151900	Componentes de circuitos integrados
43201600	Componentes de computadores
43201800	Dispositivos de almacenamiento
43201900	Dispositivos de red
43211500	Computadores
43221700	Equipo de comunicaciones
43221800	Equipo de comunicaciones de datos
43222500	Equipos de seguridad de red
43222600	Equipo de servicio de red
43223100	Componentes y accesorios de redes
43232200	Software de gestión de contenidos
43232700	Software de aplicaciones de red
43233200	Software de seguridad y protección
43233400	Software de controladores de dispositivos y utilidades
43233700	Software de administración de sistemas
82121500	Impresión

8.4 AUTORIZACIONES

Quien va a suscribir el contrato objeto del presente estudio, por parte de la Entidad territorial, cuenta con las siguientes normas que lo autorizan para el efecto:

1. El Decreto Departamental No. 041 del 30 de enero de 2025, por el cual se delega en los Secretarios de Despacho y Jefes de Oficina del nivel central del Departamento de Santander la competencia para ordenar el gasto y ejercer la facultad de seleccionar, adjudicar, celebrar, ejecutar, adicionar, prorrogar, reanudar, modificar, aclarar, suspender, terminar y liquidar convenios o contratos a nombre del Departamento, con personas públicas o privadas. Igualmente, se delega la expedición de actos administrativos que se produzcan con motivo u ocasión de la actividad contractual, en cumplimiento de las funciones y misión asignadas a cada Secretaría u Oficina, con cargo al presupuesto de inversión o funcionamiento, según corresponda.

2. Decreto 651 del 21 de noviembre de 2022, por la cual se adopta el manual de contratación del Departamento de Santander.

3. Decreto 462 del 17 de septiembre de 2021 – “Por medio del cual se modifica el manual de funciones y/o actividades que deben cumplir los Interventores y/o Supervisores, para realizar en forma debida sus funciones como supervisor”

9 MODALIDAD DE SELECCIÓN DEL CONTRATISTA, JUSTIFICACIÓN Y FUNDAMENTOS JURÍDICOS.

9.1 MODALIDAD DE SELECCIÓN.

La escogencia de contratista se efectuará con arreglo a la modalidad de LICITACIÓN PÚBLICA.

9.2 JUSTIFICACIÓN.

De conformidad con el articulo 2 numeral 1 de la ley 1150 de 2007, la entidad contratara mediante la modalidad de selección por licitación Pública, esto por cuanto el valor estimado del contrato, objeto del proceso de selección a realizar, supera el valor máximo de la menor cuantía de la Entidad, correspondiendo este último a **Mil setecientos cincuenta millones novecientos cinco mil un peso mcte ($ 1.705.905.001)** y atendiendo a su mismo al objeto del contrato.

9.3 FUNDAMENTOS JURÍDICOS.

La norma que soporta la modalidad del proceso selección de contratista que nos ocupa, es el artículo 2 de la Ley 1150 de 2007, que a la letra dice:" *De las modalidades de selección. La escogencia del contratista se efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos y contratación directa, con base en las siguientes reglas:*

Licitación pública. La escogencia del contratista se efectuará por regla general a través de licitación pública, con las excepciones que se señalan en los numerales 2, 3 y 4 del presente artículo.

Cuando la Entidad estatal así lo determine, la oferta en un proceso de la licitación pública podrá ser presentada total o parcialmente de manera dinámica mediante subasta inversa, en las condiciones que fije el reglamento."

Igualmente, en cumplimiento a lo establecido en el artículo 2.2.1.1.2.2.2 del Decreto 1082 de 2015, la Entidad debe determinar la oferta más favorable para el caso de licitación teniendo en cuenta:

"a) La ponderación de los elementos de calidad y precio soportados en puntajes o fórmulas; o
b) La ponderación de los elementos de calidad y precio que representen la mejor relación de costo-beneficio."3

Así mismo, es del caso señalar que las normas que se aplican para el proceso de contratación a realizar son:

a. Ley 80 de 1993. (Estatuto General de Contratación de la Administración Pública)
b. Ley 1150 de 2007. (Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.)
c. Ley 1474 de 2011. (Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública).
d. Ley 361 de 1997. (Por la cual se establecen mecanismos de integración social de las personas con limitación y se dictan otras disposiciones).
e. Ley 590 de 2000. (Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresas).
f. Ley 816 de 2003. (Por medio de la cual se apoya a la industria nacional a través de la contratación pública).
g. Decreto 2680 de 2009. (Por el cual se definen los criterios para el Registro de Productores de Bienes
h. Nacionales).
i. Decreto ley 4170 de 2011. (Por el cual se reglamenta el sistema de compras y contratación pública).
j. Decreto ley 019 de 2012. (Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública).
k. Decreto 1082 de 2015. (Por medio del cual se expide el decreto único reglamentario del sector administrativo de planeación nacional).
l. Decreto 399 de 2021
m. Decreto 1860 de 2021

Por su parte, el proyecto a nivel técnico se enmarca en la siguiente normatividad vigente y aplicable, de la cual se desprenden ciertos criterios de calidad:

a. Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada..."
b. Decreto 1747 de 2000, que reglamenta parcialmente la ley 527 de 1999, con lo relacionado a las entidades de certificación, los certificados y las firmas digitales.
c. Ley Estatutaria 1266 de 2008: que establece las disposiciones generales del habeas data y regula el manejo de la información que se contiene en las bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

d. Ley 599 de 2000 Código Penal de Colombia: Esta ley contempla artículos relacionados con delitos informáticos en Colombia, como acceso abusivo a un sistema informático, daño informático y otros.
e. Ley 1273 de 2009: Esta ley, promulgada por el Congreso de la República de Colombia, establece disposiciones específicas relacionadas con la protección de la información y los datos. Tipifica una serie de conductas delictivas relacionadas con el manejo de datos personales.
f. Ley 527 de 1999, Comercio Electrónico: Esta ley regula el comercio electrónico en Colombia.
g. Ley 906 de 2004, Código de Procedimiento Penal de Colombia: Contiene artículos relacionados con delitos informáticos y procedimientos legales asociados.
h. Ley 1480 de 2011 - Estatuto del Consumidor: Esta ley regula los derechos de los consumidores en Colombia y también tiene implicaciones en la seguridad de la información. Las organizaciones deben proteger la información del consumidor y garantizar la confidencialidad de sus datos.
i. Resolución 306 de 2019: Esta resolución del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece directrices sobre la gestión de la seguridad de la información en las entidades públicas de Colombia. Contiene pautas para la implementación de un SGSI en el sector público.
j. Resolución 061 de 2019: Esta resolución establece el régimen de protección de datos personales para entidades del sector público colombiano y establece directrices para el cumplimiento de la Ley 1581 de 2012 en estas entidades.
k. Otras normativas sectoriales: Dependiendo de la industria o sector al que pertenezca una organización, puede estar sujeta a regulaciones específicas relacionadas con la seguridad de la información.
    - ISO/IEC 17799:2005: Esta norma internacional establece pautas para la gestión de la seguridad de la información en las organizaciones. Proporciona un marco integral que requiere el respaldo sólido de la alta dirección para su implementación. Publicada por la International Organization for Standardization (ISO) en 2000, esta norma ofrece recomendaciones para la gestión de la seguridad de la información dirigidas a quienes son responsables de iniciar, implementar o mantener la seguridad de una organización.
    - COBIT (Control Objectives for Information and related Technology): Desarrollado por la Information Systems Audit and Control Foundation (ISACA), COBIT se enfoca en la gobernanza, control, aseguramiento y auditorías de Tecnologías de la Información (TI). Ha ganado importancia en los últimos años debido a su aplicación específica en el ámbito de las TI.
    - ISO Serie 27000: Esta serie de estándares ISO incluye definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), guía de implementación de SGSI (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoría y certificación de SGSI (ISO 27006), guía de auditoría de SGSI (ISO 27007), y otros estándares relacionados con la seguridad de la información en diversos contextos.
    - Norma Técnica Colombiana NTC ISO/IEC 27003: Esta norma proporciona directrices específicas para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001. Ofrece pautas detalladas sobre cómo establecer, operar y mejorar un SGSI.
    - Norma Técnica Colombiana NTC ISO/IEC 27004: Esta norma establece métricas y técnicas de medición aplicables para evaluar la eficiencia y efectividad de la implementación de un SGSI y de los controles relacionados. Ayuda a las organizaciones a medir el rendimiento de su SGSI.
    - Norma Técnica Colombiana NTC ISO/IEC 27005: Esta norma proporciona una guía para la gestión del riesgo de seguridad de la información. Es relevante para la identificación, evaluación y tratamiento de riesgos de seguridad de la información.
    - Norma Técnica Colombiana NTC ISO/IEC 27006: Esta norma específica el proceso de acreditación de entidades de certificación y el registro de Sistemas de Gestión de Seguridad de la Información (SGSI). Es importante para las organizaciones que buscan certificar su SGSI.
    - Norma Técnica Colombiana NTC ISO/IEC 27011: Esta norma ofrece directrices específicas para la gestión de seguridad de la información en el sector de las telecomunicaciones. Ayuda a las organizaciones de telecomunicaciones a fortalecer la seguridad de la información en sus operaciones.
    - Norma Técnica Colombiana NTC ISO/IEC 27032: Esta norma proporciona directrices sobre ciberseguridad, incluyendo la protección de la información en un entorno

cibernético. Es relevante para enfrentar las amenazas cibernéticas y proteger la información en línea.

- Norma Técnica Colombiana NTC ISO/IEC 27033: Esta norma se enfoca en la seguridad en redes y proporciona directrices sobre cómo garantizar la seguridad de las redes de comunicación. Ayuda a proteger la información transmitida a través de redes.
- Norma Técnica Colombiana NTC ISO/IEC 27034: Esta norma se centra en la seguridad de las aplicaciones y proporciona pautas para desarrollar aplicaciones seguras y proteger la información que manejan.
- CONPES 3975 – 08 de noviembre de 2019 - Política Nacional Para La Transformación Digital e Inteligencia Artificial. Por medio del cual impulsar la transformación digital y la inteligencia artificial en Colombia, fomentando la innovación y la competitividad.
- CONPES 3995 – 01 de julio de 2020. Política Nacional de Confianza y Seguridad Digital: Por medio del cual se busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.

I. Decreto 620 de 2020. Por el cual se establecen lineamientos generales para los Servicios Ciudadanos Digitales (SCD) en Colombia. Este decreto subroga un título del Decreto 1078 de 2015 y reglamenta parcialmente varios artículos de leyes relacionadas con tecnologías de la información y comunicaciones, así como con la gestión documental y la interacción con el ciudadano en la administración pública.

10 IDENTIFICACIÓN DEL CONTRATO A CELEBRAR

El contrato a celebrar: se identifica como un contrato de PRESTACIÓN DE SERVICIOS.

10.1 PLAZO DEL CONTRATO:

El plazo estipulado por la entidad para la ejecución del contrato es de **ONCE (11) MESES Y VEINTISÉIS (26) DÍAS** contados a partir de la suscripción del acta de inicio.

10.2 LUGAR DE EJECUCIÓN:

El objeto del contrato, se ejecutará en el Departamento de Santander y/o en el lugar que disponga el supervisor del contrato.

11 VALOR ESTIMADO DEL CONTRATO Y LA JUSTIFICACIÓN DEL MISMO

11.1. VALOR ESTIMADO DEL CONTRATO

Se estima para efectos fiscales la suma de **SEIS MIL OCHOCIENTOS SESENTA Y SIETE MILLONES TRESCIENTOS CINCUENTA Y NUEVE MIL CIENTO SESENTA Y SEIS PESOS ($6.867.359.166,00) INCLUIDO ESTAMPILLAS, IVA Y GASTOS DE LEGALIZACIÓN (3922,17smmlv)**

11.2 JUSTIFICACIÓN DEL VALOR ESTIMADO DEL CONTRATO - ESTUDIO DE MERCADO

El valor estimado del presente proceso fue determinado por la Entidad considerando un estudio de mercado para los servicios necesarios a contratar dentro de la guía ejecutiva del presente proyecto y los estudios del sector. Tales estimaciones, así como los resultados de las cotizaciones recepcionadas mediante SECOP se compilan en estudio del sector adjunto.

PRESUPUESTO ESTIMADO DEL CONTRATO: El presupuesto es de **SEIS MIL OCHOCIENTOS SESENTA Y SIETE MILLONES TRESCIENTOS CINCUENTA Y NUEVE MIL CIENTO SESENTA Y SEIS PESOS ($6.867.359.166,00) INCLUIDO ESTAMPILLAS, IVA Y GASTOS DE LEGALIZACIÓN**. El Departamento de Santander sólo pagará los precios del contrato y, por tanto, no reconocerá suma alguna por concepto de impuestos u otros gravámenes. En materia de impuestos no se aceptarán salvedades de ninguna naturaleza. El Departamento efectuará a las cuentas del contratista las retenciones que, en materia de impuestos, tenga establecida la ley, las devoluciones o exenciones a que crea tener derecho el contratista, deberán ser tramitadas por éste a su costo ante la respectiva Administración de Impuestos, sin responsabilidad alguna por parte del Departamento.

La consulta de los precios de mercado esta soportada en el respectivo proyecto viabilizado por la Oficina Gestora, en el cual consta la forma en que se calcularon y su soporte; proyecto que se encuentra registrado en el Banco de Programas y Proyectos de Inversión Departamental según Certificado No. 336 de fecha 31 de agosto de 2026 con SSEPI 20250680000079 y BPIN 202500000028652.

11.3. DISPONIBILIDAD PRESUPUESTAL Y PROYECTO

El departamento a través de la oficina gestora se encuentra tramitando el certificado de disponibilidad presupuestal, una vez se cumplan los presupuestos administrativos y de procedimiento necesarios para la aprobación de vigencias futuras. No obstante, la entidad se acoge a lo definido en el Artículo 71 del Decreto 111 de 1996, Artículo 25, numeral 6, de la Ley 80 de 1993 y Artículo 2.2.1.1.2.1.5, numeral 6, del Decreto 1082 de 2015, así como el concepto 2389 de 2018 del Consejo de Estado.

12. FORMA DE PAGO

El Departamento de Santander determina como forma de pago del presente contrato, la siguiente:

Una vez firmado el contrato, legalizado y suscrita el acta de inicio, el Departamento de Santander realizara un primer pago mediante la suscripción de acta parcial del 15,7% del valor total del contrato cuando el contratista demuestre que cuenta con la infraestructura tecnológica para la ejecución del contrato, esto se demostrará con la presentación soporte de facturación y/o certificación del distribuidor autorizado de esta infraestructura donde se evidencie la solicitud de pedido y la garantía de entrega. Así mismo, pagará al Contratista el restante 84.3% mediante actas parciales en mensualidades vencidas por el servicio efectivamente prestado, previa presentación de la respectiva factura, actas de ejecución e informes aprobados por la supervisión del contrato del Departamento, acorde con el valor total de los servicios prestados, de conformidad con la oferta finalmente presentada por el contratista en relación con el componente fijo y el componente variable del presupuesto.

Para el último pago se requerirá acta de liquidación final del contrato. Para ordenar cualquier pago se deberá allegar por el contratista la constancia de cumplimiento a satisfacción del objeto contractual expedido por el supervisor designado por el Departamento, al igual que el pago del sistema de seguridad social integral y parafiscal.

NOTA 1: En el evento de agotarse el plazo de ejecución y no se haya agotado la totalidad del presupuesto asignado se liberará el correspondiente saldo si a ello hubiere lugar.

NOTA 2: VALOR. En el valor se entienden incluidos los costos directos e indirectos que ocasione la ejecución del contrato.

NOTA 3: DOCUMENTOS SOPORTES. El contratista deberá presentar la factura o la cuenta de cobro, según sea el caso, constancia de pago de aportes a la seguridad social, parafiscales, riesgos profesionales y demás documentos requeridos para el pago de la cuenta de cobro.

NOTA 4. El proceso contempla la adquisición de soluciones de ciberseguridad destinadas a la protección de bases de datos, lo cual es evidenciado en el alcance del ítem 3. Adicionalmente, incorpora otras capacidades y soluciones de seguridad informática, dando cumplimiento al enfoque integral de experiencia requerido. La infraestructura necesaria, soportada para el primer pago en mención, deberá ser entregada por el contratista a la orden y propiedad del Departamento de Santander. La misma se detalla en el anexo técnico.

12.1. GRAVÁMENES:

El presente listado de gravámenes es una lista meramente enunciativa y no vinculante para el contratista, razón por la cual, dependiendo de la cuantía y el tipo de contrato a ejecutar, el monto y el tipo de gravamen puede variar, por lo cual el contratista puede acercarse a la Secretaría de Hacienda del Departamento a fin de obtener toda la información correspondiente. Así mismo, el contratista no podrá alegar desequilibrio económico con base a que la entidad no comunicó adecuada y cabalmente los gravámenes o impuestos a pagar con ocasión de ejecución del

contrato, puesto que las normas tributarias son de carácter público, general y de conocimiento completo por parte de todos los ciudadanos.

DESCRIPCION	TARIFA	OBSERVACIONES Fuente estatuto tributario Departamental
Estampilla Pro Adulto Mayor	**2%**	**EXENCIONES:1). Los convenios interadministrativos, entendiendo por éstos los negocios jurídicos celebrados por dos o más entidades públicas para aunar esfuerzos, recursos e intereses comunes para lograr el cumplimiento de una finalidad estatal impuesta por la Constitución ó la ley sin que por ello se reciba ningún pago ó ventaja económica para alenzar los fines que en todo caso deben ser acordes con el interés general. 2). Los contratos y/o convenios interadministrativos que celebre el Departamento desarrollado con Monopolios Rentísticos (Ley 223 de 1995)' 3). Los contratos de empréstito que celebre le Departamento con entidades financieras. 4). Los contratos Interadministrativos que celebre el Departamento con la Red Pública en salud para la compra de servicios de salud para la atención de la población vinculada.**
Estampilla Pro Cultura	**2%**	**EXENCIONES: Los convenios interadministrativos, entendiendo por éstos los negocios jurldicos celebrados por dos o más entidades públicas para aunar esfuerzos, recursos e intereses comunes para lograr el cumplimiento de una finalidad estatal impuesta por la Constitución ó la ley sin que por ello se reciba ningún pago ó ventaja económica para alenzar los fines que en todo caso deben ser acordes con el interés general.**
Estampilla Pro Electrificación	**2%**	**EXENCIONES: Los convenios interadministrativos, entendiendo por éstos los negocios jurídicos celebrados por dos o más entidades públicas para aunar esfuerzos, recursos e intereses comunes para lograr el cumplimiento de una finalidad estatal impuesta por la Constitución ó la ley sin que por ello se reciba ningún pago ó ventaja económica para alenzar los fines que en todo caso deben ser acordes con el interés general.**
Estampilla Pro Desarrollo	**2%**	**EXENCIONES:1). Los convenios interadministrativos, entendiendo por éstos los negocios jurídicos celebrados por dos o más entidades públicas para aunar esfuerzos, recursos e intereses comunes para lograr el cumplimiento de una finalidad estatal impuesta por la Constitución ó la ley sin que por ello se reciba ningún pago ó ventaja económica para alenzar los fines que en todo caso deben ser acordes con el interés general. 2). Los Contratos de prestación de servicios de cuantía mínima de orden departamental y municipal**
Estampilla Pro Uis	**2%**	**EXENCIONES:1). Los convenios interadministrativos, entendiendo por éstos los negocios jurídicos celebrados por dos o más entidades públicas para aunar esfuerzos, recursos e intereses comunes para lograr el cumplimiento de una finalidad estatal impuesta por la Constitución ó la ley sin que por ello se reciba ningún pago ó ventaja económica para alenzar los fines que en todo caso deben ser acordes con el interés general. 2). Se fija como mínimo para gravar la prestación de servicios aquellos que superen los tres (3) salarios mínimos legales mensuales vigentes.**
Estampilla Pro Hospitales	**2%**	**EXENCIONES: Los convenios interadministrativos, entendiendo por éstos los negocios jurídicos celebrados por dos o más entidades públicas para aunar esfuerzos, recursos e intereses comunes para lograr el cumplimiento de una finalidad estatal impuesta por la Constitución ó la ley sin que por ello se reciba ningún pago ó ventaja económica para alenzar los fines que en todo caso deben ser acordes con el interés general.**
Tasa Pro Deporte	**2%**	**EXENCIONES: Los convenios y contratos de condiciones uniformes de los servicios públicos domiciliarios, de prestación de servicios suscritos con personas naturales, educativos y los que tienen que ver con el refinanciamiento y el servicio de la deuda pública**
ESTAMPILLA PRO ADULTO MAYOR (*Dependen de la categoría del DPTO)		**De conformidad con el Artículo 4 de la ley 1276 de 2009 y el Artículo 2 de la ley 687 de 2001 una vez el Departamento sea recategorizado a primera categoría, la tarifa que se aplicara por concepto de estampillas para el bienestar del adutto mayor será del 2% del valor de los contratos, sus adicionales celebrados por los municipios el departamento y sus entidades descentralizadas. Se tiene en cuenta la fecha del contrato, asi: 2% 2407221001 Contratos suscritos del 2020 en adelante 2.5% 2407221002 Contratos suscritos del 2014 a 2015 3% 2407221003 Contratos suscritos del 2016 a 2019**

Nota 1: 5 X 1000 – ICA (Solo aplica para obras ejecutadas en Bucaramanga)

Nota 2 Los demás gravámenes Ordenanzales y de Ley a que haya lugar.

OTROS PAGOS:

a) Fondo de seguridad ciudadana: (5%). Contribución especial de que trata la Ley 418 de 1997, prorrogada y modificada por las leyes 548 de 1999, 782 de 2002, 1106 de 2006, 1421 de 2010 y 1738 de 2014.
b) Sujeto pasivo CREE.
c) Retención en la fuente, según corresponda. 1% Obra.
d) Igualmente debe tener en cuenta el costo de las pólizas y demás erogaciones a que haya lugar.

13. ESTUDIOS DEL SECTOR

En cumplimiento del artículo 2.2.1.1.1.6.1 del Decreto 1082 de 2015, el Departamento de Santander realizó en documento anexo al presente documento, y siguiendo los lineamientos que para el efecto Colombia Compra Eficiente estableció en la respectiva guía, el correspondiente análisis económico del sector con el fin de establecer el contexto del proceso de contratación a realizar, el cual contiene tres áreas a saber:

a) Análisis del mercado
b) Análisis de la demanda
c) Análisis de la oferta

14. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE.

Según lo establecido en el artículo 2.2.1.1.2.2.2 del Decreto 1082 de 2015, la Entidad debe determinar la oferta más favorable para el caso de selección mediante licitación pública teniendo en cuenta:

*"**a)** La ponderación de los elementos de calidad y precio soportados en puntajes o fórmulas;*
o
***b)** La ponderación de los elementos de calidad y precio que representen la mejor relación de costo- beneficio."*

Para el presente proceso de selección se aplicará la alternativa **a), esto es la ponderación de los elementos de calidad y precio soportados en puntajes o fórmulas.**

14.1. REQUISITOS HABILITANTES

El Departamento de Santander verificara con el Registro Único de Proponentes el cumplimiento de los requisitos habilitantes. Esta verificación se hará de acuerdo con el artículo 2.2.1.1.1.5.2. y 2.2.1.1.1.5.3. del Decreto 1082 de 2015 y el Manual para determinar y verificar los requisitos habilitantes en Procesos de Contratación expedido por Colombia Compra Eficiente.

De conformidad con el numeral 6.1 del artículo 6 de la Ley 1150 de 2007, solo en aquellos casos en que por las características del objeto a contratar se requiera la verificación de requisitos del Proponente adicionales a los contenidos en el RUP, la Entidad Estatal puede hacer tal verificación en forma directa.

14.2 CAPACIDAD JURÍDICA

En el presente Proceso de Contratación pueden participar personas naturales o jurídicas, nacionales o extranjeras; consorcios, uniones temporales o promesas de sociedad futura, cuyo objeto social sea igual o similar con el objeto del contrato a celebrarse.

Las personas jurídicas, nacionales o extranjeras, ya sea en calidad de proponente o integrantes de un proponente plural (Consorcio o Unión Temporal, promesas de sociedad futura o cualquier otro tipo de asociación); deberán acreditar que su duración abarca como mínimo el término contemplado para la ejecución del contrato y UN (1) año más. "

Para participar deberán cumplir con lo siguiente:

a) En caso de persona jurídica, quien presenta la propuesta debe estar autorizado para comprometer la firma por el valor del contrato. En caso de requerir el representante legal autorización para celebrar contratos a partir de determinadas cuantías, deberá presentar la respectiva autorización, para la presentación de la oferta y la suscripción del contrato que se llegare a adjudicar como resultado del presente proceso.

El acta que para el efecto se aporte deberá cumplir con los requisitos y formalidades establecidos en el artículo 189 del Código de Comercio. Si se anexa copia de la respectiva acta, donde se autoriza, esta debe estar firmada en ORIGINAL por el secretario y/o presidente del órgano competente, con la respectiva constancia que es fiel copia del original, que reposa en el libro de actas y que se encuentra debidamente firmada por el presidente y secretario.

En el caso de proponentes plurales, el representante legal de cada una de las personas jurídicas que los integren, deberá contar con dicha autorización, en los mismos términos.

b) Tener capacidad jurídica para la presentación de la oferta, la suscripción y ejecución del contrato.

c) No estar incursos en ninguna de las causales de inhabilidad, incompatibilidad, conflicto de intereses para celebrar o ejecutar el contrato, previstas en la Constitución Política, las leyes de Colombia, en especial las previstas en la Ley 80 de 1993, la Ley 1150 de 2007 y la ley 1474 de 2011. Con la firma de la propuesta se entiende que el oferente, cuando sea persona natural, el representante legal de la persona jurídica, el representante del proponente plural, o los integrantes del plural, no se halla incurso en ninguna causal de incompatibilidad o inhabilidad prevista en la Ley. Cuando la inhabilidad o incompatibilidad sobrevenga en el curso de la selección se entenderá que el proponente renuncia a su participación en el proceso y a los derechos surgidos del mismo.

Para ello, el Departamento revisará el boletín de responsables fiscales, el certificado de antecedentes disciplinarios, el certificado de antecedentes judiciales y el RUP para verificar que no haya sanciones inscritas.

d) No estar incursos en ninguna causal de disolución y/o liquidación.

e) No encontrarse en un proceso de liquidación obligatoria o forzosa

f) Ninguna persona natural o jurídica podrá presentar más de una oferta de manera individual, ni podrá presentar una oferta de manera individual y a su vez formar parte de uno o varios proponentes plurales. En los casos de este numeral, se rechazarán todas las ofertas presentadas en tales condiciones.

Esta disposición se aplicará igualmente para personas jurídicas en su calidad de matrices, filiales o subsidiarias que presenten varias ofertas de manera individual y hagan parte de proponentes plurales.

g) Los proponentes extranjeros deben acreditar un apoderado o representante en Colombia para todos los efectos del proceso contractual, cuando sea el caso, y ceñirse en un todo a lo reglado por las normas legales vigentes.

h) Deberá tenerse en cuenta que un proponente, ya sea como persona natural o jurídica o un miembro de un proponente plural, no podrá ser adjudicatario en dos procesos de selección de los cuales uno de ellos corresponda a la Interventoría del otro. En aplicación del principio de transparencia que rige la contratación estatal, cuando un proponente participe en los dos procesos y resulte adjudicatario de uno de ellos, a partir de dicha adjudicación no podrá continuar participando en el segundo y su propuesta para este último será considerada rechazada.

i) Encontrarse en curso de una de las causales de inhabilidad por incumplimiento reiterado establecida en el artículo 90 de la ley 1474 de 2011

j) No podrá participar quien haya realizado previamente los estudios y/o diseños del proyecto objeto de la presente contratación.

k) Quien haya celebrado un contrato de suministro, obra pública, de concesión, suministro de medicamentos y de alimentos o su conyugue, compañero o compañera permanente, pariente hasta el segundo grado de consanguinidad, segundo de afinidad y/o primero civil o sus socios

en sociedades distintas de las anónimas abiertas, con el Departamento durante el plazo de ejecución y hasta la liquidación del mismo no podrá celebrar contratos de interventoría con esta misma entidad.

l) En el caso de proponente plural cada uno de los miembros del consorcio o unión temporal deberá acreditar los requisitos indicados en el presente pliego dependiendo de su naturaleza jurídica. En el evento que existan limitaciones estatutarias a la capacidad del representante de alguna de las sociedades que conforman el plural para comprometerlas en la presentación de las propuestas o la firma del contrato, deberá aportar autorización del órgano social competente facultando a quien obre en nombre y representación de la persona jurídica para participar en el consorcio o unión temporal y a través de este presentar la propuesta, celebrar y ejecutar el contrato.

m) Las personas jurídicas extranjeras deben acreditar su existencia y representación legal con el documento idóneo expedido por la autoridad competente en el país de su domicilio no anterior a tres (3) meses desde la fecha de presentación de la Oferta, en el cual conste su existencia, fecha de constitución, objeto, duración, nombre representante legal, o nombre de la persona que tenga la capacidad de comprometerla jurídicamente, y sus facultades, señalando expresamente que el representante no tiene limitaciones para contraer obligaciones en nombre de la misma, o aportando la autorización o documento correspondiente del órgano directo que lo faculta.

14.2.1 CARTA DE PRESENTACIÓN DE LA PROPUESTA.

Este documento se realizará de acuerdo con el formato suministrado por la Entidad en el Formato anexo en los pliegos de condiciones, el cual debe estar firmado en original por el proponente, persona natural o por el representante legal de la persona jurídica, o por el representante del proponente plural, indicando su nombre, documento de identidad y demás datos allí requeridos.

El contenido de dicho documento (formato anexo) no podrá ser variado, sin embargo, debe diligenciarse los espacios en blanco y los necesarios para suscribirlo. No podrán señalarse condiciones diferentes a las establecidas en el mismo, no se aceptarán propuestas condicionadas.

Cuando se trate de proponentes que sean personas jurídicas privadas extranjeras que no tengan establecida sucursal en Colombia deberán, además, adjuntar a la propuesta los documentos con los cuales acreditan un apoderado domiciliado en Colombia, debidamente facultado para presentar la propuesta, para la celebración del contrato y para representarla judicial y extrajudicialmente.

No podrán señalarse condiciones diferentes a las establecidas en este pliego de condiciones, so pena de rechazar la propuesta ni se aceptarán propuestas condicionadas.

14.2.2 CERTIFICADO VIGENTE DE CONSTITUCIÓN, EXISTENCIA Y REPRESENTACIÓN LEGAL

a.) Las personas jurídicas ya sea en calidad de proponente o integrantes de un proponente plural (Consorcio o Unión Temporal, promesas de sociedad futura o cualquier otro tipo de asociación; cuyo objeto social sea igual o similar con el objeto del contrato a celebrarse) deberán presentar el certificado de existencia y representación legal con fecha de expedición no superior a treinta (30) días calendario anteriores a la fecha límite de recepción de ofertas, donde conste que de acuerdo con su objeto social cuenta con la capacidad jurídica para celebrar y ejecutar contratos, igualmente el objeto social de la empresa, debe corresponder a actividades relacionadas con el objeto del contrato y acreditar que su duración abarca como mínimo el término contemplado para la ejecución y UN (1) año más

b.) De conformidad con lo establecido en la ley 1258 de 2008, en el documento de constitución de las sociedades por acciones simplificadas, artículo 5°, su objeto social se puede comprender una enunciación clara y completa de las actividades principales o puede expresar que la sociedad realizara cualquier actividad comercial o civil licita. Si nada se expresa en el acto de constitución, se entenderá que la sociedad por acciones simplificadas podrá realizar cualquier actividad lícita. En el evento en que el objeto social de una sociedad por acciones simplificadas no especifica las actividades iguales o similares al objeto a contratar, se entenderá que estas se encuentran dentro de las actividades licitas de la persona jurídica.

c.) Para las personas jurídicas extranjeras, se aplicarán las mismas reglas establecidas para las personas jurídicas nacionales, así mismo los proponentes extranjeros individuales, en consorcio, en unión temporal, o promesa de sociedad futura, deberán cumplir con las condiciones generales establecidas en el Pliego de condiciones y además, deberán tener en cuenta lo siguiente:

c.1.) Las personas jurídicas extranjeras sin sucursal, ni domicilio en Colombia deberán cumplir los siguientes requisitos:

c.1.1.) Acreditar su existencia y representación legal, con el documento idóneo expedido por la autoridad competente en el país de su domicilio, expedido a más tardar dentro de los tres (3) meses anteriores a la fecha de cierre de la convocatoria, en el que conste su existencia, su fecha de constitución, objeto, vigencia, nombre del representante legal, o de la(s) persona(s) que tengan la capacidad para comprometerla jurídicamente y sus facultades, señalando expresamente que el representante no tiene limitaciones para contraer obligaciones en nombre de la misma, o aportando la autorización o documento correspondiente del órgano directivo que le faculte expresamente.

c.1.2.) Acreditar que su objeto social incluya actividades iguales o similares con el objeto del contrato del presente proceso.

c.1.3.) Acreditar la suficiencia de la capacidad de su apoderado o Representante Legal en Colombia, lo cual deberá quedar evidenciado en el documento de constitución de apoderado.

c.1.4.) Si una parte de la información solicitada no se encuentra incorporada en el certificado que acredita la existencia y representación, o si este tipo de certificados no existen de acuerdo con las leyes que rijan estos aspectos en el país de origen de la persona jurídica, la información deberá presentarse adjuntado documento bajo gravedad de juramento, donde se exprese la información antes mencionada y autenticado por una autoridad competente del país de origen.

d.) Todos los proponentes personas jurídicas o integrantes de proponentes plurales nacionales o extranjeros, deben acreditar autorización suficiente del órgano social respectivo para contraer obligaciones en nombre de la sociedad. Dicha autorización debe haber sido otorgada previamente al cierre del proceso de selección. La ausencia definitiva de autorización suficiente determinará la falta de capacidad jurídica para presentar la oferta.

Cuando se prorrogue la fecha de presentación de la propuesta, el certificado de existencia y representación legal tendrá validez con la inicialmente prevista.

Todos los documentos (públicos y privados) otorgados en países no miembros del Convenio de La Haya de 1961, y los privados otorgados en países miembros de este Convenio tendientes a acreditar la existencia y representación legal, deberán presentarse legalizados en la forma prevista en las normas que regulen la materia y en especial el artículo 480 del Código de Comercio, 251 de la ley 1564 de 2011 y la resolución 7144 de 2014 del Ministerio de Relaciones Exteriores.

14.2.2.1 PARA PERSONAS NATURALES

Si el Oferente es una persona natural comerciante ya sea en calidad de proponente o integrantes de un proponente plural (Consorcio o Unión Temporal) deberá presentar un Certificado de Inscripción en el Registro Mercantil expedido por la Cámara de Comercio en donde conste que se encuentra inscrito y su actividad relacionada con el objeto del presente proceso de selección, este certificado debe tener fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha límite de recepción de ofertas. En éste evento, la propuesta se recibe a nombre de la persona natural y no del Establecimiento de Comercio.

14.2.3 INSCRIPCIÓN EN EL REGISTRO ÚNICO DE PROPONENTES (RUP).

De conformidad con el artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015, la información para renovar el registro en la cámara de comercio, debe ser presentada por la persona inscrita en el RUP, a más tardar el quinto día hábil del mes de abril de cada año; de lo contrario cesan los efectos del RUP.

Los proponentes ya sean personas naturales o jurídicas y cada uno de los integrantes del Proponente Plural, deberán estar inscritos en el Registro Único de Proponentes, expedido por la Cámara de Comercio, con fecha no mayor a treinta (30) días de anterioridad a la fecha de cierre del

proceso de selección respectivo, en el cual conste su inscripción y clasificación en el Registro Único de Proponentes (RUP).

NOTA 1: La inscripción del proponente debe encontrarse vigente y en firme, de conformidad con el numeral 6.3 del artículo 6 de la Ley 1150 de 2007 modificado por el Decreto Ley 019 de 2012.

NOTA 2: El Certificado constituye plena prueba respecto de la información allí contenida.

Según el Decreto 579 de 2021 "*Artículo 1. Sustitución de los parágrafos transitorios del artículo 2.2.1.1.1.5.2. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional. Sustitúyanse los parágrafos transitorios del artículo 2.2.1.1.1.5.2. de la Subsección 5 de la Sección 1 del Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, los cuales quedarán así: "PARÁGRAFO TRANSITORIO 1: A partir del 1 de junio de 2021, para efectos de la inscripción en el Registro Único de Proponentes, el interesado reportará la información contable de que tratan los numerales 1.3 Y 2.3 de este artículo, correspondiente a los últimos tres (3) años fiscales anteriores al respectivo acto. En aquel/os eventos en que el proponente no tenga la antigüedad suficiente para aportar la información financiera correspondiente a los tres (3) años descritos en el inciso anterior, podrá acreditar dicha información desde su primer cierre fiscal. El proponente con inscripción activa y vigente que no tenga la información de la capacidad financiera y organizacional de los años 2018 y/o 2019 inscrita en el Registro Único de Proponentes, durante el mes de junio de 2021, podrá reportar por única vez, mediante una solicitud de actualización, únicamente la información contable correspondiente a estos años, sin costo alguno. El proponente que tenga o haya tenido inscrita en la cámara de comercio la información de la capacidad financiera y organizacional de los años 2018 y/o 2019, no deberá presentar la información que repose en la respectiva cámara de comercio, la cual conservará la firmeza para efectos de su certificación. PARÁGRAFO TRANSITORIO 2. En el año 2022, para efectos de la inscripción o renovación del Registro Único de Proponentes, el interesado reportará la información contable de que tratan los numerales 1.3 Y 2.3 de este artículo, correspondiente a los últimos tres (3) años fiscales anteriores al respectivo acto.*
En aquellos eventos en que el proponente no tenga la antigüedad suficiente para aportar la información financiera correspondiente a los tres (3) años descritos en el inciso anterior, podrá acreditar dicha información desde su primer cierre fiscal. El proponente que tenga o haya tenido inscrita en la cámara de comercio la información de la capacidad financiera y organizacional de los años 2019 y/o 2020, no deberá presentar la información que repose en la respectiva cámara de comercio, la cual conservará la firmeza para efectos de su certificación. "

Y de conformidad con el artículo 4 del Decreto 399 de 2021 "*ARTÍCULO 4. Adición de dos parágrafos transitorios al artículo 2.2.1.1.1.5.2. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional. Adiciónense dos (2) parágrafos transitorios al artículo 2.2.1.1.1.5.2. de la Subsección 5 de la Sección 1 del Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, los cuales quedarán así: "PARÁGRAFO TRANSITORIO 1: A partir del 1 de agosto de 2021, para efectos de la inscripción en el Registro Único de Proponentes, el interesado reportará la información contable de que tratan los numerales 1.3 y 2.3 de este artículo, correspondiente a los últimos tres (3) años fiscales anteriores al respectivo acto. En aquellos eventos en que el proponente no tenga la antigüedad suficiente para aportar la información financiera correspondiente a los tres (3) años descritos en el inciso anterior, podrá acreditar dicha información desde su primer cierre fiscal.*

El proponente con inscripción activa y vigente que no tenga la información de la capacidad financiera y organizacional de los años 2018 y/o 2019 inscrita en el Registro Único de Proponentes, durante el mes de agosto de 2021, podrá reportar por única vez, mediante una solicitud de actualización, únicamente la información contable correspondiente a estos años, sin costo alguno.

El proponente que tenga inscrita en la cámara de comercio la información de la capacidad financiera y organizacional de los años 2018 y/o 2019, no deberá presentar la información que repose en la respectiva cámara de comercio, la cual conservará la firmeza para efectos de su certificación.

PARÁGRAFO TRANSITORIO 2: En el año 2022, para efectos de la inscripción o renovación del Registro Único de Proponentes, el interesado reportará la información contable de que tratan los numerales 1.3 y 2.3 de este artículo, correspondiente a los últimos tres (3) años fiscales anteriores al respectivo acto.

En aquellos eventos en que el proponente no tenga la antigüedad suficiente para aportar la información financiera correspondiente a los tres (3) años descritos en el inciso anterior, podrá acreditar dicha información desde su primer cierre fiscal.

El proponente que tenga inscrita en la cámara de comercio la información de la capacidad financiera y organizacional de los años 2019 y/o 2020, no deberá presentar la información que repose en la respectiva cámara de comercio, la cual conservará la firmeza para efectos de su certificación."
Respecto a las sociedades extranjeras con sucursal en el país, el artículo 2.2.1.1.1.5.2 del Decreto 1082 de 2015, señala que deben presentar para el registro único de proponentes, la información contable y financiera de su casa matriz. En consecuencia deben presentar el RUP y el NIT, respectivo, de la sucursal en Colombia.

Los proponentes, personas naturales extranjeras o los plurales que tengan al interior de sus integrantes personas naturales extranjeras no inscritas en el Registro Único de Proponentes por no tener domicilio o sucursal en el país, podrán acreditar este requisito con el documento equivalente en el país donde tengan su domicilio principal o con una declaración rendida bajo la gravedad del juramento donde se exprese que este tipo de certificado no existe en su país de origen, documento que debe estar autenticado por una autoridad competente de dicho país.

Los proponentes, personas jurídicas extranjeras o los plurales que tengan al interior de sus integrantes personas jurídicas extranjeras no inscritas en el Registro Único de Proponentes por no tener domicilio o sucursal en el país, podrán acreditar este requisito con el documento equivalente en el país donde tengan su domicilio principal o con una declaración rendida bajo la gravedad del juramento donde se exprese que este tipo de certificado no existe en su país de origen, documento que debe estar autenticado por una autoridad competente de dicho país.

Todos los documentos (públicos y privados) otorgados en países no miembros del Convenio de La Haya de 1961, y los privados otorgados en países miembros de este Convenio tendientes a acreditar el Registro Único de Proponentes, deberán presentarse legalizados en la forma prevista en las normas que regulen la materia y en especial el artículo 480 del Código de Comercio, 251 de la ley 1564 de 2011 y la resolución 7144 de 2014 del Ministerio de Relaciones Exteriores.

Cuando se prorrogue la fecha de presentación de la propuesta, el certificado te*n*drá validez con la inicialmente prevista.

14.2.4 GARANTIA DE SERIEDAD DE LA PROPUESTA.

El proponente deberá allegar Garantía de Seriedad del Ofrecimiento por un valor del **diez por ciento (10%) del valor de la oferta**, (el artículo 2.2.1.2.3.1.9 del Decreto 1082 de 2015 establece que el valor de esta garantía debe ser de por lo menos el diez (10%) del valor de la oferta), y su vigencia será desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato.

Así mismo, el artículo 2.2.1.2.3.1.6 del Decreto 1082 de 2015, establece que la garantía de seriedad de la oferta debe cubrir la sanción derivada del incumplimiento de la oferta, en los siguientes eventos:

- **a.)** 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 prórroga sea inferior a tres (3) meses.
- **b.)** El retiro de la oferta después de vencido el plazo fijado para la presentación de las ofertas.
- **c.)** La no suscripción del contrato sin justa causa por parte del adjudicatario.
- **d.)** La falta de otorgamiento por parte del proponente seleccionado de la garantía de cumplimiento del contrato.

Esta garantía será otorgada a favor del Departamento de Santander NIT No. 890201235 – 6, y como tomador el nombre del proponente persona natural o el nombre de la persona jurídica, deberá figurar su razón social completa, según el Certificado de Existencia y Representación Legal, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera.

Cuando la oferta es presentada por un proponente plural, como consorcio, unión temporal o promesa de sociedad futura, la garantía debe ser otorgada por todos sus integrantes.

La póliza y sus anexos deberán estar firmados por el garante y el tomador, esto es, por el proponente persona natural, el representante legal de la persona jurídica o el representante del consorcio o unión temporal.

Garantía de Seriedad de la Oferta – Criterios diferenciales para Mipyme y emprendimientos y empresas de mujeres en el sistema de compras públicas. Art 2.2.1.2.4.2.14. y 2.2.1.2.4.2.18. Decreto 1860 de 2021

Con el fin de promover y facilitar la participación en los procedimientos de selección competitivos de las Mipyme domiciliadas en Colombia en cumplimiento de lo establecido en el Decreto 1082 de 2015, Artículo 2.2.1.2.4.2.14. y 2.2.1.2.4.2.18. Criterios diferenciales para Mipyme y emprendimientos y empresas de mujeres en el sistema de compras públicas. (Adicionado por el artículo 3 del Decreto 1860 del 24 de diciembre de 2021), cuando el oferente sea una Mipyme o emprendimientos y empresas de mujeres deberán y/o podrán presentar una GARANTÍA DE SERIEDAD DE LA OFERTA, por Valor Asegurado: Equivalente al cinco por ciento (5%) del valor del presupuesto oficial.

Salvo el valor asegurable, esta garantía deberá cumplir con las mismas condiciones exigidas en el numeral 14.2.4 del presente documento.

Para acreditar la condición de Mipyme, el Proponente entregará copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación. Por su parte, la condición de emprendimientos y/o empresas de mujeres, se probará mediante el diligenciamiento del Formato- Acreditación de emprendimientos y empresas de mujeres, –el cual deberá aportarse con la documentación requerida en el artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015 o la norma que lo modifique, complemente o sustituya.

En cumplimiento de lo dispuesto en el artículo 2.2.1.2.4.2.18. Criterios diferenciales para Mipyme en el sistema de compras públicas del Decreto Reglamentario 1082 de 2015, Adicionado por el Art. 3 del Decreto 1860 de 2021, fija como condición habilitante diferencial que promueve y facilita la participación de las Mipyme domiciliadas en Colombia en los procesos de selección de contratistas el requisito habilitante de experiencia, por lo cual, las Mipymes deberán acreditar el referido requisito de acuerdo a lo siguiente:

Las Mipymes colombianas deben acreditar que tiene el tamaño empresarial establecido por la ley de la siguiente manera:

1. Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil.
2. Las personas jurídicas mediante certificación expedida por el representante legal y el contador o 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 complementen.

La Gobernación de Santander se reserva el derecho de verificar integralmente la autenticidad, exactitud y coherencia de la información aportada por el proponente, tendiente a acreditar su experiencia, pudiendo acudir para ello a las personas, empresas o entidades contratantes.

Con el propósito de adoptar medidas afirmativas que incentiven la participación de las mujeres en el sistema de compras públicas, se entenderán como emprendimientos y empresas de mujeres aquellas que cumplan con alguna de las siguientes condiciones, de acuerdo con el art. 2.2.1.2.4.2.14. del Decreto 1082 de 2015:

“Definición de emprendimientos y empresas de mujeres. (…)
1. Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica pertenezcan a mujeres 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. 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 conste la distribución de los derechos en la sociedad y el tiempo en el que las mujeres han mantenido su participación.

2. Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a 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.

Se entenderá como empleos del nivel directivo aquellos cuyas funciones están relacionadas con la dirección de áreas misionales de la empresa y la toma de decisiones a nivel estratégico. En este sentido, serán cargos de nivel directivo los que dentro de la organización de la empresa se encuentran ubicados en un nivel de mando o los que por su jerarquía desempeñan cargos encaminados al cumplimiento de funciones orientadas a representar al empleador.

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 todas las personas que conforman los cargos de nivel directivo del proponente, el número de mujeres y el tiempo de vinculación.

La certificación deberá relacionar el nombre completo y el número de documento de identidad de cada una de las personas que conforman el 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.

3. Cuando la persona natural sea una mujer y haya ejercido actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior a la fecha de cierre del proceso de selección. Esta circunstancia se acreditará mediante la copia de cédula de ciudadanía, la cédula de extranjería o el pasaporte, así como la copia del registro mercantil.

4. Para las asociaciones y cooperativas, cuando más del cincuenta por ciento (50%) de los asociados sean mujeres y la participación haya correspondido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección. Esta circunstancia se acreditará mediante certificación expedida por el representante legal.

PARÁGRAFO. Respecto a los incentivos contractuales para los emprendimientos y empresas de mujeres, las certificaciones de 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 procedimiento de selección”

A su vez de acuerdo con el parágrafo 1 del artículo 2.2.1.2.4.2.15. del Decreto 1082 de 2015, se tiene que:

“PARÁGRAFO 1. Tratándose de proponentes plurales, los criterios diferenciales y los puntajes adicionales solo se aplicarán si por lo menos uno de los integrantes acredita que es emprendimiento y empresa de mujeres bajo los criterios dispuestos en el artículo precedente y que tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

PARÁGRAFO 2. Los incentivos contractuales para las empresas y emprendimientos de mujeres no excluyen la aplicación de los criterios diferenciales para Mipyme en el sistema de compras públicas”.

Los contratos presentados para acreditación de experiencia, cuyo valor ejecutado se encuentre expresado con moneda extranjera, deben efectuar el siguiente procedimiento para re expresar el valor de dichos contratos en pesos colombianos

a) En caso de que el valor del contrato se encuentre expresado en una moneda o unidad de cuenta diferente al dólar estadounidense, se deben re-expresar a dólares estadounidenses, utilizando para ello la tasa de cambio, correspondiente a la fecha de inicio del contrato, publicada en el sitio de Internet del Banco de La República de Colombia, de acuerdo con la siguiente ruta:

www.banrep.gov.co
Menú de contenido
Series estadísticas
Tasas de cambio
Tasa de cambio de algunas monedas del mundo países que no pertenecen al continente americano
Tipo de tasa (elegir compra)
Serie para un rango de fechas dado
Seleccionar la fecha
Seleccionar la moneda (se obtiene cambio de dólares a la moneda elegida en la fecha requerida, en

el caso del euro considerar hasta la quinta cifra decimal expresa)

Si la tasa de cambio con el dólar estadounidense de la moneda en la que se encuentre el valor del contrato no se encuentra listada, se deberá certificar por la entidad facultada para ello del país de origen del contrato, la tasa de cambio oficial entre esta moneda y el dólar estadounidense en la respectiva fecha de inicio del contrato.

b) Si el valor ejecutado del contrato ya se encuentra expresado en dólares estadounidenses, o se re-expresa a dólares estadounidenses según el procedimiento descrito en el literal anterior, se deberá re-expresar de dólares estadounidenses a pesos colombianos utilizando la Tasa Representativa del Mercado (TRM) publicada en el sitio de Internet del Banco de La República de Colombia, de acuerdo con la siguiente ruta:
www.banrep.gov.co
Menú de contenido Series estadísticas
Cambio Tasa de cambio del peso colombiano
TRM

Serie histórica de la tasa de cambio representativa del mercado (se obtiene cambio de pesos colombianos a dólares en la fecha de inicio del contrato, considerando hasta la segunda cifra decimal expresa).

14.2.5 CERTIFICADO DE ANTECEDENTES FISCALES CONTRALORÍA GENERAL DE LA REPÚBLICA

De conformidad con lo consagrado en el artículo 60 Ley 610 de 2000 y el artículo 42 de la Ley 1952 de 2019, ningún proponente ni los integrantes de proponentes plurales, podrá haber sido declarado responsable fiscalmente, caso en el cual será inhábil para contratar con el Estado durante los cinco años siguientes a la ejecutoria del fallo correspondiente: inhabilidad que cesará cuando la Contraloría competente declare haber recibido el pago o, si este no fuere procedente, cuando la Contraloría General de la República excluya al responsable del boletín de responsables fiscales. Dicha circunstancia se verificará por parte de la entidad en el Boletín de Responsables Fiscales de la Contraloría General de la República vigente a la fecha de cierre del presente proceso de selección.

Igual requisito deberá cumplir el representante legal del proponente plural, así como el representante legal de la persona jurídica, ya sea como proponente o integrante de proponente plural.
Los proponentes extranjeros que no tengan sucursal o domicilio en Colombia (persona natural o persona jurídica, así como los representantes legales de las personas jurídicas y/o del proponente plural, y los integrantes de proponente plural) deberán presentar una declaración rendida bajo la gravedad de juramento en la que se declare que no tiene antecedentes fiscales.

14.2.6 CERTIFICADO DE ANTECEDENTES DISCIPLINARIOS PROCURADURÍA GENERAL DE LA NACIÓN

La entidad hará la consulta en la página web de la Procuraduría General de la Nación el Sistema de Información de Registro de Sanciones e Inhabilidades (SIRI), para verificar la existencia o no de antecedentes disciplinarios del proponente (persona natural o persona jurídica, representante legal de la persona jurídica y del proponente plural así como los integrantes del proponente plural).

En caso que en el certificado de antecedentes disciplinarios conste que el proponente presenta antecedentes disciplinarios vigentes que impliquen inhabilidad para contratar con el Estado, su propuesta será rechazada.

Los proponentes extranjeros que no tengan sucursal o domicilio en Colombia (persona natural o persona jurídica, así como los representantes legales de las personas jurídicas y/o del proponente plural, y los integrantes del proponente plural) deberán presentar una declaración rendida bajo la gravedad del juramento en la que se declare que no tiene antecedentes disciplinarios.

14.2.7 CERTIFICADO JUDICIAL

Ningún proponente persona natural o representante legal de personas jurídicas o representante legal del proponente plural, podrá registrar antecedentes judiciales, para lo cual la entidad verificará en la

página de la Policía Nacional, dicha circunstancia, antes del cierre de propuestas. De igual forma todas las personas naturales que integren los Proponentes plurales y los representantes legales de la persona jurídica que conforman dichos proponentes plurales, no podrán registrar antecedentes judiciales; así mismo de quien abona la propuesta si es del caso.

Los proponentes extranjeros que no tengan sucursal o domicilio en Colombia (persona natural o persona jurídica, así como los representantes legales de las personas jurídicas y/o del proponente plural, y los integrantes de proponentes plurales) deberán presentar una declaración rendida bajo la gravedad del juramento en la que se declare que no tiene antecedentes judiciales.

14.2.8 CERTIFICADO DE MEDIDAS CORRECTIVAS

Registro Nacional de medidas correctivas RNMC, de la Policía Nacional de Colombia, Artículo 183, Numeral 4, Código Nacional de Policía y Convivencia / Certificado del sistema nacional de medias correctivas RNMC del representante legal.

14.2.9 REGISTRO ÚNICO TRIBUTARIO (RUT)

Todo proponente, Persona Natural o Jurídica o su Representante Legal, en forma individual o integrantes de proponentes plurales, deberán presentar REGISTRO ÚNICO TRIBUTARIO, emitido por la DIAN.

14.2.10 DOCUMENTO DE IDENTIDAD

Todo proponente Persona Natural, Representante Legal de la persona jurídica o representante del proponente plural y cada uno de los integrantes de proponentes plurales deberán anexar fotocopia del documento de identificación VIGENTE; así mismo de quien abona la propuesta, si es del caso.

Así mismo todas las personas de origen extranjero que sean integrantes de proponentes plurales y/o representantes legales de estos o proponente como persona natural deberán anexar fotocopia del pasaporte actual y vigente.

14.2.11 SITUACIÓN MILITAR DEFINIDA

El Proponente futuro contratista, cuando sea Persona Natural, o Representante Legal de la Persona Jurídica, o del proponente plural, y los integrantes de proponentes plurales, deben anexar fotocopia de la libreta Militar o documento que acredite tener su situación militar definida, siempre y cuando tengan edad inferior a los 50 años. Según lo dispuesto en el artículo 111 del Decreto 2150 del 1995.

14.2.12 CERTIFICACIÓN SOBRE EL CUMPLIMIENTO DE LAS OBLIGACIONES DE SEGURIDAD SOCIAL Y PAGO DE APORTES PARAFISCALES.

De conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002 y el artículo 23 de la Ley 1150 de 2007, a la fecha de la presentación de la propuesta, el oferente deberá aportar certificación expedida por el revisor fiscal, cuando este exista, de acuerdo con los requerimientos de ley, o en su defecto por el representante legal con el cual se acreditará el cumplimiento de la obligación de los aportes de sus empleados a los sistemas de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje como mínimo en los seis (6) meses anteriores a la presentación de la oferta, debidamente firmada en **ORIGINAL**.

Si se trata de un proponente plural, se deberá allegar la certificación de cumplimiento antes mencionada para cada uno de los miembros.

De igual forma, las personas naturales que actúen a título propio o dentro de un proponente plural, deberán acreditar que se encuentran al día en el pago de los aportes parafiscales, debidamente firmada en **ORIGINAL**.

(Ver formato anexo al pliego de condiciones).

Los proponentes extranjeros que no tengan sucursal o domicilio en Colombia (persona natural o persona jurídica, así como los integrantes del proponente plural) deberán presentar una declaración rendida bajo la gravedad del juramento en la que se declare el cumplimiento de las siguientes obligaciones en Colombia, como son, los aportes de sus empleados a los sistemas de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje como mínimo en los seis (6) meses anteriores a la presentación de la oferta, debidamente firmada en **ORIGINAL**.

14.2.13 DOCUMENTO DE CONSTITUCIÓN DEL PROPONENTE PLURAL.

En el evento en que la oferta vaya a ser presentada bajo la figura del Consorcio o Unión Temporal, se deberá allegar el documento de constitución conforme al formato en el anexo 2 al pliego de condiciones y en este constar por lo menos:

a) La modalidad de asociación.
b) Objeto del proceso de selección.
c) Tiempo de duración que no debe ser inferior al término de duración del proceso, celebración y ejecución del contrato y un (1) año más.
d) Nombre del proponente plural y de sus integrantes.
e) El porcentaje de participación de cada una de las partes.
f) La indicación que ninguna de las partes podrá ceder su participación a los demás integrantes del proponente plural ni a terceros, sin autorización previa de la entidad contratante. Igual autorización se requerirá, cuando la modalidad de asociación sea el contratista.
g) La indicación que ninguna de las partes podrá ceder su participación a los demás integrantes del proponente plural ni a terceros, sin autorización previa y por escrito de la entidad contratante. Igual autorización se requerirá, en el evento que el consorcio o unión temporal ostente la calidad de contratista.
h) Cuando el representante legal de la persona jurídica integrante de proponente plural, requiere de autorización para ser parte o integrar un proponente plural, deberá anexarse el documento por medio del cual se otorgue la autorización.
i) FIRMADO EN ORIGINAL por los integrantes y el representante del proponente plural.

Cuando la constitución se efectué bajo la figura de la Unión Temporal se deben señalar los términos y extensión de la participación de cada integrante en la propuesta y en la ejecución del contrato.

14.2.14 CERTIFICADO DEL REDAM

Todo proponente Persona Natural, Representante Legal de la persona jurídica o representante del proponente plural y cada uno de los integrantes de proponentes plurales deberán anexar copia del Registro de Deudores Alimentarios Morosos (REDAM) según lo establecido en el Decreto 1310 de 2022; así mismo de quien abona la propuesta, si es del caso.

14.2.15 AUSENCIA DE INHABILIDADES, INCOMPATIBILIDADES O PROHIBICIONES PARA CONTRATAR CON EL ESTADO

Para el caso de las personas jurídicas el representante legal, deberá presentar una declaración en la cual conste que ni el, ni la persona jurídica, ni los miembros de la junta directiva se encuentran inmersos en alguna causal de inhabilidad, incompatibilidad o prohibiciones para contratar con el estado de acuerdo con la Constitución y la ley, en el mismo sentido el proponente persona natural deberá aportar dicha declaración bajo los mismos parámetros señalados en el presente numeral.

14.2.16 COMPROMISO DE TRANSPARENCIA Y ANTICORRUPCION

El oferente deberá allegar los compromisos de transparencia y anticorrupción, los cuales deberán ser diligenciados conforme a los formatos contenidos en el anexo al pliego de condiciones.

14.2.17 ACTA DE JUNTA DE SOCIOS.

Cuando se desprenda del Registro Único de Proponentes que el representante legal del proponente ya sea como persona jurídica o como proponente plural, requiere de autorización para presentar oferta y/o suscribir contratos, deberá anexar el documento por medio del cual se otorgue esa autorización.

Lo anterior de conformidad con las formalidades establecidas en el artículo 189 de la ley 410 de 1971 (Código de Comercio).

14.3 REQUISITOS DE ORDEN TECNICO

14.3.1 CONDICIONES DE EXPERIENCIA

La Entidad requerirá como experiencia un mínimo de condiciones, que van desde requerimientos generales hasta requerimientos específicos, los cuales se consideran adecuados y proporcionales al objeto del contrato a ejecutar, a la magnitud, el alcance, el presupuesto asignado y a la finalidad de la Entidad, la cual busca un contratista que cuente con la experiencia suficiente en la realización de labores iguales o similares al objeto contractual. Se busca que quienes formulen propuesta, sean oferentes que gracias a su experiencia cuenten con solidez, posicionamiento y permanencia en el mercado. Así, deberá ajustarse a las siguientes reglas o condiciones:

i. La experiencia solicitada respecto al objeto y a los códigos del Clasificador de los Bienes y servicios de Naciones Unidas (UNSPSC), obedecen a requerimientos generales que consisten en que el proponente cuente con experiencia en las principales actividades, bienes o servicios a ejecutar o entregar de acuerdo con el correspondiente presupuesto del contrato, las cuales son un referente mínimo que debe cumplir el proponente.

ii. Los proponentes deben acreditar su experiencia a través de: i) la información consignada en el RUP para aquellos que estén obligados a tenerlo, ii) la presentación el Formato – Experiencia para todos los proponentes y iii) alguno de los documentos válidos para la acreditación de la experiencia cuando se requiera la verificación de información del proponente adicional a la contenida en el RUP.

iii. La evaluación de la experiencia se efectuará a partir de la información contenida en el Registro Único de Proponentes (RUP) vigente y en firme antes del cierre del proceso.

iv. Los proponentes podrán acreditar experiencia proveniente de contratos celebrados con particulares o entidades estatales.

v. La Entidad solo tendrá en cuenta los contratos cuyo objeto esté relacionado con la experiencia general y específica. Se deberá valorar aquellos contratos en el marco de los cuales se hayan ejecutado múltiples actividades, siempre que alguna de estas se relacione con la experiencia requerida. En este último caso, se acreditará la experiencia de acuerdo con el valor proporcional a las actividades, bienes o servicios requeridos.

vi. Los contratos deben haber terminado antes de la fecha de cierre del presente proceso de contratación.

vii. Para los contratos que sean aportados por personas jurídicas que no cuentan con más de tres (3) años de constituidas, que pretendan acreditar la experiencia de sus socios, accionistas o constituyentes, de conformidad con la posibilidad establecida en el numeral 2.5 del artículo 2.2.1.1.1.5.2. del Decreto 1082 de 2015, además del RUP deben adjuntar un documento suscrito por el representante legal y el revisor fiscal o contador público (según corresponda) donde se indique la conformación de la persona jurídica. La Entidad tendrá en cuenta la experiencia de los accionistas, socios o constituyentes de las sociedades con menos de tres (3) años de constituidas. Pasado este tiempo, la sociedad conservará esta experiencia, tal y como haya quedado registrada en el RUP.

viii. Las auto certificaciones no servirán para acreditar la experiencia requerida, ya que con estas no puede constatarse la ejecución de contratos que deben certificar los terceros que recibieron los bienes, servicio u obra. Para la aplicación de esta regla se entiende por auto certificaciones aquellas expedidas por el mismo Proponente, sus representantes, los integrantes del Proponente Plural o del mismo grupo empresarial para demostrar su propia experiencia.

ix. El oferente para acreditar su experiencia, teniendo en cuenta que el RUP presenta información limitada que no permite determinar el objeto y alcance del contrato, deberá presentar copia del contrato con el anexo técnico y certificación de contrato terminado, y/o acta de terminación y/o recibo final del contrato.

14.3.1.1. EXPERIENCIA GENERAL

Para acreditar esta experiencia, la Entidad solicita la presentación de hasta **dos (2) contratos ejecutados en su totalidad**, es decir, con un porcentaje de ejecución del cien por ciento (100%), y debidamente terminados y/o liquidados, cuyo objeto evidencie la prestación de servicios con características técnicas iguales o similares a las requeridas por la Entidad, relacionadas con adquisición o prestación de servicios de monitoreo con implementación o administración y seguridad de plataformas tecnológicas, infraestructura tecnológica y/o monitoreo de incidentes de seguridad informática, atención correctiva de incidentes, gestión de eventos de seguridad, operación de centros de monitoreo y ciberseguridad (SOC), o que dentro de su alcance permitan evidenciar la ejecución de actividades principales y no accesorias contempladas en el numeral 8.2 del Estudio Previo.

Dicho(s) contrato(s) deberá(n) constar en el RUP, identificado(s) cada uno con el Clasificador de Bienes y/o Servicios de Naciones Unidas (UNSPSC). La inscripción en los códigos se acredita mediante el Certificado de Registro Único de proponentes. Cada contrato aportado deberá contar con al menos 15 códigos de la clasificación aquí señalada:

CLASIFICACION	DESCRIPCION
80101500	Servicios de consultoría de negocios y administración corporativa
80101600	Gerencia de Proyectos
80111500	Desarrollo de recursos humanos
80111700	Servicios de contratación
81111500	Ingeniería de software o hardware
81111700	Sistema de manejo de información MIS
81111800	Servicios de sistemas y administración de componentes de sistemas
81111900	Sistema de recuperación de información
81112000	Servicios de datos
81112200	Mantenimiento y soporte de software
81112300	Mantenimiento de soporte de hardware de computador
81161700	Servicios de telecomunicaciones
81161800	Servicios de alquiler o arrendamiento de equipos o plataformas de voz y datos o multimedia
72151200	Servicios de instalación y mantenimiento de sistemas de climatización
72151500	Servicios de instalación y mantenimiento de sistemas eléctricos
32151900	Componentes de circuitos integrados
43201600	Componentes de computadores
43201800	Dispositivos de almacenamiento
43201900	Dispositivos de red
43221700	Equipo de comunicaciones
43221800	Equipo de comunicaciones de datos
43222500	Equipos de seguridad de red
43222600	Equipo de servicio de red
43232200	Software de gestión de contenidos
43233200	Software de seguridad y protección
43233400	Software de controladores de dispositivos y utilidades
43233700	Software de Administración de sistemas

CONDICIONES PARA LA ACREDITACIÓN DE LA EXPERIENCIA GENERAL

NOTA 1: Al menos uno (1) de los contratos aportados deberá acreditar experiencia en la operación de un Centro de Operaciones de Ciberseguridad (SOC), incluyendo como mínimo actividades de monitoreo y correlación de eventos de seguridad mediante el suministro e implementación de plataformas tipo SIEM, gestión y atención de incidentes de ciberseguridad y gestión de

vulnerabilidades sobre activos tecnológicos.

NOTA 2: Contenido de las certificaciones de experiencia.

Los documentos de certificación presentados por los proponentes para acreditar la experiencia deberán ser expedidas por la entidad contratante, donde se especifique por lo menos lo siguiente:

a. Nombre del contratante
b. Nombre del contratista.
c. Objeto y alcance del contrato.
d. Fecha de inicio y fecha de terminación del contrato.
e. Valor del contrato

Nombre y firma de quien(es) suscribe(n) el documento y/o de quien(es) emite(n) la certificación
Estas condiciones de experiencia se han basado en el análisis de servicios a adquirir necesarios para la entidad, como resultado del análisis de contratos de objetos y alcances similares, los cuales se citan en los documentos del actual proceso y sus estudios previos. Es así como se ha determinado que la idoneidad de los proponentes requiere de su experiencia previa en contratos cuyos objetos, cuantías y alcance sean proporcionales al objeto del presente proceso

NOTA 3: Acreditación de experiencia obtenida mediante consorcios o uniones temporales.

Cuando el contrato presentado para acreditar experiencia haya sido ejecutado por un consorcio o unión temporal del cual haya formado parte el proponente o alguno de sus integrantes, el valor y/o la cantidad de bienes, servicios u obras que se reconocerán corresponderán a la proporción que resulte de aplicar el porcentaje de participación del integrante en el contrato original al valor y/o a las cantidades efectivamente ejecutadas.

Para tal efecto, deberá aportarse el documento de constitución del consorcio o unión temporal cuando el porcentaje de participación no pueda determinarse a partir de los demás documentos presentados. Si no se acredita dicho porcentaje, la experiencia no podrá ser reconocida en la proporción correspondiente.

Cuando un mismo contrato haya sido ejecutado por uno o varios integrantes del proponente plural que participa en el presente proceso, la experiencia podrá ser acreditada por cada integrante que haya participado en su ejecución, de acuerdo con su porcentaje de participación en el contrato original. Para efectos de contabilizar el número de contratos, se aplicarán las reglas del presente proceso, sin que la presentación de un mismo contrato por varios integrantes permita contabilizarlo más de una vez por un mismo integrante.

NOTA 4: Acreditación de experiencia por parte de consorcios y uniones temporales.

Cuando el proponente se presente bajo la modalidad de consorcio o unión temporal, la experiencia general y/o específica exigida podrá ser acreditada por uno o varios de sus integrantes, de manera individual, parcial o conjunta, mediante los contratos y demás documentos admisibles conforme a las reglas del presente proceso.

En consecuencia, **no será obligatorio que cada integrante del consorcio o unión temporal acredite experiencia de manera individual**, ni que aporte un contrato propio para cumplir este requisito. Uno de los integrantes podrá acreditar por sí solo la totalidad (100 %) de la experiencia requerida, o varios integrantes podrán complementarla entre sí, siempre que se cumplan las condiciones exigidas en cuanto al objeto, las actividades, el valor, las cantidades, el número de contratos y los demás criterios de acreditación establecidos en el pliego de condiciones.

La experiencia aportada por cada integrante se verificará de acuerdo con las reglas aplicables a su naturaleza y forma de ejecución. La conformación plural no dará lugar a exigir requisitos adicionales de experiencia individual que no estén previstos expresamente en el presente proceso. En el caso que solo uno o algunos de los integrantes del Proponente Plural acredite(n) la experiencia General, este o estos, deberá tener una participación mínima igual o superior al treinta por ciento (30%) en el Consorcio o en la Unión Temporal.

NOTA 5. Conversión de valores expresados en moneda extranjera.

Cuando el valor ejecutado del contrato se encuentre expresado en una moneda diferente al dólar

estadounidense, deberá convertirse a dólares estadounidenses utilizando la tasa de cambio correspondiente a la fecha de inicio del contrato, publicada por el Banco de la República de Colombia, cuando se encuentre disponible para la moneda respectiva.

Para consultar la información, podrá utilizarse la página oficial www.banrep.gov.co, en la sección de series estadísticas y tasas de cambio. Deberá seleccionarse la serie correspondiente a la moneda del contrato y la fecha requerida, aplicando la tasa de compra, cuando corresponda a la metodología de conversión establecida por dicha fuente.

Si la tasa de cambio de la moneda del contrato frente al dólar estadounidense no se encuentra disponible en la fuente indicada, deberá aportarse certificación expedida por la autoridad o entidad competente del país de origen que permita establecer la tasa de cambio oficial aplicable a la fecha de inicio del contrato.

Cuando el valor ejecutado se encuentre expresado en dólares estadounidenses, o se haya convertido a dicha moneda conforme al procedimiento anterior, deberá convertirse a pesos colombianos utilizando la Tasa Representativa del Mercado (TRM) correspondiente a la fecha de inicio del contrato, publicada por el Banco de la República de Colombia.

Para efectos de las conversiones, se aplicará la precisión decimal establecida por la fuente oficial correspondiente.

NOTA 6: Experiencia de personas jurídicas con menos de tres (3) años de constitución.

Cuando el proponente sea una persona jurídica, que tenga menos de tres (3) años de constituida, puede acreditar la experiencia de sus accionistas, socios o constituyentes, siempre y cuando se cumplan las condiciones para su validez y acreditación.

NOTA 7: **Formato de relación de experiencia.**

El proponente deberá diligenciar y presentar el FORMATO establecido para la relación de EXPERIENCIA, del pliego de condiciones.

NOTA 8: Número de contratos y valor mínimo de experiencia.

Dar lectura a numeral B.1.1.

NOTA 9. Acreditación de experiencia en contratos celebrados entre particulares.

Para acreditar experiencia derivada de contratos celebrados entre particulares, el proponente deberá aportar los documentos exigidos en el presente proceso y, adicionalmente, una certificación de facturación expedida con posterioridad a la fecha de terminación del contrato, suscrita por el revisor fiscal o contador público del proponente que acredita la experiencia, según corresponda.

A la certificación deberán adjuntarse copia de la tarjeta profesional y certificado de antecedentes disciplinarios vigente del profesional, expedido por la Junta Central de Contadores, o los documentos equivalentes que correspondan en el país de expedición, cuando se trate de profesionales sujetos a una regulación extranjera.

NOTA 10. No aceptación de subcontratos.

Para acreditar la experiencia exigida en el presente proceso, no se aceptarán subcontratos.

NOTA 11. Acreditación de actividades principales y no accesorias.

Por *"actividades principales y no accesorias"* se entenderán los dispuestos en aquellos contratos que se presenten para acreditar experiencia general y que contemplen un objeto donde su servicio sea el mismo o similar directamente relacionado con la actividad acreditada en el numeral 8.2 del estudio previo, para el cumplimiento del criterio. Por lo tanto, no serán validos contratos que acrediten objetos distintos a los del alcance del mencionado numeral, o que en las actividades dispuestas en el contrato de acreditación incluya una de las del numeral 8.2, de manera accesoria a servicios o adquisiciones de otra índole.

14.3.1.2 EXPERIENCIA ESPECÍFICA

El proponente deberá acreditar la ejecución de **un (1) contrato**, cuyo valor ejecutado sea igual o superior al cien por ciento (100 %) del presupuesto oficial del presente proceso, y que se encuentre debidamente finalizado y/o liquidado y/o facturado, según corresponda.

Número de contratos con los cuales el Proponente cumple la experiencia acreditada	Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)
1 contrato	100%

El objeto, las obligaciones o el alcance del contrato deberán acreditar el suministro, adquisición o licenciamiento de soluciones de ciberseguridad destinadas a la protección de bases de datos, y deberán incluir, adicionalmente, al menos una (1) de las siguientes capacidades o soluciones de seguridad informática:

1. Protección de estaciones de trabajo y servidores mediante tecnologías de detección y respuesta extendida (XDR).
2. Detección y respuesta ante amenazas de red mediante soluciones especializadas de seguridad de red (NDR).
3. Monitoreo de marca, presencia digital y riesgos asociados a la reputación de la entidad.
4. Gestión de vulnerabilidades y protección de servicios de directorio activo.

Las capacidades descritas podrán acreditarse mediante el objeto, las obligaciones, el alcance o las actividades efectivamente ejecutadas en el contrato presentado, siempre que su documentación permita verificar su correspondencia con los requisitos establecidos.

El contrato deberá estar inscrito en el Registro Único de Proponentes (RUP) y clasificado mediante los códigos del Clasificador de Bienes y Servicios de las Naciones Unidas (UNSPSC) exigidos en el presente proceso. Para acreditar este requisito, el proponente deberá aportar el certificado del RUP vigente y en firme, conforme a las disposiciones aplicables.

Entre los contratos aportados para la acreditación de la experiencia específica, se deberá contar con al menos quince (15) códigos UNSPSC correspondientes a los bienes y servicios relacionados con el objeto contractual y definidos por la Entidad en el pliego de condiciones.

CLASIFICACION	DESCRIPCION
80101500	Servicios de consultoría de negocios y administración corporativa
80101600	Gerencia de Proyectos
80111700	Servicios de contratación
81111500	Ingeniería de software o hardware
81111700	Sistema de manejo de información MIS
81111800	Servicios de sistemas y administración de componentes de sistemas
81111900	Sistema de recuperación de información
81112000	Servicios de datos
81112200	Mantenimiento y soporte de software
81112300	Mantenimiento de soporte de hardware de computador
81161700	Servicios de telecomunicaciones
81161800	Servicios de alquiler o arrendamiento de equipos o plataformas de voz y datos o multimedia
72151200	Servicios de instalación y mantenimiento de sistemas de climatización
72151500	Servicios de instalación y mantenimiento de sistemas eléctricos
43232200	Software de gestión de contenidos
43233200	Software de seguridad y protección

43233400	Software de controladores de dispositivos y utilidades
43233700	Software de Administración de sistemas

14.3.2 CONDICIONES TÉCNICAS.

El Departamento de Santander estima conveniente solicitar unas condiciones técnicas mínimas para la ejecución del contrato, que se consideran indispensables y prioritarias para cumplir a cabalidad con las especificaciones técnicas de las actividades a ejecutar.

Adicionalmente se requiere una cantidad de profesionales, que obedecen a las diferentes especialidades necesarias para la ejecución del contrato, teniendo en cuenta el objeto, valor, magnitud y grado de complejidad del mismo. Para ello es necesario que los proponentes acrediten que cuentan para la ejecución del proyecto, con la disponibilidad de los profesionales que cumplan con los perfiles exigidos, características técnicas y de calidad empresariales en su segmento, así como del equipo requerido.

Lo anterior busca garantizar que los oferentes al realizar sus propuestas incluyan estos aspectos técnicos que afectan de manera directa y ponderada su presupuesto económico

Estas condiciones de experiencia se han basado de los Estudios del sector realizados por la entidad, el cual ha sido el resultado de análisis de contratos de objetos y alcances similares, los cuales se citan en los documentos del actual proceso y sus estudios previos. Es así como se ha determinado que la idoneidad de los proponentes requiere de su experiencia previa en contratos cuyos objetos, cuantías y alcance sean proporcionales al objeto del presente proceso.

14.3.2.1 PERSONAL MINIMO REQUERIDO

El contratista deberá tener disponible para la ejecución del contrato el equipo necesario para dar cumplimiento a su objeto. El Contratista no se exime de la obligación de suministrar oportunamente el equipo necesario para cumplir con los programas, plazos y especificaciones técnicas de los trabajos, a solicitud del Supervisor, so pena de la aplicación de las sanciones que se establezcan en el contrato.

El contratista además del personal mínimo podrá contar con el personal que él estime conveniente para el buen desenvolvimiento del servicio encomendado. Es obligación del contratista suministrar y mantener durante la ejecución del servicio y hasta la terminación del mismo, a satisfacción de la entidad contratante, todo el personal idóneo y calificado de profesionales, tecnólogos y demás que se requieran.

1. El proponente deberá presentar en la propuesta, las hojas de vida de los siguientes perfiles profesionales, los cuales para acreditar su experiencia cumplirán con lo siguiente:

CARGO	CAN	PROFESIONAL	DEDIC.	EXPERIENCIA GENERAL
INGENIERO GERENTE DE PROYECTO PARA LA IMPLEMENTACION Y ASEGURAMINETO DE CALIDAD	1	Título: Ingeniero Eléctrico, Electrónico, Sistemas, Telecomunicaciones y/o carreras afines. Especialización o Maestría en Gerencia de Proyectos y/o especialista en seguridad de la información	50%	**EXPERIENCIA GENERAL** Siete (7) años de experiencia a partir de la expedición de la tarjeta profesional **EXPERIENCIA ESPECÍFICA** Cinco (5) años de experiencia como líder en la implementación de seguridad de la información, gerente de proyecto, diseño, implementación y actualización de las políticas de seguridad de la

		Deberá contar con Certificación PMP vigente.		información alineadas con la norma ISO 27001 **Certificaciones adicionales:** mínimo Seis (6) certificaciones vigentes, de las siguientes: • ITIL foundation V.4 • ISO 27001: 2022 Auditor Lider • IPV6 SILVER • COBIT CERTIFICATION, • CISA (Certified Information System Auditor) • CISM (Certified Information Security Manager) • SFPC (Scrum Foundation Professional Certificate), • CEH (Certified Ethical Hacker). • CNDA - Certified Network Defense Architect • CCISO - Associate Certified Chief Information Security Officer • ISO/IEC 27032:2012 Lead Cybersecurity Manager
INGENIERO GERENTE DE SERVICIO SOC	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines. Especialización o Maestría en Seguridad de la Información ó Informatica ó Ciberseguridad	100%	**EXPERIENCIA GENERAL** Diez (10) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de Siete (7) años como líder o coordinador o gerente de servicios de TI. **EXPERIENCIA ESPECÍFICA** Mínimo Cinco (5) años en Liderar equipo de operaciones y servicios de seguridad. **Certificaciones adicionales:** mínimo Seis (6) certificaciones vigentes, de las siguientes: •Certificación vigente en SCRUM Foundations Professional (SFPC). •Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. •Certificación vigente en LÍDER GESTOR CIBERSEGURIDAD en la norma ISO/IEC 27032:2012 o Superior.

				•ISO31000: 2018 (Lead Risk Manager) •CEH (Certified Ethical Hacker) •CCISO (Associate Certified Chief Information Secutity Officer) •ECSA EC-Council Certified Security Analyst •ISO27035:2016 (INCIDENT MANAGER) •IPv6 Network Engineering Certification •ISO31000: 2018 (Lead Risk Manager) •CNDA (Certified Network Defense Architect)
UN (01) INGENIERO IMPLEMENTADOR	1	Título: Ingeniero Eléctrico, Electrónico, Sistemas, Telecomunicaciones y/o carreras afines. Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad e Informatica forense Deberá contar con Certificación ISO 22301:2019 AUDITOR LIDER	50%	**EXPERIENCIA GENERAL** Cinco (5) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cuatro (4) años en implementación, soporte y/o monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional. **EXPERIENCIA ESPECÍFICA** Tres (3) años de experiencia como líder de Implementación. **Certificaciones adicionales:** • El profesional deberá acreditar como mínimo cuatro (4) certificaciones vigentes, expedidas por el fabricante de las soluciones objeto del proyecto, que certifiquen sus competencias, conocimientos y capacidades para la implementación, administración y soporte de plataformas de ciberseguridad, tales como SIEM, WAF, EDR, Firewall y demás tecnologías afines contempladas en el alcance del contrato.
UN (01) INGENIERO DE SOPORTE	1	Título: Ingeniero Eléctrico, Electrónico, Sistemas, Telecomunicaciones y/o carreras afines.	50%	**EXPERIENCIA GENERAL** Cinco (5) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cuatro (4) años en implementación, soporte y/o monitoreo de soluciones de seguridad.

		Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad		La experiencia se cuenta a partir de la expedición de la tarjeta profesional **EXPERIENCIA ESPECÍFICA** Tres (3) años de experiencia como líder de Soporte de soluciones de seguridad **Certificaciones adicionales:** mínimo tres (3) certificaciones vigentes, de las siguientes: • Certificación ISO 20000-1: 2018 o superior IT SERVICE MANAGEMENT SYSTEMS • Certificación ISO 27032: 2023 o superior (CYBERSECURITY LEAD MANAGER • Certificación vigente en Gestión de Vulnerabilidades emitida por un fabricante que haga parte del cuadrante de Gartner, Forester, o otros • Certificación vigente como especialista en soluciones de acceso seguro perimetral basadas en arquitectura SASE (Secure Access Service Edge) • Certificación vigente como Profesional en Seguridad de Redes **Nota 1:** Las certificaciones requeridas podrán ser acreditadas mediante documentos expedidos por fabricantes de tecnologías, entidades certificadoras o instituciones avaladas y reconocidas en las competencias técnicas exigidas.
UN (01) INGENIERO ANALISTA DE NORMATIVIDAD, PRUEBAS FORENSES – ETHICAL HACKING -	1	Título: Ingeniero Eléctrico, Electrónico, Sistemas, Telecomunicaciones y/o carreras afines. Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad	50%	**EXPERIENCIA GENERAL** Dos (2) años de experiencia a partir de la expedición de la tarjeta profesional **EXPERIENCIA ESPECÍFICA** Un (1) año de experiencia como líder Soc Nivel 2. **Certificaciones adicionales:** mínimo tres (3) certificaciones vigentes, de las siguientes: • Certificación vigente COMPUTER HACKING

				FORENSIC INVESTIGATOR – CHFI • Certificación en SFPC (SCRUM FOUNDATION PROFESSIONAL CERTIFICATE). • ETHICAL HACKING ESSENTIALS – EHE • DIGITAL FORENSICS ESSENTIALS – DFE • AUDITOR INTERNO ISO 27001:2022 BAJO LA NORMA ISO 19011:2018 **Nota 1:** Las certificaciones requeridas podrán ser acreditadas mediante documentos expedidos por fabricantes de tecnologías, entidades certificadoras o instituciones avaladas y reconocidas en las competencias técnicas exigidas.
UN (01) INGENIERO ANALISTA SOC NIVEL 1	1	Título: Ingeniero Eléctrico, Electrónico, Sistemas, Telecomunicaciones y/o carreras afines. Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad ó Seguridad de Redes Telematicas	100%	**EXPERIENCIA GENERAL** Dos (2) años de experiencia a partir de la expedición de la tarjeta profesional **EXPERIENCIA ESPECÍFICA** Un (1) año de experiencia en atención de incidentes informáticos, Gestión de servicio al cliente, soporte técnico, Servicios de Ciberseguridad o seguridad de la información **Certificaciones adicionales:** mínimo tres (3) certificaciones vigentes, de las siguientes: • Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC 27001:2022 • Certificación Vigente CEHPC - ETHICAL HACKING PROFESSIONAL • Certificación vigente como Analista en Centro de Operaciones de Seguridad (SOC) – v1 • Certificación vigente como Profesional en Inteligencia Artificial (CAIPC) - ARTIFICIAL INTELLIGENCE PROFESSIONAL CERTIFICATE • Certificación profesional vigente en DFE – Digital Forensics Essentials (Fundamentos de Informática Forense Digital).

				Nota 1: Las certificaciones requeridas podrán ser acreditadas mediante documentos expedidos por fabricantes de tecnologías, entidades certificadoras o instituciones avaladas y reconocidas en las competencias técnicas exigidas.

NOTA 1: El proponente del proceso deberá anexar, los siguientes documentos del equipo profesional mínimo requerido junto con su propuesta.

1. Fotocopia del certificado de vigencia y antecedentes disciplinarios del consejo nacional profesional de ingeniería, COPNIA, o certificación de vigencia expedida por el ente que corresponda, (certificado vigente a la fecha de inicio).
2. Fotocopia de los diplomas o actas de grado que acrediten la formación de los profesionales.
3. Certificación laboral y/o certificación de prestación de servicios realizada en ejercicio de su profesión requerida en cada perfil específico.
4. El personal mínimo propuesto deberá encontrarse vinculado al proponente mediante una relación contractual vigente, de naturaleza laboral o de prestación de servicios, según corresponda, que garantice su disponibilidad para ejecutar las actividades y cumplir la dedicación exigida para el perfil ofertado.
5. Con la presentación de la oferta, el proponente deberá aportar los documentos que acrediten la vinculación del personal mínimo propuesto, así como los soportes de afiliación y pago de los aportes al Sistema de Seguridad Social Integral y de los aportes parafiscales a que haya lugar, de acuerdo con la modalidad de vinculación y las obligaciones legales aplicables.

NOTA 2: La experiencia general se refiere a la experiencia en ejercicio profesional del equipo profesional mínimo requerido, y corresponde a los años comprendidos entre la fecha de expedición de la matricula profesional y la fecha de cierre del presente proceso en las carreras profesionales exigidas. La experiencia específica corresponde al tiempo certificado en que el profesional ha desarrollado o ejecutado ciertas actividades exigidas.

NOTA 3: El oferente deberá diligenciar el FORMATO EXPERIENCIA DEL PERSONAL PROPUESTO Y MODELO DE CARTA DE COMPROMISO DEL PERSONAL PROPUESTO, adjunto al pliego de condiciones. (Se deberá diligenciar correctamente los formatos por cada profesional presentado)

NOTA 4: Tratándose de títulos obtenidos en el exterior, estos deberán estar debidamente homologados ante el Ministerio de Educación Nacional, de acuerdo con la reglamentación vigente. El proponente debe anexar copia de la respectiva resolución de validación de los estudios y títulos académicos expedida por el Ministerio de Educación Nacional.

NOTA 5: Una vez el Supervisor apruebe el personal mínimo, el proponente adjudicatario no podrá cambiarlo durante la ejecución del contrato, a menos que exista una justa causa, la cual deberá ser sustentada ante la Entidad, para su evaluación y posterior autorización, el personal deberá reemplazarse por uno que cumpla con los requisitos exigidos en el Pliego

NOTA 6: La experiencia específica debe entenderse la adquirida en ejercicio de las funciones propias de un empleo concreto o preciso, en el desempeño de actividades en una determinada área de trabajo o en el ejercicio profesional, o en el desempeño de una ocupación, arte u oficio, igual o similar al cargo, empleo o responsabilidad que se va a desempeñar.

NOTA 7: La entidad al realizar la exigencia de perfiles determinados ha establecido la importancia de la exigencia de criterios de altas capacidades técnicas particulares del personal. Los mismos, obedecen a un análisis técnico de cada uno de los ítems de la ficha técnica, al proceso de instalación y puesta en marcha del sistema y a la complejidad que pesa sobre la necesidad a satisfacer, dado que corresponde a un sistema que busca garantizar la protección de los sistemas de información bajo estándares internacionales, por lo anterior se consideran como mínimos requeridos para una correcta implementación del este proceso.

14.3.2.2. CERTIFICACION Y CONDICIONES MÍNIMAS DE CALIDAD

14.3.2.2.1 IDONEIDAD TECNICA Y CONDICIONES MÍNIMAS DE OPERACIÓN

El oferente deberá acreditar que cuenta con un **Centro de Operaciones de Seguridad (SOC)** propio ubicado y operando en Colombia, destinado a la gestión, monitoreo, prevención, detección y respuesta ante incidentes de ciberseguridad.

Para tal efecto, el proponente deberá aportar junto con la propuesta:

1. Certificación suscrita por el representante legal, bajo la gravedad de juramento, en la que manifieste que dispone de un SOC propio en Colombia, que este permanecerá operativo durante toda la ejecución del contrato y que dicho servicio cumpla con los controles establecidos en los estándares **SOC 2 TYPE II,** para lo cual deberá contar con la **Certificación SOC 2 Type II** vigente.
2. Así mismo, el oferente deberá acreditar la disponibilidad de un **Centro de Operaciones de Seguridad (SOC) alterno**, igualmente ubicado y en operación en Colombia, que garantice la continuidad operativa de los servicios ante contingencias, fallas, indisponibilidad o eventos que afecten la operación del SOC principal.
3. El oferente deberá acreditar, mediante documento vigente expedido por **FIRST (Forum of Incident Response and Security Teams)** o por la entidad competente para ello, que su **Centro de Operaciones de Seguridad (SOC) propio ubicado en Colombia** ostenta la calidad de **miembro activo de FIRST con una antigüedad mínima de 12 meses.**

La entidad verificará la vigencia y antigüedad de la membresía mediante los soportes aportados por el oferente o mediante validación en los registros oficiales de FIRST.

El oferente deberá garantizar la disponibilidad de servicios de atención, soporte especializado y respuesta ante incidentes de ciberseguridad durante la ejecución contractual, incluyendo capacidad de atención remota y en sitio conforme a los niveles de servicio establecidos en el presente proceso.

14.3.2.2.2 CERTIFICACIÓN DISTRIBUIDOR AUTORIZADO

El proponente deberá presentar certificación vigente que lo acredite como **distribuidor autorizado en Colombia,** en el **máximo nivel de membresía otorgado por el respectivo fabricante,** para el suministro, implementación, instalación, configuración y soporte de las tecnologías ofertadas, de conformidad con lo establecido en la ficha técnica.

1. Cuando la propuesta incluya soluciones de **más de un fabricante**, el proponente deberá allegar la certificación correspondiente de **cada uno de los fabricantes** con los cuales acreditará el cumplimiento de los requisitos técnicos del proceso. En consecuencia, deberá presentar las certificaciones que acrediten el nivel de membresía exigido para **cada una de las tecnologías ofertadas**, incluyendo, entre otras, soluciones de **SIEM, WAF, EDR/XDR, Gestión de Vulnerabilidades, Monitoreo de Marca (Digital Risk Protection), Protección de Correo Electrónico** y las demás tecnologías con las que se dará cumplimiento a las especificaciones técnicas establecidas en la ficha técnica.

2. Cada certificación deberá acreditar que el proponente cuenta con el **máximo nivel de membresía, partnership o especialización vigente** otorgado por el fabricante correspondiente, que lo habilite para el suministro, implementación, instalación, configuración, administración y soporte de la tecnología ofertada.

3. La certificación expedida por cada fabricante deberá indicar expresamente la **tecnología o solución que respalda**, así como el **ítem del requerimiento técnico descrito en la ficha técnica**, con el fin de garantizar la trazabilidad entre la certificación aportada y el cumplimiento de cada uno de los requisitos técnicos ofertados.

4. La certificación deberá estar dirigida a la entidad contratante, tener una fecha de expedición no superior a treinta (30) días calendario anteriores al cierre del plazo para la presentación de ofertas y tener el número del proceso.

Nota 1: No se aceptan soluciones open source, ni de código abierto.

14.3.2.2.3 CERTIFICACIÓN FICHA TECNICA:

El oferente en su propuesta deberá incluir ficha técnica contemplada en el numeral del Estudio previo, señalando marca, modelo, referencia y especificaciones técnicas de cada uno de los ítems.

- La ficha técnica deberá estar firmada por el representante Legal del proponente.

14.3.2.2.5 CAPACIDAD FINANCIERA

La capacidad financiera y organizacional a exigir guarda relación con el valor del contrato a celebrar, siendo esta adecuada y proporcional, teniendo como objetivo la consecución de un contratista que disponga de los recursos financieros suficientes para ejecutar el contrato dentro del plazo previsto. Con el fin de verificar la solidez financiera, el Proponente deberá cumplir con los indicadores financieros establecidos en este documento.

El certificado de Registro Único de Proponentes será plena prueba de las circunstancias que en ella se hagan constar y que hayan sido verificadas por las Cámaras de Comercio. En tal sentido, la verificación de las condiciones de capacidad jurídica y las condiciones de experiencia, capacidad financiera y de organización de los proponentes, se demostrará exclusivamente con el respectivo certificado del RUP en donde deberán constar dichas condiciones. En consecuencia, las entidades estatales en los procesos de contratación no podrán exigir, ni los proponentes aportar documentación que deba utilizarse para efectuar la inscripción en el registro. No obstante, lo anterior, sólo en aquellos casos en que por las características del objeto a contratar se requiera la verificación de requisitos del proponente adicionales a los contenidos en el RUP, la entidad podrá hacer tal verificación en forma directa.

Se evaluará con base en la información financiera contenida en el certificado de inscripción, calificación y clasificación, en el Registro Único de Proponentes (RUP), el cual deberá estar actualizado y con la información financiera. Con base en la información financiera 2024, el mismo deben estar en firme al cierre de la entrega de propuestas.

La entidad verificará toda la información financiera en moneda legal colombiana, de conformidad con los artículos 50 y 51 del Decreto número 2649 de 1993 y demás normas que lo modifiquen adicionen o sustituyan, así mismo deberán estar en idioma español.

PARA LAS PERSONAS NATURALES O JURÍDICAS NACIONALES Y EXTRANJERAS CON DOMICILIO O SUCURSAL EN COLOMBIA, La evaluación financiera y organizacional de las propuestas se efectuará a partir de la información contenida en el RUP vigente y en firme. En tal sentido, la evaluación de la capacidad financiera se realizará de acuerdo con la información reportada en el Registro, de acuerdo con las disposiciones establecidas en la Subsección 5, de la Sección 1, del Capítulo 1, del Título 1, de la Parte 2 del Decreto 1082 de 2015, o las normas que las modifiquen, adicionen o sustituyan, por lo que se tomará la información financiera del mejor año fiscal que se refleje en el registro del proponente y que esté vigente y en firme.

LOS PROPONENTES EXTRANJEROS SIN DOMICILIO O SUCURSAL EN COLOMBIA NO ESTÁN OBLIGADOS A TENER RUP Y POR TANTO LA VERIFICACIÓN DE ESTA INFORMACIÓN PROCEDERÁ EN LOS TÉRMINOS DEFINIDOS, Los Proponentes extranjeros deberán presentar la siguiente información financiera de conformidad con la legislación propia del país de origen. Los valores deben: (i) presentarse en pesos colombianos; (ii) convertirse a la tasa de cambio de la fecha de corte de los mismos, y (iii) estar avalados con la firma de quien se encuentre en obligación de hacerlo de acuerdo con la normativa del país de origen.

A. El estado de situación financiera (balance general) y estado de resultado integral (estado de resultados), acompañados por el informe de auditoría (sí aplica de acuerdo con la legislación de origen) con traducción simple al castellano de acuerdo con las normas NIIF. Los oferentes extranjeros deben presentar sus estados financieros a la fecha de corte establecida en los países de origen o en sus estatutos sociales.

B. Copia de la tarjeta profesional del Contador Público o Revisor Fiscal y certificado de antecedentes disciplinarios vigente expedido por la Junta Central de Contadores de quien realiza la conversión.

Los oferentes deben presentar sus estados financieros en la moneda legal del país en el cual fueron emitidos y adicionalmente en pesos colombianos. El proponente y la Entidad Estatal 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 Estatal tendrán en cuenta las tasas de cambio certificadas por la Superintendencia Financiera.

Para aquellas sociedades extranjeras cuyas prácticas contables difieran de lo establecido en las normas colombianas, se deberá aportar junto con la información financiera de la persona jurídica extranjera, certificación suscrita por el contador público o revisor fiscal de la sociedad extranjera o en su defecto el revisor fiscal de la sucursal en Colombia, en la que se indiquen los rubros que correspondan a las cuentas, que se entenderá prestada bajo la gravedad del juramento.

El Proponente tiene que alcanzar todos los indicadores financieros requeridos para su propuesta sea considerada hábil.

Los estados financieros deben reflejar la situación financiera del Proponente individual, o de los integrantes del Proponente, y no de una sociedad matriz u otra perteneciente al mismo grupo Empresarial.

En atención a la naturaleza del contrato a suscribir y de su valor, el Departamento hace uso de los siguientes indicadores, los cuales considera adecuados respecto al objeto del Proceso de Contratación.

CAPACIDAD FINANCIERA

ÍNDICE DE LIQUIDEZ

Indica cual es la capacidad del proponente para cancelar sus deudas a corto plazo comprometiendo sus activos corrientes, es decir, por cada peso de deuda corriente establece cuanto se tiene de respaldo en activo corriente; entre más alto sea el índice, menor es el riesgo de que exista incumplimiento de las deudas a corto plazo.

Los activos corrientes normalmente incluyen caja, títulos valores de corto plazo, cuentas por cobrar e inventarios. Los pasivos corrientes normalmente incluyen las cuentas por pagar, deuda de corto plazo y gastos acumulados.

El Departamento de Santander realizó el análisis del sector y determinó como Índice de Liquidez que **debe ser mayor o igual a 1,3**

.

FORMULA: $$Indice\ de\ Liquidez\ (IL) = \frac{Activo\ Corriente}{Pasivo\ Corriente}$$

Para el caso de proponentes plurales se calculará el índice de liquidez, con base en la suma de los componentes del indicador, independientemente de la participación de los integrantes del oferente plural.

FORMULA: $$Indice\ de\ Liquidez\ (IL) = \frac{\sum_{i=1}^{n} Activo\ Corriente\ i}{\sum_{i=1}^{n} Pasivo\ Corriente\ i}$$

ÍNDICE DE ENDEUDAMIENTO (IE).

Este índice determina el grado de endeudamiento en la estructura de financiación (pasivos y patrimonio) del proponente. A mayor índice de endeudamiento, mayor es la probabilidad del proponente de no poder cumplir con sus pasivos.

El Departamento de Santander realizó el análisis del sector y determinó como Índice de Endeudamiento que **debe ser menor o igual a 0,65**

FORMULA : $$Indice\ de\ Endeudamiento\ (IE) = \frac{Pasivo\ Total}{Activo\ Total}$$

Para el caso de proponentes plurales se calculará el índice de endeudamiento con base en la suma de los componentes del indicador, independientemente de la participación de los integrantes del oferente plural.

FORMULA : $$Indice\ de\ Endeudamiento\ (IE) = \frac{\sum_{i=1}^{n} Pasivo\ Total\ i}{\sum_{i=1}^{n} Activo\ Total\ i}$$

RAZON DE COBERTURA DE INTERESES (RCI).

Este indicador refleja la capacidad del proponente de cumplir con sus obligaciones financieras. A mayor cobertura de intereses, menor es la probabilidad de que el proponente incumpla sus obligaciones financieras. Es el resultado de la utilidad operacional dividida por los gastos de intereses. Es fundamental para un oferente estar al día con sus obligaciones financieras, particularmente con la obligación de pagar intereses financieros. Una compañía puede encontrarse en dificultades financieras y operacionales y mantener el giro ordinario de sus negocios por un buen tiempo en la medida en que sea capaz de pagar sus intereses de deuda.
Es un nuevo Indicador de capacidad financiera según el decreto 1082 de 2015, la muestra para este indicador y para su cálculo se toma información financiera de la base de datos de la superintendencia de sociedades del Sector de Telecomunicaciones.

El Departamento de Santander realizó el análisis del sector y determinó como Razón de Cobertura de intereses que **debe ser mayor o igual a 2,0**

Las compañías que no tienen gastos de interés y cuya utilidad operacional es positiva cumplen con el indicador de razón de cobertura de intereses.

FORMULA: $$Razv = n\ de\ Cobertura\ de\ Intereses\ (RCI) = \frac{Utilidad\ Operacional}{Gastos\ de\ intereses}$$

Para el caso de proponentes plurales, se calculará la razón de cobertura de intereses con base en la suma de los componentes del indicador, independientemente de la participación de los integrantes del oferente plural.

FORMULA:

$$Razon\ de\ Cobertura\ de\ Intereses\ (RCI) = \frac{\sum_{i=1}^{n} Utilidad\ Operacional\ i}{\sum_{i=1}^{n} Gastos\ de\ Interés\ i}$$

Para el evento de encontrarse el proponente o integrante de la modalidad de asociación con gastos de intereses cero (0), el indicador de la razón de cobertura de intereses será considerado con un valor absoluto igual a 10 (diez). Cuando el cálculo por proponente o integrante sea superior a diez (10), la entidad otorgará un indicador máximo de diez (10).

Las personas naturales y las personas jurídicas en calidad de proponentes o integrantes de un proponente plural, no podrán tener utilidad operacional negativa, caso el cual definirá al proponente como no cumple con el indicador de razón de cobertura de intereses.

PATRIMONIO (P)

Teniendo en cuenta que las Entidades Estatales pueden establecer indicadores adicionales a los establecidos en el numeral 3 del artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015 con ocasión de la naturaleza o complejidad del Proceso de Contratación, El Departamento de Santander ha determinado usar este indicador financiero porque se requiere analizar la cantidad de recursos propios en términos absolutos.

Determina el valor residual de los activos del proponente después de deducir todos sus pasivos. Es el conjunto de bienes, derechos y obligaciones que constituyen los medios económicos y financieros a través de los cuales el Oferente puede cumplir sus fines.

Patrimonio = Activo Total – Pasivo Total

Se considerará hábil el proponente que presente un (P) mayor o igual (≥) al **50 % del Presupuesto Oficial, es decir, mayor o igual a $3.434.924.002**.

Para el caso de proponentes plurales, se calculará el patrimonio con base en la sumatoria del patrimonio de cada uno de los miembros del proponente plural, sin importar el porcentaje de participación.

CAPACIDAD ORGANIZACIONAL

La capacidad que tiene una organización para entregar bienes y servicios está relacionada con una combinación de mediciones que involucra el margen de ganancia, la eficiencia en el manejo de sus activos, y el riesgo de su operación. De acuerdo con lo establecido en el Estudio de Mercado, la Entidad cuenta con información de posibles Oferentes quienes pertenecen a subsectores diferentes de la industria de la construcción, por lo cual sus resultados financieros no se comportan de una manera uniforme y muestran desviaciones estadísticas muy altas.

Los siguientes indicadores miden el rendimiento de las inversiones y la eficiencia en el uso de activos del interesado:

RENTABILIDAD DEL PATRIMONIO

Determina la rentabilidad del patrimonio del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el patrimonio. A mayor rentabilidad sobre el patrimonio, mayor es la rentabilidad de los accionistas y mejor la capacidad organizacional del proponente.

Este indicador es el resultado de dividir la utilidad operacional sobre el Total Patrimonio, el cual expresa qué porciento representa la utilidad neta del valor del financiamiento de capital, o, cuantos pesos de utilidad neta genera la empresa por cada peso de financiamiento, está razón mide el rendimiento sobre la inversión, por lo tanto, muestra qué tan eficientemente usa su Patrimonio para generar ganancias.

Es un nuevo Indicador de capacidad organizacional según el Decreto 1082 de 2015, la muestra para este indicador y para su cálculo, se basa en la información financiera de la base de datos de la Superintendencia de Sociedades del Sector de la Telecomunicaciones.

El Departamento de Santander establece que para el presente proceso el oferente debe mostrar eficiencia con un resultado mínimo positivo de la utilidad operacional sobre el Patrimonio.

El Departamento de Santander realizó el análisis del sector y determinó que la Rentabilidad del Patrimonio **debe ser mayor o igual a 0,10**

FORMULA: $$\boldsymbol{Rentabilidad\ del\ Patrimonio\ (RP) = \frac{Utilidad\ Operacional}{Patrimonio}}$$

Para el caso de proponentes plurales, se calculará la rentabilidad del patrimonio con base en la suma de los componentes del indicador, independientemente de la participación de los integrantes del oferente plural.

FORMULA:

$$\boldsymbol{Rentabilidad\ del\ Patrimonio\ (RP) = \frac{\sum_{i=1}^{n} Utilidad\ operacional\ i}{\sum_{i=1}^{n} Patrimonio\ i}}$$

RENTABILIDAD DEL ACTIVO

Determina la rentabilidad de los activos del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el activo. A mayor rentabilidad sobre activos, mayor es la rentabilidad del negocio y mejor la capacidad organizacional del proponente. Este indicador debe ser siempre menor o igual que el de rentabilidad sobre patrimonio.

Este indicador es el resultado de dividir la utilidad operacional sobre el Total Activo y mide la eficiencia en el uso de los Activos de una empresa para establecer la efectividad total de la administración y producir utilidades sobre los Activos Totales disponibles.

Es un nuevo Indicador de capacidad organizacional según el Decreto 1082 de 2015, la muestra para este indicador y para su cálculo, se toma información financiera de la base de datos de la superintendencia de sociedades del Sector de Telecomunicaciones.

La Entidad considera que el Oferente muestra su eficiencia al tener un resultado positivo de la utilidad operacional sobre el activo.

El Departamento de Santander realizó el análisis del sector y determinó que la Rentabilidad del Activo **debe ser mayor o igual a 0,05 como indicador mínimo**

FORMULA: $$Rentabilidad\ del\ Activo\ (RA) = \frac{Utilidad\ Operacional}{Activo}$$

Para el caso de proponentes plurales, se calculará la rentabilidad del activo con base en la suma de los componentes del indicador, independientemente de la participación de los integrantes del oferente plural.

FORMULA: $$Rentabilidad\ del\ Activo\ (RA) = \frac{\sum_{i=1}^{n} Utilidad\ Operacional\ i}{\sum_{i=1}^{n} Activo\ Total\ i}$$

16. EVALUACION DE LA OFERTA

La Entidad Contratante evaluará las ofertas de los Proponentes que hayan acreditado los requisitos habilitantes establecidos en este pliego de condiciones.

En la evaluación de las ofertas, el Departamento de Santander, realizará ponderación del factor económico,del factor técnico y del incentivo a la industria nacional, de acuerdo con los porcentajes que se indican en elsiguiente cuadro:

Puntaje por criterios de evaluación		
Criterio de evaluación	**Detalle**	**Puntaje máximo**
Factor económico	Precio	10
Factor técnico	Condiciones técnicas	78.5
Incentivo a la industria nacional	Ley 816 de 2003	10
Personal en condición de discapacidad		1
Incentivo empresa de emprendimiento mujeres		0.25
Incentivo MiPymes		0.25
	Total	**100**

De acuerdo con el puntaje obtenido por cada uno de los proponentes, se establecerá un orden de elegibilidad de mayor a menor puntaje, para la adjudicación del contrato.

En caso de empate en el puntaje total de dos o más Ofertas, el Departamento de Santander escogerá el proponente aplicando los criterios de desempate previstos en el artículo 2.2.1.1.2.2.9 del Decreto 1082 de 2015. Se tiene como primer factor de desempate al oferente con mayor puntaje por factor técnico

16.1 FACTOR ECONOMICO (PUNTAJE MAXIMO 10 PUNTOS)

El Departamento de Santander, a partir del valor total corregido de la propuesta asignará un puntaje máximo de (10) puntos acumulables de acuerdo con el método escogido en forma aleatoria para la ponderación del factor económico.

Para la asignación de puntaje se define el METODO DE LA TRM. Este es un método que utiliza fórmulas para la asignación de puntaje de acuerdo al valor total corregido de la oferta de cada proponente.

Los valores corregidos de las propuestas económicas, para efecto del método TRM, se consideran datos o variables cuantitativos dispersos que se pueden sintetizar con la utilización de parámetros estadísticos.

La media aritmética y la media geométrica son parámetros estadísticos de centralización o medidas de tendencia central que nos indican en torno a qué valor (centro) se distribuyen los datos, pero son muy sensibles a valores extremos y por ende poco representativas de la distribución.

La entidad realizó un análisis de precios del mercado serio que respalda el valor estimado por la misma (presupuesto oficial) para la ejecución del objeto del presente proceso de selección, soportado principalmente por los análisis de precios unitarios y es por esto que la entidad identifica y considera los valores que se encuentren dentro de un rango o recorrido del dos por ciento (2%) del presupuesto oficial como valores representativos de la distribución. Efectuada por la Entidad la respectiva corrección aritmética, y en el evento en que dicha corrección aritmética arroje en valor absoluto una diferencia entre el valor ofertado y el valor corregido superior al dos por ciento (2%) del valor de la propuesta económica presentada, estas propuestas no se incluirán en la aplicación del método de la TRM y se les asignará un puntaje único y fijo de tres (03) puntos por factor económico, esto a efectos de que los posibles interesados en presentar oferta, tengan la mayor diligencia y cuidado en su elaboración, para que las propuestas económicas presentadas sean producto de un debido estudio técnico detallado de todas y cada una de las actividades requeridas por la entidad, necesarias para la ejecución del proyecto.

De acuerdo a lo anterior, para la asignación de puntaje por la propuesta económica y considerando ponderar los valores representativos de la distribución, se tendrá en cuenta los siguientes casos:

CASO No.	DESCRIPCION	PROCEDIMIENTO
1	Propuestas económicas que presenten en valor absoluto una diferencia entre el valor ofertado y el valor corregido, superior al dos por ciento (2%) del valor de la propuesta presentada.	Se les asignará 3 puntos
2	Propuestas económicas que presenten en valor absoluto una diferencia entre el valor ofertado y el valor corregido, menor o igual al dos por ciento (2%) del valor de la propuesta presentada.	Se les asignará el puntaje de acuerdo al METODO DE LA TRM

METODO DE LA TRM

Para la selección del método a utilizar se tendrá en cuenta los decimales (décima y centésima) de la Tasa Representativa del Mercado del dólar (TRM) calculada por la Superintendencia Financiera de Colombia, correspondiente al día de la publicación del informe de evaluación, de acuerdo al siguiente cuadro:

RANGO SEGÚN TRM	MÉTODO A UTILIZAR
DE 0.00 A 0.33	**a. MEDIA ARITMÉTICA**
DE 0.34 A 0.66	**b. MEDIA ARITMÉTICA ALTA**
DE 0.67 A 0.99	**c. MEDIA GEOMÉTRICA CON PRESUPUESTO OFICIAL**

a. MÉTODO DE LA MEDIA ARITMETICA

MÉTODO DE LA MEDIA ARITMETICA

Consiste en la determinación del promedio aritmético de los valores totales corregidos de las propuestas que no han sido rechazadas y se encuentran validas, incluyendo en el cálculo un número determinado de veces el noventa y ocho por ciento (98%) del presupuesto oficial.

Para el cálculo de la media aritmética ($\bar{x}$) se tendrá en cuenta el número de propuestas válidas y se incluirá el 98% del presupuesto oficial del Proceso de Contratación en el cálculo tantas veces como se indica en el siguiente cuadro:

Cantidad de Ofertas (n)	Número de veces que se incluye el 98% del presupuesto oficial (nv)
1 – 3	1
4 – 6	2
7 – 9	3
10 – 12	4
13 – 15	5
…	

Y así sucesivamente, por cada tres propuestas válidas se incluirá una vez el 98% del presupuesto oficial del presente proceso de Contratación.

Posteriormente, se determinará $\bar{x}$, mediante la siguiente fórmula:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i + (n_v \times 98\% PO)}{n + n_v}$$

$\bar{x}$ = Media aritmética
x_i = Valor total corregido de la propuesta i
n = Número total de las propuestas válidas presentadas
nv= Número de veces que se incluye el 98% del presupuesto oficial (PO)
98% PO= El 98% del Presupuesto oficial del proceso de contratación.

Ponderación de las propuestas por el método de la media aritmética.

Obtenida la media aritmética se procederá a ponderar las propuestas de acuerdo con la siguiente fórmula:

$$puntaje\ i = \begin{cases} 19{,}50\ x\left(1 - \left(\frac{|\bar{x} - v_i|}{\bar{x}}\right)\right) para\ valores\ mayores\ a\ \bar{x} \\ 19{,}50\ x\left(1 - 2\left(\frac{|\bar{x} - v_i\ |}{\bar{x}}\right)\right) para\ valores\ menores\ o\ iguales\ a\ \bar{x} \end{cases}$$

Donde,

$\bar{x}$ = Media aritmética
v_i= Valor total corregido de cada una de las propuestas i
i=Numero de propuesta

Para la ponderación de las propuestas económicas se tomará el valor absoluto de la diferencia entre la media aritmética y el valor total corregido de la propuesta, como se observa en la fórmula de ponderación.

MÉTODO DE LA MEDIA ARITMÉTICA ALTA.

Consiste en la determinación de la media aritmética entre el valor total corregido de la propuesta valida más alta y el promedio aritmético de las propuestas que no han sido rechazadas y se encuentran validas, incluyendo en este último calculo un número determinado de veces el presupuesto oficial, para esto se aplicaran las siguientes fórmulas:

$$x_{A} = \frac{V\max + \bar{y}}{2}$$

Donde,

X_A= Media aritmética alta
$Vmax$= Valor total corregido de la propuesta más alta
$\bar{y}$ = Promedio aritmético de las propuestas válidas incluyendo el presupuesto oficial

Cálculo de $\bar{y}$

Para el cálculo de $\bar{y}$ se tendrá en cuenta el número de propuestas válidas y se incluirá el presupuesto oficial del Proceso de Contratación en el cálculo tantas veces como se indica en el siguiente cuadro:

Cantidad de Ofertas (n)	Número de veces que se incluye el presupuesto oficial (nv)
1 – 3	1
4 – 6	2
7 – 9	3
10 – 12	4
13 – 15	5
….	

Y así sucesivamente, por cada tres propuestas válidas se incluirá una vez el presupuesto oficial del presente proceso de Contratación.

Posteriormente, se determinará $\bar{y}$, mediante la siguiente fórmula:

$$\bar{y} = \frac{\sum_{i=i}^{n} x_i + (n_v \times PO)}{n + n_v}$$

Donde,

$\bar{y}$ = Promedio aritmético de las propuestas válidas incluyendo el presupuesto oficial
x_i = Valor total corregido de la propuesta i
nv= Número de veces que se incluye el presupuesto oficial (PO)
n= Número de propuestas validas
PO= Presupuesto oficial del proceso de contratación.

Ponderación de las propuestas por el método de la media aritmética alta.

Obtenida la media aritmética alta se procederá a ponderar las propuestas de acuerdo con la siguiente fórmula:

$$puntaje\ i = \begin{cases} 19{,}50x\left(1 - \left(\frac{|X_{A-V_i}|}{X_A}\right)\right) para\ valores\ mayores\ a\ X_A \\ 19{,}50x\left(1 - 2\left(\frac{|X_{A-V_i}|}{X_A}\right)\right) para\ valores\ menores\ o\ iguales\ a\ X_A \end{cases}$$

Donde,

X_A= Media aritmética alta
v_i= Valor total corregido de cada una de las propuestas i
i=Numero de propuesta

Para la ponderación de las propuestas económicas se tomará el valor absoluto de la diferencia entre la media aritmética alta y el valor total corregido de la propuesta, como se observa en la fórmula de ponderación.

MÉTODO DE LA MEDIA GEOMETRICA CON PRESUPUESTO OFICIAL

Consiste en establecer la media geométrica de las propuestas válidas y el presupuesto oficial un número determinado de veces y la asignación de puntos en función de la proximidad de las propuestas a dicha media geométrica, como resultado de aplicar las fórmulas que se indican en seguida.

Para el cálculo de la media geométrica con presupuesto oficial se tendrá en cuenta el número de propuestas válidas y se incluirá el presupuesto oficial del Proceso de Contratación en el cálculo tantas veces como se indica en el siguiente cuadro:

Cantidad de Ofertas (n)	Número de veces que se incluye el presupuesto oficial (nv)
1 – 3	1
4 – 6	2
7 – 9	3
10 – 12	4
13 – 15	5
….	

Y así sucesivamente, por cada tres propuestas válidas se incluirá una vez el presupuesto oficial del presente proceso de Contratación.

Posteriormente, se determinará la media geométrica con la inclusión del presupuesto oficial de acuerdo a lo establecido en el cuadro anterior, mediante la siguiente fórmula:

$$G_{PO=}\ \sqrt[nv+n]{PO \text{ x } PO \text{ x } \dots \text{ x } PO_{nv} \text{ x } P_1 \text{ x} P_2 \text{ x } \dots \text{x } P_n}$$

Donde,

G_{po}= Media geométrica con prepuesto oficial.
nv= Número de veces que se incluye el presupuesto oficial (PO)
n= Número de propuestas validas
PO= Presupuesto oficial del proceso de contratación.
P_i = Valor de la propuesta económica corregida del proponente i

Ponderación de las propuestas por el método de la media geométrica con presupuesto oficial.

Obtenida la media geométrica con presupuesto oficial se procederá a ponderar las propuestas de acuerdo con la siguiente fórmula:

$$Puntaje\ i = \begin{cases} 19{,}50\ x\left(1-\left(\dfrac{|G_{PO}-V_i|}{G_{PO}}\right)\right) para\ valores\ mayores\ \ a\ G_{PO} \\ 19{,}50\ x\left(1-2\left(\dfrac{|G_{PO}-V_i|}{G_{PO}}\right)\right) para\ valores\ menores\ o\ iguales\ a\ G_{PO} \end{cases}$$

Donde,

G_{PO}= Media geométrica con presupuesto oficial
v_i= Valor total corregido de cada una de las propuestas i
i=Numero de propuesta

Para la ponderación de las propuestas económicas se tomará el valor absoluto de la diferencia entre la media geométrica con presupuesto oficial y el valor total corregido de la propuesta, como se observa en la fórmula de ponderación.

APROXIMACIÓN NUMÉRICA PARA EL PUNTAJE POR VALOR DE LA PROPUESTA

En todos los casos anteriores se tendrá en cuenta hasta el séptimo (7°) decimal del valor obtenido como puntaje.

16.2 FACTOR TÉCNICO. (78.5 PUNTOS)

Teniendo en cuenta lo señalado en el numeral primero del artículo 32 de la ley 80 de 1993 y que el objeto a contratar consiste en "**PRESTACIÓN DE SERVICIO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, MONITOREO DE INCIDENTES DE SEGURIDAD Y ATENCIÓN CORRECTIVA A INCIDENTES DE LA GOBERNACIÓN DE SANTANDER, EN EL MARCO DEL PROYECTO DE IMPLEMENTACIÓN DE ACCIONES PARA EL ASEGURAMIENTO TECNOLÓGICO Y LA TRANSFORMACIÓN DIGITAL EN EL DEPARTAMENTO DE SANTANDER**".

El contrato resultado del presente proceso de selección es un contrato de PRESTACIÓN DE SERVICIOS.

Por ello, se estima conveniente solicitar unas condiciones técnicas con lo cual se busca que haya una mayor ventaja de calidad y de funcionamiento generando mayor eficiencia y rendimiento por parte del contratista en la ejecución del objeto contractual..

Con lo anterior se minimiza los riegos económicos y técnicos que se pueden presentar en la etapa contractual al contar con mayores rendimientos en la ejecución de las actividades más representativas del proyecto, lo cual permite al contratista garantizar una mayor calidad y eficiencia del servicio a prestar al Departamento de Santander.

16.2.1. Implementación: Hasta veinte (20) puntos.

Se otorgarán hasta veinte (20) puntos de acuerdo con el ofrecimiento que realice EL OFERENTE, con respecto a la implementación de las plataformas que se relaciona a continuación:

Implementador	Descripción	Puntaje
Oferente	El Oferente ejecutará directamente la implementación de la arquitectura SIEM y deberá contar con especializaciones tipo SASE comprobada mediante certificación de Fabricante.	10
Fabricante	El fabricante ejecutará directamente la implementación, integración, puesta en operación y optimización de toda la arquitectura SIEM comprobada mediante certificación de Fabricante que indique el cumplimiento.	20

16.2.2 CERTIFICACIONES INTERNACIONALES DEL SOC (MÁXIMO 20 PUNTOS)

Los oferentes deberán allegar como parte de la oferta técnica certificaciones internacionales vigentes y verificables, relacionadas con la operación y gestión de Centros de Operaciones de Seguridad (SOC), seguridad de la información, continuidad del negocio y gestión de servicios tecnológicos.

Serán válidas las siguientes certificaciones:

1. ISO/IEC 27001:2022 en procesos asociados a la operación SOC.
2. ISO 22301:2019 o superior. Gestión de Servicios de TI
3. ISO/IEC 27035-3:2020 o Superior
4. ISO/IEC 20000-1:2018 o Superior, aplicable a: Servicios de Consultoría en Ciberseguridad y Seguridad de la Información y/o Servicios SOC/NOC/CSIRT y/o Servicios gestionados de ciberseguridad y/o Ingeniería e infraestructura tecnológica especializada y/o Servicios de nube segura y continuidad tecnológica.
5. ISO/IEC 9001:2015 o Superior, aplicable a: comercialización, implementación, soporte y administración de soluciones de ciberseguridad, infraestructura tecnológica, hiperconvergencia, conectividad y redes; prestación de servicios de SOC/NOC, mesa de servicios, consultoría especializada, ethical hacking y gestión de sistemas de información; así como la operación, monitoreo, detección, análisis, reporte y gestión de incidentes y eventos de ciberseguridad.

6. ISO/IEC 45001:2018 aplicable a seguridad de la informacion: centro de operacion SOC, Supervision y administracion de seguridad de la informacion, reporte, deteccion de analisis y gestion de incidentes y eventos de Ciberseguridad.

Certificación	Descripción	Puntaje
Acredita entre una (1) y tres (3) certificaciones válidas	Acredita la posesión de entre una (1) y tres (3) certificaciones válidas y vigentes, mediante documentos expedidos por el organismo certificador competente, que demuestren el cumplimiento de estándares internacionales de calidad, seguridad de la información o gestión de servicios de TI, según los requisitos establecidos.	5
Acredita entre cuatro (4) y cinco (5) certificaciones válidas	Acredita la posesión de entre cuatro (4) y cinco (5) certificaciones válidas y vigentes, mediante documentos expedidos por el organismo certificador competente, que demuestren el cumplimiento de estándares internacionales de calidad, seguridad de la información o gestión de servicios de TI, según los requisitos establecidos.	10
Acredita la totalidad de las certificaciones válidas - Seis (6)	Acredita la posesión de seis (6) certificaciones válidas y vigentes, mediante documentos expedidos por el organismo certificador competente, que demuestren el cumplimiento de estándares internacionales de calidad, seguridad de la información o gestión de servicios de TI, según los requisitos establecidos.	20

NOTA 1: Para la validación de este criterio el oferente deberá aportar copia de las certificaciones vigentes expedidas por organismo acreditado.

16.2.3 MEMBRESÍA FIRST DEL SOC (MÁXIMO 8,5 PUNTOS)

Se otorgará puntaje adicional al oferente que acredite que su SOC propio en Colombia es miembro activo de FIRST (Forum of Incident Response and Security Teams), Lo anterior permite evidenciar capacidades avanzadas de coordinación internacional, intercambio de inteligencia de amenazas y madurez operativa en atención de incidentes de ciberseguridad.

Criterio	Puntaje
Membresía FIRST con antigüedad entre doce (12) y treinta y seis (36) meses.	5
Membresía FIRST con antigüedad superior a cuarenta y ocho (48) meses.	8,5

16.2.4 PRUEBA DE VULNERABILIDAD Y TRANSFERENCIA DE CONOCIMIENTO (MÁXIMO 20 PUNTOS)

A. **Profesional Prueba de Vulnerabilidad:** Se otorgará puntaje adicional al oferente que suministre, sin costo adicional para la Entidad, una prueba de vulnerabilidades sobre cinco (5) aplicaciones productivas definidas por el Departamento de Santander. La actividad deberá realizarse durante la etapa de puesta en marcha de los equipos, plataformas o servicios suministrados e instalados en ejecución del contrato.

La prueba deberá incluir como mínimo:

- Identificación de vulnerabilidades.
- Validación técnica de hallazgos.
- Clasificación de riesgos.
- Recomendaciones básicas de mitigación.
- Entrega de informe técnico ejecutivo y detallado.

La ejecución de la prueba deberá estar coordinada y avalada por un profesional que cumpla con el siguiente perfil:

Perfil Profesional Requerido

- Título profesional correspondiente al Núcleo Básico del Conocimiento (NBC) en Ingeniería Electrónica, Telecomunicaciones o Afines; Ingeniería de Sistemas, Telemática y Afines; o con título profesional de Licenciatura en Electrónica, Licenciatura en Sistemas o programas afines.
- Postgrado en Seguridad de la Información y/o Seguridad Informática y/o seguridad de las tecnologías de la información y de las comunicaciones.
- Experiencia profesional mínima de siete (7) años en seguridad informática y/o análisis de vulnerabilidades y/o ethical hacking o ciberseguridad.

El profesional deberá acreditar mínimo cinco (5) de las siguientes certificaciones vigentes:

- ISO 27001:2022 Lead Auditor.
- Ethical Hacking Professional Certificación (CEHPC).
- ISO 27035: 2024 Gestión de incidentes de seguridad de la información
- ISO 27032:2012 o Superior Cybersecurity Manager.
- Certificacion Scrum Master Professional.
- Certificacion Digital Forensics Essiantials

Certificación	Descripción	Puntaje
A - Prueba de Vulnerabilidad	El oferente acredita parcialmente el ofrecimiento adicional del Item **(A)** y cumple con el **Perfil Profesional Requerido**	10

B. Transferencia de Conocimiento

Como parte del ofrecimiento adicional, el profesional propuesto deberá realizar sin costo para la Entidad mínimo dos (2) capacitaciones durante la ejecución del contrato, orientadas al fortalecimiento de capacidades institucionales en defensa de redes y ciberseguridad.

Las capacitaciones deberán estar alineadas con buenas prácticas y fundamentos asociados a la certificación EC-Council Network Defense Essentials (NDE), abordando como mínimo los siguientes temas:

- Seguridad de redes.
- Control de acceso e identificación.
- Monitoreo y análisis de tráfico.
- Herramientas de defensa (IDS/IPS, SIEM, Firewall, VPN y antimalware).
- Seguridad inalámbrica, móvil e IoT.
- Criptografía y protección de datos.

NOTA1: Las jornadas deberán incluir componentes teóricos y prácticos orientados a fortalecer las capacidades técnicas del personal de la Entidad y seran dictadas de manera presencial o virtual de acuerdo a solicitud de la entidad con previa coordinacion.

Para la validación del presente criterio, el oferente deberá aportar:

- El curso debera ser dictado por el profesional propuesto

- Certificación suscrita por el representante legal en la que se comprometa a realizar la prueba de vulnerabilidades y las capacitaciones sin costo adicional para la Entidad.
- Hoja de vida del profesional propuesto.
- Copias de títulos académicos y certificaciones exigidas.
- Carta de compromiso y aceptación del profesional para participar en la ejecución contractual.
- Comprobante de vinculacion directa con el oferente por medio de certificado de parafiscales de los ultimos 6 meses.

Certificación	Descripción	Puntaje
A - Prueba de Vulnerabilidad **B - Transferencia de Conocimiento**	El oferente acredita totalmente el ofrecimiento adicional Item (A) Y (B) Y cumple con el **Perfil Profesional Requerido**	20

NOTA 1. Asignación del puntaje. El puntaje se otorgará exclusivamente en dos modalidades: diez (10) puntos cuando el oferente acredite parcialmente el ofrecimiento correspondiente al componente A y cumpla con el perfil profesional requerido, o veinte (20) puntos cuando acredite integralmente los componentes A y B y cumpla con dicho perfil, conforme a los requisitos y documentos establecidos en el presente numeral.

NOTA 2. Verificación de requisitos. La asignación del puntaje estará sujeta a la revisión y verificación del cumplimiento de las condiciones técnicas, académicas, de experiencia, certificaciones y documentos exigidos para cada modalidad. La falta de acreditación de los requisitos correspondientes impedirá la asignación del puntaje respectivo.

NOTA 3. No acumulación de puntajes. Los puntajes de diez (10) y veinte (20) puntos son excluyentes y no acumulables. En consecuencia, el oferente recibirá únicamente el puntaje que corresponda al nivel de cumplimiento debidamente acreditado, hasta un máximo de veinte (20) puntos.

NOTA 4. Obligaciones sin costo adicional. Las actividades ofrecidas de prueba de vulnerabilidades y transferencia de conocimiento deberán ejecutarse sin costo adicional para la Entidad, de acuerdo con las condiciones establecidas en el presente numeral y con el compromiso suscrito por el representante legal del oferente.

16.2.5 SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD SIN COSTO ADICIONAL (MÁXIMO 10 PUNTOS)

Se otorgará puntaje al oferente que suministre al Departamento de Santander servicios especializados adicionales de ciberseguridad sin costo adicional durante la ejecución contractual.

Perfil Profesional Requerido

- Título profesional en Ingeniería de Sistemas, Telemática y Afines. Ingeniero Eléctrico, Electrónico, Sistemas, Telecomunicaciones y/o carreras afines.
- Postgrado en Seguridad de la Información y/o Seguridad Informática y/o Postgrado en Ciberseguridad y Privacidad.
- Experiencia profesional mínima de cinco (5) años en Casos de Uso Personalizados SIEM, Servicio de Análisis de Sentimiento, enfocada en la gestión de riesgos digitales, la identificación de amenazas externas, la detección de exposición de información y la protección de la marca en entornos digitales.

El profesional deberá acreditar mínimo tres (3) de las siguientes certificaciones vigentes:

- Certificación Ethical Hacking Professional (CEHPC).
- Certificación Ethical Hacking y Penetration Tester CEHPT.
- Certificación en análisis, interpretación y normalización de registros para plataformas SIEM expedida directamente por fabricante (Vigente).
- Certificación Profesional en Operaciones de Ciberseguridad y Gestión de Riesgos Digitales expedida directamente por fabricante (Vigente).

A. Cacería de Amenazas – Threat Hunting

El servicio deberá prestarse bajo un enfoque estructurado basado en estándares internacionales y orientado a la identificación proactiva de amenazas.

El ejercicio incluirá:

- Análisis histórico de eventos SIEM.
- Revisión de logs hasta por dos (2) meses.
- Construcción de hipótesis de amenaza.
- Correlación de eventos.
- Identificación de comportamientos anómalos.
- Informe ejecutivo y técnico de hallazgos y recomendaciones.

Certificación	Descripción	Puntaje
A - Cacería de Amenazas Threat Hunting	El oferente acredita parcialmente el ofrecimiento adicional del Item **(A)** mediante certificacion firmada por el Rep Legal	5

B. Casos de Uso Personalizados SIEM

Creación bajo demanda de casos de uso personalizados para la plataforma SIEM orientados a detectar comportamientos anómalos y eventos de seguridad.

Los casos de uso deberán:

- Basarse en MITRE ATT&CK.
- Incluir parametrización inicial.
- Contemplar ajuste y afinamiento.

Certificación	Descripción	Puntaje
A - Cacería de Amenazas Threat Hunting **B - Casos de Uso Personalizados SIEM**	El oferente acredita Parcialmente el ofrecimiento adicional Item (A) Y (B) Y cumple con el **Perfil Profesional Requerido**	7

C. Servicio de Análisis de Sentimiento

Servicio de análisis de sentimiento durante Dos (2) meses sobre redes sociales y plataformas digitales.

El servicio deberá:

- Monitorear Reddit, YouTube y X.
- Clasificar opiniones positivas, negativas y neutras.
- Generar métricas, tableros y tendencias.

Certificación	Descripción	Puntaje
A - Cacería de Amenazas Threat Hunting **B - Casos de Uso Personalizados SIEM** **C - Servicio de Análisis de Sentimiento**	El oferente acredita totalmente el ofrecimiento adicional Item (A) Y (B) Y (C)	10

NOTA 1. Asignación del puntaje. Se otorgarán cinco (5) puntos por el ofrecimiento del servicio A – Cacería de Amenazas (Threat Hunting); siete (7) puntos por el ofrecimiento conjunto de los servicios A y B – Casos de Uso Personalizados SIEM; y diez (10) puntos por el ofrecimiento integral de los servicios A, B y C. La asignación estará sujeta al cumplimiento de las condiciones técnicas y documentales establecidas para cada servicio.

NOTA 2. Puntajes excluyentes. Los puntajes definidos corresponden a niveles de cumplimiento excluyentes y no acumulables. En consecuencia, se asignará únicamente el puntaje del nivel más alto debidamente acreditado, hasta un máximo de diez (10) puntos.

NOTA 3. Acreditación del perfil profesional. Para acceder al puntaje correspondiente, el oferente deberá acreditar el cumplimiento del perfil profesional exigido, incluyendo la formación académica, la experiencia específica y mínimo tres (3) de las certificaciones establecidas, las cuales deberán encontrarse vigentes cuando así se requiera en el presente numeral.

NOTA 4. Soportes y compromiso de ejecución. El oferente deberá presentar los documentos que acrediten el perfil profesional y las certificaciones exigidas, así como el compromiso suscrito por su representante legal de prestar los servicios ofrecidos sin costo adicional para la Entidad. La asignación del puntaje estará condicionada a la verificación de estos soportes y del cumplimiento técnico de cada servicio.

16.3 INCENTIVO A LA INDUSTRIA NACIONAL (10 PUNTOS)

El componente denominado Estimulo a la industria nacional tendrá una asignación máxima de puntaje equivalente a diez (10) puntos. Los cuales se asignarán de la manera como se expone en adelante. Esto se establece en seguimiento a lo estipulado en el artículo 2 de la Ley 816 de 2003 para apoyar la industria nacional, modificado parcialmente por el Decreto 680 de 2021, a través del sistema de compras y contratación pública en la evaluación de las ofertas.

PROMOCIÓN A LA INDUSTRIA NACIONAL – PROMOCIÓN DE BIENES Y SERVICIOS NACIONALES O CON TRATO NACIONAL

Se entiende por BIENES NACIONALES los bienes inscritos en el Registro de Productores de Bienes Nacionales – RPBN, que son aquellos totalmente obtenidos en el territorio colombiano, los bienes elaborados en el país con materiales nacionales; y los bienes que hayan sufrido una transformación sustancial en función de un porcentaje mínimo de Valor Agregado Nacional o un proceso productivo sustancial.

Se entiende por SERVICIOS NACIONALES aquellos prestados por personas natural colombiana o residente en Colombia; Personas Jurídicas constituidas en el país, se acreditará el origen nacional de la oferta de la siguiente manera:

✓ Persona Natural Colombiana, con la presentación de la cédula de ciudadanía del proponente en copia simple, la cual deberá ser aportada con su oferta.

✓ Persona Natural Extranjera Residente en Colombia, con la presentación de la visa correspondiente(http://www.cancilleria.gov.co/tramites_servicios/visas/categorias/neg ocios) que le permita la ejecución ejecutar el objeto contractual de conformidad con la Ley. La cual deberá ser aportada con la oferta en copia simple. • Persona Jurídica constituida en el país, se verificará con el Certificado de Cámara y Comercio que el domicilio de la persona jurídica este dentro del territorio nacional.

✓ Persona Jurídica Extranjera: De acuerdo al artículo 2.2.1.2.4.1.3. del Decreto 1082 de 2015, las personas jurídicas extranjeras recibirán trato nacional cuando se cumpla alguna de las siguientes tres condiciones, para lo cual se verificará por la Entidad en el orden que se relaciona y de manera excluyente:

Se dará trato nacional a: a. Los bienes y servicios de otros Estados con los cuales exista un Acuerdo Comercial aplicable al Proceso de Contratación; b. A los bienes y servicios respecto de los cuales exista trato nacional por reciprocidad (situación que se verificará de conformidad con lo establecido por el artículo 2.2.1.2.4.1.3. del Decreto 1082 de 2015) y, a los servicios de la Comunidad Andina de Naciones –CAN.

PROMOCIÓN A LA INDUSTRIA NACIONAL – PROMOCIÓN DE LA INCORPORACIÓN DE COMPONENTE NACIONAL EN BIENES Y SERVICIOS EXTRANJEROS Incorporación de componente colombiano en servicios extranjeros:

En el evento en que se presenten ofertas de origen extranjero sin derecho a trato nacional, que ofrezcan servicios profesionales, técnicos u operativos de origen colombiano se le otorgará puntaje como se establece a continuación:

✓ Cuando la propuesta válida oferte bienes o servicios extranjeros, se asignarán cincuenta (05) puntos, si incorpora componente colombiano de bienes y servicios profesionales, técnicos y operativos en un porcentaje mayor al 50% del total requerido.

✓ Cuando la propuesta válida oferte bienes o servicios extranjeros, e incorpora componente colombiano de bienes y servicios profesionales, técnicos y operativos en un porcentaje inferior al 50% del total requerido, se asignará cero (0) puntos por este criterio

✓ La no presentación de la certificación requerida para acreditar este requisito, se le asignará 0 puntos.

En los contratos que deban cumplirse en Colombia, el servicio es nacional cuando además de ser ofertado por una persona natural colombiana o por un residente en Colombia, por una persona jurídica constituida de conformidad con la legislación colombiana o por un proponente plural conformado por estos o por estos y un extranjero con trato nacional, (i) usa el o los bienes nacionales relevantes definidos por la Entidad Estatal para el desarrollo del objeto contractual (ii) vincula el porcentaje mínimo de personal colombiano, según corresponda.
Los puntajes para estimular a la industria nacional se relacionan en la siguiente tabla

CONCEPTO	PUNTAJE
PROMOCION DE SERVICIOS NACIONALES O CON TRATO NACIONAL	10
INCORPORACION DE COMPONENTE NACIONAL EN SERVICIOS EXTRANJEROS	5

Además de la incorporación del bien nacional relevante o la mano de obra nacional, tratándose de proponentes plurales, su composición deberá estar acorde con lo exigido por la noción de Servicios Nacionales prevista en el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015, de lo que dependerá la franja del puntaje aplicable en lo referente al apoyo de la industria nacional. A tales efectos en la siguiente tabla se indican las posibles composiciones de proponentes plurales, la regla de origen que les aplica en virtud de dicha conformación, así como la franja de puntaje correspondiente:

ITEM	COMPOSICIÓN DEL PROPONENTE PLURAL	REGLA DE ORIGEN APLICABLE	PUNTAJE APLICABLE
1	ÚNICAMENTE INTEGRANTES COLOMBIANOS	DECRETO 1082 DE 2015	PROMOCIÓN DE SERVICIOS NACIONALES O CON TRATO NACIONAL

2	COLOMBIANOS EN ASOCIO CON EXTRANJEROS CON TRATO NACIONAL	DECRETO 1082 DE 2015	PROMOCIÓN DE SERVICIOS NACIONALES O CON TRATO NACIONAL
3	ÚNICAMENTE EXTRANJEROS CON TRATO NACIONAL	LA REGLA DE ORIGEN DEL PAÍS CON EL QUE SE TENGA ACUERDO COMERCIAL O LA DEL DECRETO 1082 DE 2015. SI EL PROPONENTE PLURAL NO ESPECIFICA A CUÁL REGLA SE ACOGE, SE APLICARÁ LA DEL DECRETO 1082 DE 2015.	PROMOCIÓN DE SERVICIOS NACIONALES O CON TRATO NACIONAL
4	PROPONENTE PLURAL EN EL QUE AL MENOS UNO DE LOS INTEGRANTES ES EXTRANJERO SIN TRATO NACIONAL.	NO APLICA A REGLA DE ORIGEN DEL DECRETO 1082 DE 2015, NI LA DE LOS PAÍSES DE ORIGEN.	INCORPORACIÓN DE COMPONENTE NACIONAL EN SERVICIOS EXTRANJEROS

ACREDITACIÓN DEL PUNTAJE POR BIENES O SERVICIOS NACIONALES O CON TRATO NACIONAL

Para que el Proponente nacional obtenga el puntaje de bienes o servicios nacionales debe presentar, además del Formato Bienes o Servicios Nacionales el certificado de existencia y representación legal emitido por la cámara de comercio correspondiente a la ciudad en donde tenga su domicilio principal.

El Departamento de Santander otorgará el puntaje por bienes o servicios nacionales al Proponente Plural conformado por nacionales cuando cada uno de sus integrantes presente alguno de los documentos indi de cados en este numeral, según corresponda. A su vez, el representante del proponente Plural deberá diligenciar el «Formato – Bienes o Servicios Nacionales». Cuando uno o varios de sus integrantes no cumplan con las condiciones descritas, el Proponente Plural no obtendrá el puntaje.

16.4 PERSONAL EN CONDICION DE DISCAPACIDAD (1 PUNTO)

Conforme lo ordena el numeral 7 del artículo 13 de la Ley 1618 de 2013, el cual establece que el Gobierno Nacional debe implementar mediante Decreto reglamentario un sistema de preferencias aplicable a los procesos de adjudicación y celebración de contratos de organismos estatales para quienes vinculen laboralmente a personas con discapacidad debidamente certificadas, en un porcentaje mínimo del 10% de su planta de trabajadores, lo que se encuentra reglamentado por el Decreto 1082 de 2015 en el artículo 2.2.1.2.4.2.6 estableciendo un sistema de preferencias como factor de desempate, así como un puntaje mínimo, para los proponentes que acrediten por lo menos el 10% de su nómina personas con discapacidad en el respectivo proceso de contratación.

Que tal como el mencionado artículo 2.2.1.2.4.6 del Decreto 1082 de 2015 lo establece, la regla de calificación quedará de la siguiente manera:

En el presente proceso contractual con la finalidad de incentivar el sistema de preferencias a favor de las personas con discapacidad, se otorgarán el uno por ciento (1%) del total de los puntos establecidos en el pliego de condiciones, a los proponentes que acrediten la vinculación de trabajadores con discapacidad en su planta de personal, de acuerdo con los siguientes requisitos:

1. La persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda. certificará el número total de trabajadores vinculados a la planta de personal del proponente o sus integrantes a la fecha de cierre del proceso de selección.

2. Acreditar el número mínimo de personas con discapacidad en su planta de personal, de conformidad con lo señalado en el certificado expedido por el Ministerio de Trabajo, el cual deberá estar vigente a la fecha de cierre del proceso de selección.

Verificados los anteriores requisitos, se asignarán un (1) punto de la presente licitación, a quienes acrediten el número mínimo de trabajadores con discapacidad, señalados a continuación:

NUMERO TOTAL DE TRABAJADORES DE LA PLANTA DE PERSONAL DEL PROPONENTE	NUMERO MINIMO DE TRABAJADORES CON DISCAPACIDAD EXIGIDO	PUNTAJE
Entre 1 y 30	1	
Entre 31 y 100	2	

Entre 101 y 150	3	1 PUNTO
entre 151 y 200	4	
Mas de 200	5	

16.5 PUNTAJE ADICIONAL EN EL SISTEMA DE COMPRAS PÚBLICAS

a. PUNTAJE ADICIONAL PARA PROPONENTES CON EMPRENDIMIENTOS Y /O EMPRESAS DE MUJERES (PUNTAJE MÁXIMO 0,25 PUNTOS)

Conforme a lo estipulado en el Decreto 1860 de 2021, en los procesos de Licitación Pública, Selección Abreviada de menor y Concurso de Méritos, las entidades estatales otorgaran un puntaje adicional de hasta el (0,25%) del valor total de los puntos establecidos en los pliegos de condiciones o documentos equivalentes a los proponentes que acrediten alguno de los supuestos del Articulo 2.2.1.2.4.2.14.

CRITERIO	PUNTAJE
Quien aporte o acredite alguno de los supuestos del artículo 2.2.1.2.4.2.14 conforme a los señalado en el requisito anterior	0,25 puntos
Quien no lo acredite esté requisito conforme a lo solicitado	0 puntos
TOTAL	**0,25 puntos**

b. PUNTAJE ADICIONAL PARA CRITERIO DIFERENCIAL MIPYME (PUNTAJE MÁXIMO 0,25 PUNTOS)

Conforme el decreto 1860 de 2021 se le da aplicación a MIPYME La entidad asignará un puntaje máximo de hasta 0.25 puntos al proponente que acredite la calidad de MIPYME domiciliada en Colombia de conformidad con el tamaño empresarial previsto en el artículo 2.2.1.13.2.2. del decreto 1074 de 2015 o la norma que lo modifique, sustituya o complemente.
El puntaje se asignará en función del tamaño empresarial de acuerdo con la siguiente tabla:

CRITERIO	PUNTAJE
Microempresa	0,25 puntos
Pequeña empresa	0,20 puntos
Mediana empresa	0,15 puntos
TOTAL	**0,25 puntos**

Las Mipymes colombianas deben acreditar que tienen el tamaño empresarial establecido por la ley de la siguiente manera: 1. Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil. 2. Las personas jurídicas mediante certificación expedida por el representante legal y el contador o 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 complementen. 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. Tratándose de proponentes plurales este puntaje se otorgará si por lo menos uno de los integrantes acredita la calidad de MIPYME y tiene una participación igual o superior al 10% en el consorcio o unión temporal.

16.6 REDUCCIÓN DE PUNTOS

En aplicación del artículo 58 de la Ley 2195 de 2022, el Departamento de Santander durante el término de evaluación de las ofertas reducirá el dos por ciento (2%) del total de los puntos establecidos en el proceso a los proponentes que se les haya impuesto una o más multas o cláusulas penales durante el último año, contado a partir de la fecha prevista para la presentación de las ofertas, sin importar la cuantía y sin perjuicio de las demás consecuencias derivadas del incumplimiento. Esta reducción también afecta a los consorcios y uniones temporales si alguno de sus integrantes se encuentra en la situación

anterior. La reducción del puntaje no se aplicará en caso de que los actos administrativos que hayan impuesto las multas sean objeto de medios de control jurisdiccional a través de las acciones previstas en la Ley 1437 de 2011 o las normas que la modifiquen, adicionen o sustituyan.

En todo caso, no se descontará el puntaje en los términos previstos en el inciso anterior cuando el Proponente no oferte el factor de calidad, por lo que éste obtendrá cero (0) puntos en este criterio de evaluación. En esta circunstancia, la Entidad no podrá reducir el puntaje de la sumatoria obtenida en los demás factores de ponderación.

16.7 CRITERIOS DE DESEMPATE

Para los factores de desempate la Entidad tomará lo expuesto en el Art. 35 de la Ley 2069 de 2020, reglamentados mediante Decreto 1860 de 2021.

ARTÍCULO 2.2.1.2.4.2.17. Factores de desempate y acreditación. En caso de empate en el puntaje total de dos o más ofertas en los Procesos de Contratación realizados con cargo a recursos públicos, en los Procesos de Contratación realizados por las Entidades Estatales indistintamente de su régimen de contratación, así como los celebrados por los Procesos de Contratación de los patrimonios autónomos constituidos por Entidades Estatales, el contratante deberá utilizar las siguientes reglas de forma sucesiva y excluyente para seleccionar al oferente favorecido, respetando en todo caso las obligaciones contenidas en los Acuerdos Comerciales vigentes, especialmente en materia de trato nacional.

1. Preferir la oferta de bienes o servicios nacionales frente a la oferta de bienes o servicios extranjeros. Para acreditar este factor de desempate se tendrán en cuenta las definiciones de que trata el artículo 2.2.1.1.1.3.1., en concordancia con el artículo 2.2.1.2.4.2.9. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, que trata del puntaje para la promoción de la industria nacional en los Procesos de Contratación de servicios. Para estos efectos, incluso se aplicará el inciso tercero de la definición de Servicios Nacionales establecida en el artículo 2.2.1.1.1.3.1., citado anteriormente.

En este sentido, en los procesos en los que aplique el puntaje previsto en el inciso 1 del artículo 2 de la Ley 816 de 2003, el requisito se cumplirá en los mismos términos establecidos en los artículos indicados en el inciso anterior. Por tanto, este criterio de desempate se acreditará con los mismos documentos que se presenten para obtener dicho puntaje.

2. Preferir la propuesta de la mujer cabeza de familia. Su acreditación se realizará en los términos del parágrafo del artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008, o la norma que lo modifique, aclare, adicione o sustituya. Es decir, la condición de mujer cabeza de familia y la cesación de esta se otorgará desde el momento en que ocurra el respectivo evento y se declare ante un notario. En la declaración que se presente para acreditar la calidad de mujer cabeza de familia deberá verificarse que la misma dé cuenta del cumplimiento de los requisitos establecidos en el artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008.

Igualmente, se preferirá la propuesta de la mujer víctima de violencia intrafamiliar, la cual acreditará dicha condición de conformidad con el artículo 21 de la Ley 1257 de 2008, esto es, cuando se profiera una medida de protección expedida por la autoridad competente. En virtud del artículo 16 de la Ley 1257 de 2008, la medida de protección la debe impartir el comisario de familia del lugar donde ocurrieron los hechos y, a falta de este, del juez civil municipal o promiscuo municipal, o la autoridad indígena en los casos de violencia intrafamiliar en las comunidades de esta naturaleza.

En el caso de las personas jurídicas se preferirá a aquellas en las que participen mayoritariamente mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar, para lo cual el representante legal o el revisor fiscal, según corresponda, presentará un certificado, mediante el cual acredita, bajo la gravedad de juramento, que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar. Además, deberá acreditar la condición indicada de cada una de las mujeres que participen en la sociedad, aportando los documentos de cada una de ellas, de acuerdo con los dos incisos anteriores.

Finalmente, en el caso de los proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en los incisos anteriores de este numeral.

De acuerdo con el artículo 5 de la Ley 1581 de 2012, el titular de la información de estos datos sensibles, como es el caso de las mujeres víctimas de violencia intrafamiliar, deberá autorizar de manera previa y expresa el tratamiento de esta información, en los términos del literal a) del artículo 6 de la precitada Ley, como requisito para el otorgamiento del criterio de desempate.

3. Preferir la propuesta presentada por el proponente que acredite en las condiciones establecidas en la ley que por lo menos el diez por ciento (10%) de su nómina está en condición de discapacidad, de acuerdo con el artículo 24 de la Ley 361 de 1997, debidamente certificadas por la oficina del Ministerio del Trabajo de la respectiva zona, que hayan sido contratados con por lo menos un (1) año de anterioridad a la fecha de cierre del Proceso de Contratación o desde el momento de la constitución de la persona jurídica cuando esta es inferior a un (1) año y que manifieste adicionalmente que mantendrá dicho personal por un lapso igual al término de ejecución del contrato.

Si la oferta es presentada por un proponente plural, el integrante que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad, en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25%) en la estructura plural y aportar como mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

El tiempo de vinculación en la planta referida de que trata este numeral se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

4. Preferir la propuesta presentada por el oferente que acredite la vinculación en mayor proporción de personas mayores que no sean beneficiarias de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la ley, para ello, la persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda, entregará un certificado, en el que se acredite, bajo la gravedad de juramento, las personas vinculadas en su nómina y el número de trabajadores que no son beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que cumplieron el requisito de edad de pensión. Solo se tendrá en cuenta la vinculación de aquellas personas que se encuentren en las condiciones descritas y que hayan estado vinculadas con una anterioridad igual o mayor a un (1) año contado a partir de la fecha del cierre del proceso. Para los casos de constitución inferior a un (1) año, se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de la constitución de la persona jurídica.

El tiempo de vinculación en la planta referida, de que trata el inciso anterior, se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de constitución de la persona jurídica, cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

En el caso de los proponentes plurales, su representante legal acreditará el número de trabajadores vinculados que son personas mayores no beneficiarias de la pensión de vejez, familiar o de sobrevivencia, y que cumplieron el requisito de edad de pensión establecido en la ley, de todos los integrantes del proponente. Las personas enunciadas anteriormente podrán estar vinculadas a cualquiera de sus integrantes.

En cualquiera de los dos supuestos anteriores, para el otorgamiento del criterio de desempate, cada uno de los trabajadores que cumpla las condiciones previstas por la ley, allegará un certificado, mediante el cual acredita, bajo la gravedad de juramento, que no es beneficiario de pensión de vejez, familiar o sobrevivencia, y cumple la edad de pensión; además, se deberá allegar el documento de identificación del trabajador que lo firma.

La mayor proporción se definirá en relación con el número total de trabajadores vinculados en la planta de personal, por lo que se preferirá al oferente que acredite un porcentaje mayor. En el caso de proponentes plurales, la mayor proporción se definirá con la sumatoria de trabajadores vinculados en la planta de personal de cada uno de sus integrantes.

5. Preferir la propuesta presentada por el oferente que acredite que por lo menos el diez por ciento (10%) de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana, para lo cual, la persona natural, el representante legal o el revisor fiscal, según corresponda, bajo la gravedad de juramento señalará las personas vinculadas a su nómina, y el número de identificación y nombre de las personas que pertenecen a la población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana. Solo se tendrá en cuenta la vinculación de aquellas personas que hayan estado vinculadas con una anterioridad igual o mayor a un (1) año contado a partir de la fecha del cierre del proceso. Para los casos de constitución inferior a un (1)

año, se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de constitución de la persona jurídica.

El tiempo de vinculación en la planta referida, de que trata el inciso anterior, se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

Además, deberá aportar la copia de la certificación expedida por el Ministerio del Interior, en la cual acredite que el trabajador pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana, en los términos del Decreto Ley 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

En el caso de los proponentes plurales, su representante legal presentará un certificado, mediante el cual acredita que por lo menos diez por ciento (10%) del total de la nómina de sus integrantes pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana. Este porcentaje se definirá de acuerdo con la sumatoria de la nómina de cada uno de los integrantes del proponente plural. Las personas enunciadas anteriormente podrán estar vinculadas a cualquiera de sus integrantes. En todo caso, deberá aportar la copia de la certificación expedida por el Ministerio del Interior, en la cual acredite que el trabajador pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana en los términos del Decreto Ley 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo con el artículo 5 de la Ley 1581 de 2012, se requiere que el titular de la información de estos, como es el caso de las personas que pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana autoricen de manera previa y expresa el tratamiento de la información, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012, como requisito para el otorgamiento del criterio de desempate.

6. Preferir la propuesta de personas naturales en proceso de reintegración o reincorporación, para lo cual presentará copia de alguno de los siguientes documentos: i) la certificación en las desmovilizaciones colectivas que expida la Oficina de Alto Comisionado para la Paz, ii) el certificado que emita el Comité Operativo para la Dejación de las Armas respecto de las personas desmovilizadas en forma individual, iii) el certificado que emita la Agencia para la Reincorporación y la Normalización que acredite que la persona se encuentra en proceso de reincorporación o reintegración o iv) cualquier otro certificado que para el efecto determine la Ley. Además, se entregará copia del documento de identificación de la persona en proceso de reintegración o reincorporación.

En el caso de las personas jurídicas, el representante legal o el revisor fiscal, si están obligados a tenerlo, entregará un certificado, mediante el cual acredite bajo la gravedad de juramento que más del cincuenta por ciento (50 %) de la composición accionaria o cuotas partes de la persona jurídica está constituida por personas en proceso de reintegración o reincorporación. Además, deberá aportar alguno de los certificados del inciso anterior, junto con los documentos de identificación de cada una de las personas que está en proceso de reincorporación o reintegración.

Tratándose de proponentes plurales, se preferirá la oferta cuando todos los integrantes sean personas en proceso de reincorporación, para lo cual se entregará alguno de los certificados del inciso primero de este numeral, y/o personas jurídicas donde más del cincuenta por ciento (50 %) de la composición accionaria o cuotas parte esté constituida por personas en proceso de reincorporación, para lo cual el representante legal, o el revisor fiscal, si está obligado a tenerlo, acreditará tal situación aportando los documentos de identificación de cada una de las personas en proceso de reincorporación.

Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo con el artículo 5 de la Ley 1581 de 2012, se requiere que el titular de la información de estos, como son las personas en proceso de reincorporación o reintegración, autoricen a la entidad de manera previa y expresa el manejo de esta información, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012 como requisito para el otorgamiento de este criterio de desempate.

7. Preferir la oferta presentada por un proponente plural siempre que se cumplan las condiciones de los siguientes numerales:

7. 1. Esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración, para lo cual se acreditarán estas condiciones de acuerdo con lo previsto en el inciso 1 del numeral 2 y/o el inciso 1 del numeral 6 del presente artículo; o por una persona jurídica en la cual participe o participen mayoritariamente madres cabeza de familia y/o personas en proceso de reincorporación o reintegración, para lo cual el representante legal o el revisor fiscal, si están obligados a tenerlo, presentarán un certificado, mediante el cual acrediten, bajo la gravedad de juramento, que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por madres cabeza de familia y/o personas en proceso de reincorporación o reintegración. Además, deberá acreditar la condición indicada de cada una de las personas que participen en la sociedad que sean mujeres cabeza de familia y/o personas en proceso de reincorporación o reintegración, aportando los documentos de cada uno de ellos, de acuerdo con lo previsto en este numeral. Este integrante debe tener una participación de por lo menos el veinticinco por ciento (25 %) en el proponente plural.

7.2. El integrante del proponente plural de que trata el anterior numeral debe aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

7.3. En relación con el integrante del numeral 7.1. ni la madre cabeza de familia o la persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales podrán ser empleados, socios o accionistas de otro de los integrantes del proponente plural, para lo cual el integrante del que trata el numeral 7.1. lo manifestará en un certificado suscrito por la persona natural o el representante legal de la persona jurídica.

Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo el artículo 5 de la Ley 1581 de 2012, se requiere que el titular de la información de estos, como es el caso de las personas en proceso de reincorporación y/o reintegración autoricen de manera previa y expresa el tratamiento de esta información, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012, como requisito para el otorgamiento del criterio de desempate.

8. Preferir la oferta presentada por una Mipyme, lo cual se verificará en los términos del artículo 2.2.1.2.4.2.4 del presente Decreto, en concordancia con el parágrafo del artículo 2.2.1.13.2.4 del Decreto 1074 de 2015.

Asimismo, se preferirá la oferta presentada por una cooperativa o asociaciones mutuales, para lo cual se aportará el certificado de existencia y representación legal expedido por la Cámara de Comercio o la autoridad respectiva. En el caso específico en que el empate se presente entre cooperativas o asociaciones mutuales que tengan el tamaño empresarial de grandes empresas junto con micro, pequeñas o medianas, se preferirá la oferta las cooperativas o asociaciones mutuales que cumplan con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

Tratándose de proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en los incisos anteriores de este numeral. En el evento en que el empate se presente entre proponentes plurales cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuales al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

9. Preferir la oferta presentada por el proponente plural constituido en su totalidad por micro y/o pequeñas empresas, cooperativas o asociaciones mutuales.

La condición de micro o pequeña empresa se verificará en los términos del artículo 2.2.1.2.4.2.4 del presente Decreto, en concordancia con el parágrafo del artículo 2.2.1.13.2.4 del Decreto 1074 de 2015.

La condición de cooperativa o asociación mutual se acreditará con el certificado de existencia y representación legal expedido por la Cámara de Comercio o la autoridad respectiva. En el evento en que el empate se presente entre proponentes plurales cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuáles al menos uno de sus integrantes

sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

10. Preferir al oferente persona natural o jurídica que acredite, de acuerdo con sus estados financieros o información contable con corte al 31 de diciembre del año anterior, que por lo menos el veinticinco por ciento (25 %) del total de sus pagos fueron realizados a Mipyme, cooperativas o asociaciones mutuales por concepto de proveeduría del oferente, efectuados durante el año anterior, para lo cual el proponente persona natural y contador público; o el representante legal de la persona jurídica y revisor fiscal para las personas obligadas por ley; o del representante legal de la persona jurídica y contador público, según corresponda, entregará un certificado expedido bajo la gravedad de juramento, en el que conste que por lo menos el veinticinco por ciento (25%) del total de pagos fueron realizados a Mipyme, cooperativas o asociaciones mutuales.

Igualmente, cuando la oferta es presentada por un proponente plural se preferirá a este siempre que:

10.1. Esté conformado por al menos una Mipyme, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural, para lo cual se presentará el documento de conformación del proponente plural y, además, ese integrante acredite la condición de Mipyme, cooperativa o asociación mutual en los términos del numeral 8 del presente artículo;

10.2. La Mipyme, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25 %) de la experiencia acreditada en la oferta; y

10.3. Ni la Mipyme, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los otros integrantes del proponente plural, para lo cual el integrante respectivo lo manifestará mediante un certificado suscrito por la persona natural o el representante legal de la persona jurídica.

En el evento en que el empate se presente entre proponentes plurales, que cumplan con los requisitos de los incisos anteriores, cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuales al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

11. Preferir las empresas reconocidas y establecidas como Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento Mipymes, para lo cual se presentará el certificado de existencia y representación legal en el que conste el cumplimiento a los requisitos del artículo 2 de la Ley 1901 de 2018, o la norma que la modifique o la sustituya. Asimismo, acreditará la condición de Mipyme en los términos del numeral 8 del presente artículo.

Tratándose de proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes acredite las condiciones señaladas en el inciso anterior de este numeral.

12. Utilizar un método aleatorio para seleccionar al oferente, el cual deberá estar establecido previamente en el pliego de condiciones, invitación o documento que haga sus veces.

PARÁGRAFO 1. Los factores de desempate deberán aplicarse en armonía con los Acuerdos Comerciales vigentes suscritos por Colombia. De esta manera, en el evento en que el empate se presente entre ofertas cubiertas por un Acuerdo Comercial, se aplicarán los factores de desempate que sean compatibles con los mencionados Acuerdos.

Sin perjuicio de la obligación anterior, el Ministerio de Comercio, Industria y Turismo y la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente señalarán en un Manual o Guía no vinculante los lineamientos para la aplicación de los factores de desempate en cumplimiento de un Acuerdo Comercial en la etapa de selección del Proceso de Contratación.

PARÁGRAFO 2. Si el empate entre las propuestas se presenta con un proponente, bien o servicio extranjero cuyo país de origen no tiene Acuerdo Comercial con Colombia, ni trato nacional por reciprocidad o con ocasión de la normativa comunitaria, se dará aplicación a todos los criterios de desempate previstos en el presente numeral.

PARÁGRAFO 3. Conforme con el artículo 18 de la Ley 1712 de 2014 y los artículos 5 y 6 de la Ley 1581 de 2012, la Entidad Estatal garantizará el derecho a la reserva legal de toda aquella información que acredita el cumplimiento de los factores de desempate de: i) las mujeres víctimas de violencia intrafamiliar, ii) las personas en proceso de reincorporación y/o reintegración y iii) la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana.
En armonía con lo anterior, en la plataforma del SECOP no se publicará para conocimiento de terceros la información relacionada con los factores de desempate de personas en procesos de reincorporación o reintegración o mujeres víctimas de violencia intrafamiliar o la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana, puesto que su público conocimiento puede afectar el derecho a la intimidad de los oferentes o de sus trabajadores o socios o accionistas.

17. ANÁLISIS DE RIESGO Y LA FORMA DE MITIGARLO.

El Departamento de Santander realizo el correspondiente análisis del riesgo y la forma de mitigarlo del proceso de licitación que nos ocupa el cual se encuentra detallado en el **ANEXO – ANÁLISIS DEL RIESGO** documento que hace parte integral del presente estudio. Así mismo en dicho anexo se incluye la correspondiente matriz de riesgos.

El día, hora y lugar señalados en el cronograma de actividades, se llevará a cabo la audiencia a la que se refieren el artículo 30 de la ley 80 de 1993, artículo 4 de la Ley 1150 de 2007, el artículo 220 del Decreto Ley 019 de 2012, y el artículo 2.2.1.2.1.1.2 del decreto 1082 de 2015. Como consecuencia de las observaciones realizadas por los interesados, el Departamento de Santander, se pronunciará sobre la pertinencia o no de las mismas y establecerá la estimación, tipificación y asignación definitiva de los Riesgos involucrados en el Proceso de Contratación.

Vencido el plazo para discutir y revisar los Riesgos identificados, si se presenta alguna observación adicional, la misma solo será estudiada y tenida en cuenta por parte del Departamento, únicamente si da lugar a modificar el Pliego de Condiciones mediante Adenda.

18. DE LAS GARANTÍAS EN EL PROCESO DE CONTRATACIÓN.

18.1. RIESGO A CUBRIR POR LAS GARANTÍAS.

De conformidad con el artículo 2.2.1.2.3.1.1 del decreto 1082 de 2015 los riesgos que deben cubrir las garantías en la contratación, son el cumplimiento de las obligaciones surgidas en favor de las Entidades Estatales con ocasión de:

a) La presentación de las ofertas;
b) Los contratos y su liquidación; y
c) Los riesgos a los que se encuentran expuestas las Entidades Estatales, derivados de la responsabilidad extracontractual que pueda surgir por las actuaciones, hechos u omisiones de sus contratistas y subcontratistas.

18.2. CLASES DE GARANTÍAS.

El oferente que resulte favorecido, en su calidad de contratista podrá otorgar para asegurar el cumplimiento de sus obligaciones las siguientes garantías:

a) Contrato de seguro contenido en una póliza.
b) Patrimonio autónomo.
c) Garantía Bancaria.
NOTA 1: La responsabilidad extracontractual de la administración derivada de las actuaciones, hechos u omisiones de sus contratistas o subcontratistas solo puede ser amparada con un contrato de seguro.

NOTA 2: El monto, vigencia, amparos o coberturas de las garantías se determinarán teniendo en cuenta el objeto, la naturaleza, las características de cada contrato y los riesgos que se deban cubrir.

18.3. INDIVISIBILIDAD DE LA GARANTÍA.

La garantía de cobertura del Riesgo es indivisible; sin embargo, en los contratos con un plazo mayor a cinco (5) años las garantías pueden cubrir los Riesgos de la Etapa del Contrato o del Periodo Contractual, de acuerdo con lo previsto en el contrato.

En consecuencia, de conformidad con lo establecido en el Decreto 1082 de 2015, la Entidad Estatal en los pliegos de condiciones para la Contratación debe indicar las garantías que exige en cada Etapa del Contrato o cada Periodo Contractual así:

a.) La Entidad Estatal debe exigir una garantía independiente para cada Etapa del Contrato o cada Periodo Contractual, cuya vigencia debe ser por lo menos la misma establecida para la Etapa del Contrato o Periodo Contractual respectivo.

b.) La Entidad Estatal debe calcular el valor asegurado para cada Etapa del Contrato, Periodo Contractual o unidad funcional, tomando el valor de las obligaciones del contratista para cada Etapa del Contrato o Periodo Contractual, de acuerdo con las reglas de suficiencia de las garantías establecidas en el decreto 1082 de 2015.

c.) Antes del vencimiento de cada Etapa del Contrato o cada Periodo Contractual, el contratista está obligado a obtener una nueva garantía que ampare el cumplimiento de sus obligaciones para la Etapa del Contrato o Periodo Contractual subsiguiente, si no lo hiciere se aplicarán las reglas previstas para el restablecimiento de la garantía.

Si el garante de una Etapa del Contrato o un Periodo Contractual decide no continuar garantizando la Etapa del Contrato o Periodo Contractual subsiguiente, debe informar su decisión por escrito a la Entidad Estatal garantizada seis (6) meses antes del vencimiento del plazo de la garantía. Este aviso no afecta la garantía de la Etapa Contractual o Periodo Contractual en ejecución. Si el garante no da el aviso con la anticipación mencionada y el contratista no obtiene una nueva garantía, queda obligado a garantizar la Etapa del Contrato o el Periodo Contractual subsiguiente.

18.4. GARANTÍAS A EXIGIR

18.4.1 GARANTÍA DE SERIEDAD DE LA OFERTA

El Proponente debe presentar junto con la Oferta una garantía de seriedad de la oferta a favor de la Entidad Contratante por el diez por ciento (10%) del valor de la oferta, (el artículo 2.2.1.2.3.1.9 del Decreto 1082 de 2015 establece que el valor de esta garantía debe ser de por lo menos el diez (10%) del valor de la oferta), y su vigencia será desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato.

Frente al particular se recomienda revisar apartado de garantía de seriedad de la oferta dispuesto en el acápite de requisitos habilitantes de orden jurídico como criterio diferencial.

18.4.2 GARANTÍA DE CUMPLIMIENTO

De conformidad con el artículo 2.2.1.2.3.1.7 del decreto 1082 de 2015, la. Garantía de cumplimiento del contrato debe cubrir:

a) CUMPLIMIENTO DEL CONTRATO.

Este amparo cubre a la Entidad Estatal de los perjuicios derivados de:

i. El incumplimiento total o parcial del contrato, cuando el incumplimiento es imputable al contratista;
ii. El cumplimiento tardío o defectuoso del contrato, cuando el incumplimiento es imputable al contratista;
iii. Los daños imputables al contratista por entregas parciales de la obra, cuando el contrato no prevé entregas parciales; y
iv. El pago del valor de las multas y de la cláusula penal pecuniaria.

SUFICIENCIA: Esta garantía debe tener una vigencia mínima hasta la liquidación del contrato. El valor de esta garantía **debe ser del veinte por ciento (20%) del valor del contrato y seis meses mas**, (según el artículo 2.2.1.2.3.1.12. del decreto 1082 de 2015, el valor de esta garantía debe ser de por lo menos el diez (10%) por ciento del valor del contrato).

b) PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES.

Este amparo debe cubrir a la Entidad Estatal de los perjuicios ocasionados por el incumplimiento de las obligaciones laborales del contratista derivadas de la contratación del personal utilizado en el territorio nacional para la ejecución del contrato amparado.

SUFICIENCIA: Esta garantía **debe estar vigente por el plazo del contrato y tres (3) años más. El**

valor de esta garantía debe ser del veinte (20%) del valor del contrato, (según el artículo 2.2.1.2.3.1.13. del decreto 1082 de 2015, el valor de esta garantía no puede ser inferior al cinco por ciento (5%) del valor total del contrato).

c) CALIDAD DEL SERVICIO.

Este amparo cubre a la Entidad Estatal por los perjuicios derivados de la deficiente calidad del servicio prestado.

SUFICIENCIA: Según el artículo 2.2.1.2.3.1.15. del Decreto 1082 de 2015, "la Entidad Estatal debe determinar el valor y el plazo de la garantía de acuerdo con el objeto, el valor, la naturaleza y las obligaciones contenidas en el contrato. En los contratos de interventoría, la vigencia de este amparo debe ser igual al plazo de la garantía de estabilidad del contrato principal en cumplimiento del parágrafo del artículo 85 de la Ley 1474 de 2011". Teniendo en cuenta esta premisa, esta garantía **debe estar vigente por el plazo del contrato y seis (6) meses más, y el valor del amparo debe ser del veinte por ciento (20%) del valor del contrato**.

d) CALIDAD DE LOS BIENES

Este amparo cubre a la Entidad Estatal por los perjuicios derivados de la deficiente calidad de los bienes que se suministren dentro de la prestación de servicio y que por su integralidad queden a favor y en propiedad del contratante.

SUFICIENCIA: Según el artículo 2.2.1.2.3.1.15. del Decreto 1082 de 2015, "la Entidad Estatal debe determinar el valor y el plazo de la garantía de acuerdo con el objeto, el valor, la naturaleza y las obligaciones contenidas en el contrato. En los contratos de interventoría, la vigencia de este amparo debe ser igual al plazo de la garantía de estabilidad del contrato principal en cumplimiento del parágrafo del artículo 85 de la Ley 1474 de 2011". Teniendo en cuenta esta premisa, esta garantía **debe estar vigente por el plazo del contrato y seis (6) meses más, y el valor del amparo debe ser del veinte por ciento (20%) del valor del contrato**.

18.4.3. RESPONSABILIDAD CIVIL EXTRACONTRACTUAL.

La Entidad Estatal debe exigir en los contratos de obra, y en aquellos en que por su objeto o naturaleza lo considere necesario con ocasión de los Riesgos del contrato, el otorgamiento de una póliza de responsabilidad civil extracontractual que la proteja de eventuales reclamaciones de terceros derivadas de la responsabilidad extracontractual que surja de las actuaciones, hechos u omisiones de su contratista.

La Entidad Estatal debe exigir que la póliza de responsabilidad extracontractual cubra también los perjuicios ocasionados por eventuales reclamaciones de terceros derivadas de la responsabilidad extracontractual que surjan de las actuaciones, hechos u omisiones de los subcontratistas autorizados o en su defecto, que acredite que el subcontratista cuenta con un seguro propio con el mismo objeto y que la Entidad Estatal sea el asegurado.

SUFICIENCIA: La vigencia de esta garantía deberá ser igual al período de ejecución del contrato. El valor asegurado por los contratos de seguro que amparan la responsabilidad civil extracontractual, teniendo en cuenta el valor del presupuesto del presente proceso, de conformidad con el artículo 2.2.1.2.3.1.17. Del decreto 1082 de 2015, deberá constituirse por un monto de **CUATROCIENTOS (400) SMMLV**

18.4.3.1. REQUISITOS DEL SEGURO DE RESPONSABILIDAD CIVIL EXTRACONTRACTUAL.

El amparo de responsabilidad civil extracontractual debe cumplir los siguientes requisitos:

i. Modalidad de ocurrencia. La compañía de seguros debe expedir el amparo en la modalidad de ocurrencia. En consecuencia, el contrato de seguro no puede establecer términos para presentar la reclamación, inferiores a los términos de prescripción previstos en la ley para la acción de responsabilidad correspondiente.

ii. Intervinientes. La Entidad Estatal y el contratista deben tener la calidad de asegurado respecto de los daños producidos por el contratista con ocasión de la ejecución del contrato amparado, y serán

beneficiarios tanto la Entidad Estatal como los terceros que puedan resultar afectados por la responsabilidad del contratista o sus subcontratistas.
iii. Amparos. El amparo de responsabilidad civil extracontractual debe contener además de la cobertura básica de predios, labores y operaciones, mínimo los siguientes amparos:

a. Cobertura expresa de perjuicios por daño emergente y lucro cesante.
b. Cobertura expresa de perjuicios extra patrimoniales
c. Cobertura expresa de la responsabilidad surgida por actos de contratistas y subcontratistas, salvo que el subcontratista tenga su propio seguro de responsabilidad extracontractual, con los mismos amparos aquí requeridos.
d. Cobertura expresa de amparo patronal.
e. Cobertura expresa de vehículos propios y no propios.

18.4. MECANISMOS DE PARTICIPACIÓN EN LA PÉRDIDA POR PARTE DE LA ENTIDAD ESTATAL ASEGURADA.

En el contrato de seguro que ampara la responsabilidad civil extracontractual solamente se pueden pactar deducibles hasta del diez por ciento (10%) del valor de cada pérdida y en ningún caso pueden ser superiores a dos mil (2.000) smmlv. No serán admisibles las franquicias, coaseguros obligatorios y demás formas de estipulación que impliquen la asunción de parte de la pérdida por la entidad asegurada.

18.5. RESTABLECIMIENTO O AMPLIACIÓN DE LA GARANTÍA.

Cuando con ocasión de las reclamaciones efectuadas por la Entidad Estatal, el valor de la garantía se reduce, la Entidad Estatal debe solicitar al contratista restablecer el valor inicial de la garantía.

Cuando el contrato es modificado para incrementar su valor o prorrogar su plazo, la Entidad Estatal debe exigir al contratista ampliar el valor de la garantía otorgada o ampliar su vigencia, según el caso. La Entidad Estatal debe prever en los pliegos de condiciones para la Contratación, el mecanismo que proceda para restablecer la garantía, cuando el contratista incumpla su obligación de obtenerla, ampliarla o adicionarla.

18.6. TÉRMINO PARA ENTREGA DE LA GARANTÍA.

El contratista entregará a El DEPARTAMENTO DE SANTANDER, a más tardar dentro de los CINCO (5) DÍAS HÁBILES siguientes a la suscripción del contrato, las garantías requeridas.

18.7. REQUISITOS GENERALES DE LA GARANTÍA

En las garantías deben figurar como afianzadas cada una de las personas que integran la parte contratista, y el beneficiario debe ser EL DEPARTAMENTO DE SANTANDER. NIT. DEL DEPARTAMENTO DE SANTANDER: No. 890.201.235-6.

En caso de que el contratista sea un consorcio o unión temporal: La póliza de garantía debe ser otorgada a nombre del Consorcio o Unión Temporal indicando el nombre de todos y cada uno de sus integrantes, así como el porcentaje de participación de cada uno. Por tanto, en caso de consorcio o unión temporal la garantía no podrá ser a nombre del representante legal del consorcio o Unión Temporal.

Las garantías deben contener la manifestación por parte del asegurador, según la cual, las mismas se encuentran cubiertas por un reasegurador inscrito en la Superintendencia Financiera de Colombia. El DEPARTAMENTO DE SANTANDER se reserva el derecho de solicitar la certificación por parte del reasegurador que se indique en dicha manifestación.
La póliza deberá estar firmada en **ORIGINAL** por el tomador, esto es, por el contratista.

19. INDICACIÓN SI EL PROCESO DE CONTRATACIÓN ESTA COBIJADO POR UN ACUERDO COMERCIAL.

ACUERDOS INTERNACIONALES

Colombia Compra Eficiente pone a disposición de las Entidades Estatales del nivel departamental el presente Anexo como guía para verificar: (a) cuáles Entidades Estatales están incluidas en cada uno de los Acuerdos Comerciales; (b) el valor a partir del cual los Procesos de Contratación están

cubiertos por los Acuerdos Comerciales y (c) la existencia de excepciones a la cobertura del Acuerdo Comercial.

Entidades Estatales incluidas en la lista de los Acuerdos Comerciales

Los Departamentos están incluidos en la lista de Entidades de los Acuerdos Comerciales con la Alianza Pacífico (únicamente con Chile y Perú), Chile, Corea, Costa Rica, los Estados AELC, Estados Unidos, el Triángulo Norte (únicamente con El Salvador y Guatemala), la Unión Europea (aplicable al Reino Unido e Irlanda del Norte), Israel y por la Decisión 439 de 1998 de la Comisión de la CAN. Las Contralorías del nivel departamental están incluidas en la lista de Entidades en los Acuerdos Comerciales con Chile, el Triángulo Norte (únicamente con Guatemala y El Salvador); la Unión Europea (aplicable al Reino Unido e Irlanda del Norte); y por la Decisión 439 de 1998 de la Comisión de la CAN. Del mismo modo, las Universidades del nivel departamental están incluidas en la lista del Acuerdo Comercial con Chile, la Unión Europea (aplicable al Reino Unido e Irlanda del Norte) y por la Decisión 439 de 1998 de la Comisión de la CAN.

Salvo por algunas excepciones, todas las demás Entidades Estatales del nivel departamental (incluidas las entidades descentralizadas indirectas) están contempladas en la lista de Entidades cubiertas por los Acuerdos Comerciales con Chile, el Triángulo Norte (únicamente con El Salvador y Guatemala), la Unión Europea (aplicable al Reino Unido e Irlanda del Norte) y por la Decisión 439 de 1998 de la Comisión de la CAN.

Valores

El Acuerdo Comercial con Alianza Pacifico es aplicable a los Procesos de Contratación para: (i) adquirir bienes y servicios a partir de 200.000 DEG y (ii) para servicios de construcción desde 5.000.000 DEG.

El Acuerdo Comercial con los Estados AELC (EFTA) es aplicable a los Procesos de Contratación para: (i) adquirir bienes y servicios a partir de 200.000 DEG y (ii) para servicios de construcción desde 5.000.000 DEG.

El Acuerdo Comercial con Costa Rica es aplicable a los Procesos de Contratación para: (i) adquirir bienes y servicios a partir de US$ 498.000 y (ii) para servicios de construcción desde US$ 7.008.000.

El Acuerdo Comercial con la Unión Europea (aplicable al Reino Unido e Irlanda del Norte) es aplicable a los Procesos de Contratación para: (i) adquirir bienes y servicios a partir de 200.000 DEG y (ii) para servicios de construcción desde 5.000.000 DEG.

El Acuerdo Comercial con Israel es aplicable a los Procesos de Contratación para: (i) adquirir bienes y servicios a partir de 250.000 DEG y (ii) para servicios de construcción a partir de 5.000.000 SDR.

El Acuerdo Comercial con el Triángulo Norte (únicamente con El Salvador y Guatemala) es aplicable a los Procesos de Contratación a partir del límite inferior de la menor cuantía.

El Acuerdo Comercial con la República de Corea es aplicable a los Procesos de Contratación para: (i) bienes y servicios a partir de 200.000 DEG y (ii) para servicios de construcción desde 15.000.000 SDR.

El Acuerdo Comercial con los Estados Unidos de América es aplicable a los Procesos de Contratación para la contratación de bienes y servicios a partir de US$ 526.000 y para servicios de construcción desde US$ 7.407.000. Esta última suma se ajusta durante los tres años siguientes a la entrada en vigor del Acuerdo comercial de conformidad con la Sección del Acuerdo Comercial o la suma de US$8,000,000, la que sea mayor.

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 departamental obligadas, independientemente del valor del Proceso de Contratación. Todos los valores anteriores deben observarse teniendo en cuenta que reflejan los umbrales base pactados en los capítulos de compra pública de los Acuerdos Comerciales. Sin embargo, debe tenerse en cuenta que estos valores son actualizados periódicamente, teniendo en cuenta las fórmulas incorporadas en cada acuerdo y la TRM aplicable.

Las Entidades Estatales podrán dirigirse al sitio web de Colombia Compra Eficiente donde podrán consultar en pesos colombianos los umbrales aplicables a los Acuerdos Comerciales.

Excepciones

Acuerdo Comercial		Excepciones
Alianza Pacífico	Chile	1, 2, 3, 4, 5, 6, 7, 12, 14, 15, 16, 17, 19, 28, 29, 32, 35, 37, 55, 61.
	Perú	
Chile		1, 2, 3, 4, 5, 6, 8, 12, 14, 15, 16, 17, 18, 19, 28, 29, 32, 33, 34, 35, 36, 37, 47.
Corea		1, 3, 4, 5, 6, 7, 10, 11, 12, 14, 15, 16, 17, 19, 28, 29, 32, 34, 35, 37, 57, 58.
Costa Rica		1, 3, 4, 5, 6 ,7, 9, 12, 14, 15, 16, 17, 19, 28, 29, 32, 34, 35, 37, 57, 58.
Estados AELC		1, 4, 5, 6, 7, 10, 11, 12, 14, 15, 16, 17, 19, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37.
Estados Unidos		1, 2, 3, 4, 5, 6, 7, 12, 14, 15, 16, 17, 19, 28, 29, 30, 32, 33, 34, 35, 36, 37.
Triángulo Norte	El Salvador	1, 2, 3, 4, 5, 6, 7, 9, 14, 20, 38, 48, 49, 59.
	Guatemala	1, 2, 3, 4, 5, 6, 7, 9, 14, 20, 21, 50, 51, 52, 53, 59.
Unión Europea Reino Unido e Irlanda del Norte		1, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17, 19, 23, 28, 29, 31, 32, 35, 37, 49, 57, 61.
Israel		1,3,4,5,7,8,11,12,13,14,15,16,19,28,29,32,34,35,37.

Por lo tanto, siguiendo las directrices señaladas en dicho manual, se procederá a realizar la verificación de la aplicabilidad de los acuerdos comerciales con el presente proceso contractual de conformidad con la siguiente tabla (Los tratados se realizan en DEG (Derechos especiales de giro) el cual tiene una razón respecto al peso de):

Nota 1: La información contenida en este documento fue elaborada por el Ministerio de Comercio Industria y Turismo – MINCIT y la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente la pública por su importancia para las entidades públicas y los participantes en la contratación.

Nota 2: Según el Ministerio de Comercio Industria y Turismo – MINCIT el valor de los umbrales tendrá vigencia del 1 de enero del 2024 hasta el 31 de diciembre de 2025, para los Acuerdos Comerciales suscritos con: (i) Canadá, (ii) Reino Unido de Gran Bretaña e Irlanda del Norte, (iii) Estados Unidos, (iv) Chile, (v) Costa Rica, (vi) Alianza del Pacífico y (vii) Corea.

Nota 3: Según el MINCIT el valor de los umbrales tendrá vigencia del 1 de enero del 2025 hasta el 31 de diciembre de 2026, para los Acuerdos Comerciales suscritos con: (i) México, (iii) países de la Unión Europea, y (iii) países EFTA (Suiza, Noruega, Liechtenstein e Islandia)

Nota 4: En cuanto al acuerdo comercial vigente con Israel los umbrales establecidos en DEG se calcularán y convertirán a pesos colombianos utilizando la Tasa Representativa del Mercado (TRM) del Banco de la República de Colombia del día anterior a la fecha de publicación del aviso de convocatoria del respectivo proceso de compra. (ver ejemplo en la sección correspondiente)

Nota 5: Sin perjuicio de las particularidades de la cobertura dispuesta por cada Acuerdo Comercial, por regla general, las entidades del nivel central corresponden a las entidades del sector nacional y las entidades del nivel subcentral corresponden a las entidades del sector territorial.

Nota 6: De conformidad con lo previsto en el artículo 5 del Decreto 1860 de 2021, que modifica el artículo 2.2.1.2.4.2.2. del Decreto 1082 de 2015, y el anexo 4 del manual para el manejo de los acuerdos comerciales en procesos de contratación, las convocatorias limitadas a MiPymes se encuentran excluidas de la aplicación de los acuerdos comerciales. El umbral para la limitación de MiPymes será el previsto por la norma equivalente a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000). Esta exclusión sólo es aplicable en los casos en que la Entidad Estatal verifique las condiciones previstas en el respectivo Acuerdo comercial y 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, para que una convocatoria sea limitada a Mipyme. Así, esta excepción no puede ser utilizada para excluir la cobertura del Acuerdo Comercial en el aviso de convocatoria; los estudios y documentos previos o el borrador del pliego de condiciones.

UMBRAL MIPYMES 2026

US $	125.000
COL $	511.708.497

Tabla VERIFICACION DE ACUERDOS COMERCIALES INTERNACIONALES

Acuerdos Comerciales			**Entidad Estatal cubierta**	**Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial**	**Excepción Aplicable al Proceso de Contratación**	**Proceso de Contratación cubierto por el Acuerdo Comercial**
			Si/No	Si/No	Si/No	Si/No
Alianza Pacífico	Chile	BIENES Y SERVICIOS $1.147.016.154 BIENES Y SERVICIOS CONSTRUCCION $ 28.675.403.847	SI	SI	NO	SI
	Perú	BIENES Y SERVICIOS $1.147.016.154 BIENES Y SERVICIOS CONSTRUCCION $ 28.675.403.847	SI	SI	NO	SI
Canadá			N/A	N/A	N/A	N/A
Chile		BIENES Y SERVICIOS $ 1.148.221.780 BIENES Y SERVICIOS CONSTRUCCION $ 28.705.544.496	SI	SI	NO	SI
Corea		BIENES Y SERVICIOS $ 1.147.000.000 BIENES Y SERVICIOS CONSTRUCCION $ 86.020.000.000	SI	SI	NO	SI
Costa Rica		BIENES Y SERVICIOS $ 2.030.722.904 BIENES Y SERVICIOS CONSTRUCCION $ 28.617.834.543	SI	NO	NO	NO
Estados Unidos		BIENES Y SERVICIOS $ 2.030.722.904. BIENES Y SERVICIOS CONSTRUCCION $ 28.617.834.543	SI	NO	NO	NO
Estado AELC		BIENES Y SERVICIOS $ 1.131.227.573 BIENES Y SERVICIOS CONSTRUCCION $ 28.280.689.315	SI	SI	NO	SI
México			N/A	N/A	N/A	N/A
Triángulo Norte	El Salvador	Valor de la menor cuantía de la entidad	SI	SI	NO	SI
	Guatemala	Valor de la menor cuantía de la entidad	SI	SI	NO	SI
	Honduras		N/A	N/A	N/A	N/A
Unión Europea		BIENES Y SERVICIOS $ 1.131.227.573	SI	SI	NO	SI

Acuerdos Comerciales		Entidad Estatal cubierta	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
		Si/No	Si/No	Si/No	Si/No
	BIENES Y SERVICIOS CONSTRUCCION $ 28.280.689.315				
Reino Unido e Irlanda del Norte	BIENES Y SERVICIOS $ 1.148.221.780 BIENES Y SERVICIOS CONSTRUCCION $ 28.705.544.496	SI	SI	NO	SI

FUENTE COLOMBIA COMPRA EFICIENTE

De acuerdo con la tabla de verificación de tratados internacionales, APLICA TRATADOS INTERNACIONES CON ALIANZA DEL PACIFICO CHILE, ALIANZA DEL PACIFICO PERÚ, CHILE, COREA, TRIANGULO DEL NORTE (GUATEMALA-SALVADOR), ESTADOS AELC (EFTA - SUIZA, LIECHTENSTEIN, NORUEGA E ISLANDIA), UNION EUROPEA – REINO UNIDO Y LA CAN. CON ISRAEL ESTA CONDICIONADO CON LA FECHA DEL AVISO DE CONVOCATORIA

El proceso no ostenta excepciones.

El presente proceso está cubierto por Acuerdos CON ALIANZA DEL PACIFICO CHILE, ALIANZA DEL PACIFICO PERÚ, CHILE, COREA, TRIANGULO DEL NORTE (GUATEMALA-SALVADOR), ESTADOS AELC (EFTA - SUIZA, LIECHTENSTEIN, NORUEGA E ISLANDIA), UNION EUROPEA – REINO UNIDO Y LA CAN. CON ISRAEL ESTA CONDICIONADO CON LA FECHA DEL AVISO DE CONVOCATORIA

APOYO A LA INDUSTRIA NACIONAL
El componente denominado Estimulo a la industria nacional tendrá una asignación máxima de puntaje equivalente a diez (10) puntos. Los cuales se asignarán de la manera como se expone en adelante. Esto se establece en seguimiento a lo estipulado en el artículo 2 de la Ley 816 de 2003 para apoyar la industria nacional, modificado parcialmente por el Decreto 680 de 2021, a través del sistema de compras y contratación pública en la evaluación de las ofertas.

PROMOCIÓN A LA INDUSTRIA NACIONAL – PROMOCIÓN DE BIENES Y SERVICIOS NACIONALES O CON TRATO NACIONAL

Se entiende por BIENES NACIONALES los bienes inscritos en el Registro de Productores de Bienes Nacionales – RPBN, que son aquellos totalmente obtenidos en el territorio colombiano, los bienes elaborados en el país con materiales nacionales; y los bienes que hayan sufrido una transformación sustancial en función de un porcentaje mínimo de Valor Agregado Nacional o un proceso productivo sustancial.

Se entiende por SERVICIOS NACIONALES aquellos prestados por personas natural colombiana o residente en Colombia; Personas Jurídicas constituidas en el país, se acreditará el origen nacional de la oferta de la siguiente manera:

- ✓ Persona Natural Colombiana, con la presentación de la cédula de ciudadanía del proponente en copia simple, la cual deberá ser aportada con su oferta.

- ✓ Persona Natural Extranjera Residente en Colombia, con la presentación de la visa correspondiente http://www.cancilleria.gov.co/tramites_servicios/visas/categorias/negocios) que le permita la ejecución ejecutar el objeto contractual de conformidad con la Ley. La cual deberá ser aportada con la oferta en copia simple. • Persona Jurídica constituida en el país, se verificará con el Certificado de Cámara y Comercio que el domicilio de la persona jurídica este dentro del territorio nacional.
- ✓ Persona Jurídica Extranjera: De acuerdo al artículo 2.2.1.2.4.1.3. del Decreto 1082 de

2015, las personas jurídicas extranjeras recibirán trato nacional cuando se cumpla alguna de las siguientes tres condiciones, para lo cual se verificará por la Entidad en el orden que se relaciona y de manera excluyente:

Se dará trato nacional a: a. Los bienes y servicios de otros Estados con los cuales exista un Acuerdo Comercial aplicable al Proceso de Contratación; b. A los bienes y servicios respecto de los cuales exista trato nacional por reciprocidad (situación que se verificará de conformidad con lo establecido por el artículo 2.2.1.2.4.1.3. del Decreto 1082 de 2015) y, a los servicios de la Comunidad Andina de Naciones –CAN.

CONVOCATORIAS LIMITADAS A MÍPYME.

El presente proceso NO es susceptible de limitación a mipyme.

NORMATIVIDAD APLICABLE

Ley 80 de 1993, se expide el Estatuto General de Contratación de la Administración Pública, en concordancia con el Decreto 1082 de 2015, sobre el deber de las entidades estatales de efectuar 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 Riesgos.
Ley 1474 de 2011, en concordancia con el numeral 12 del artículo 25 de la Ley 80 de 1993, establece que con la debida antelación a la apertura del procedimiento de selección o de la firma del contrato, según el caso, deberán elaborarse los estudios, diseños y proyectos requeridos y los pliegos de condiciones.

Ley 1341 del 2009, establece como uno de sus principios orientadores el desarrollo de los artículos 20 y 67 de la constitución política, que el Estado promoverá el derecho al acceso a las Tecnologías de la Información y las comunicaciones, que permitan, entre otros, el ejercicio pleno al derecho de la educación, el conocimiento, la ciencia, la técnica y a los demás bienes y valores de la cultura. De igual forma la Ley establece que las entidades de orden nacional y territorial promoverán, coordinaran y ejecutaran planes programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones.

Plan Nacional De Desarrollo 2022 – 2026.

Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Decreto Nacional 2433 de 2015, por el cual se reglamenta el Registro TIC y se subroga el título 1 de la parte 2 del Libro 2 del Decreto 1078 de 2015.

Plan de Desarrollo Santander ES TIEMPO DE SANTANDER 2024 – 2027.
Guía para la Elaboración de Estudios del Sector G-EES-02, expedidos por Colombia Compra Eficiente

Teniendo en cuenta la anterior legislación y demás normas que modifiquen, reglamenten o sustituyan, se procede a realizar el “Análisis del Sector” para ofrecer herramientas y establecer el contexto del Proceso de Contratación, identificar algunos de los Riesgos, determinar los requisitos habilitantes y la forma de evaluar las ofertas.[3]

20. SUPERVISIÓN.

El supervisor ejercerá un control integral o técnico, administrativo, financiero, contable o jurídico sobre el proyecto, según las funciones propias asignadas por la entidad, y podrán en cualquier momento, exigir al contratista la información que considere necesaria, así como la adopción de medidas para mantener, durante el desarrollo y ejecución del mismo.

El Contratista debe acatar las órdenes que le imparta por escrito, y con copia a la Entidad, el supervisor. No obstante, si el Contratista no está de acuerdo con las mismas debe manifestarlo por escrito al supervisor, con copia al jefe de la oficina gestora, antes de proceder a ejecutar las órdenes. En caso contrario, responderá solidariamente con el supervisor si del cumplimiento de dichas órdenes se derivan perjuicios para el departamento de Santander.

Si el Contratista rehúsa o descuida cumplir cualquier orden escrita del supervisor, éste le notificará por escrito sobre el incumplimiento de dicha orden, señalando específicamente las omisiones o infracciones y exigiendo su cumplimiento. Si esta notificación no surte ningún efecto dentro de un plazo de 5 días hábiles, el supervisor comunicará dicha situación al departamento de Santander – oficina gestora para que este tome las medidas que considere necesarias. El supervisor debe documentar las causas o motivos del incumplimiento que llegue a presentarse, como es el caso de atención de emergencias, derrumbes, hundimientos de bancas, interrupción del tránsito, entre otros, incumpliendo así el desarrollo normal de las actividades programadas. El supervisor debe cumplir lo establecido por la ley para el desarrollo de sus funciones, así como por el Decreto 462 del 17 de septiembre de 2021 – "Por medio del cual se modifica el manual de funciones y/o actividades que deben cumplir los Interventores y/o Supervisores, para realizar en forma debida sus funciones como supervisor"

21. OBLIGACIONES DE LA ENTIDAD

Son obligaciones del DEPARTAMENTO, además de las consagradas en el artículo 4 de la ley 80 de 1.993, las propias del contrato tales como las siguientes:

1) Pagarle el valor del contrato en la forma y bajo las condiciones previstas.
2.) Ejercer la supervisión general del contrato.
3.) Formular las sugerencias por escrito sobre los asuntos que estime convenientes en el desarrollo del contrato, sin perjuicio de la autonomía propia del contratista.
4.) Solicitar al contratista informes sobre el desarrollo del contrato.
5.) Atender oportunamente las dudas e inquietudes del contratista en relación con el objeto del presente contrato.

22. OBLIGACIONES DEL CONTRATISTA

En desarrollo de la contratación a realizar, se debe tener en cuenta lo establecido para el efecto en el artículo 5 de la ley 80 de 1993 y cumplir con las siguientes obligaciones:

1. Acreditar estar al día en el sistema de seguridad social y parafiscales cuando corresponda, y cumplir con lo establecido en el artículo 50 de la ley 789 de 2002, la ley 828 de 2003, ley 797 de 2003, Decreto 510 de 2003 y artículo 23 de la ley 1150 de 2007
2. Desarrollar el objeto del Contrato, en las condiciones de calidad, oportunidad, y obligaciones definidas en el presente Contrato, incluyendo sus especificaciones Técnicas y sus Pliegos de Condiciones.
3. Colaborar con el DEPARTAMENTO en cualquier requerimiento que ella haga.
4. Garantizar la calidad de los bienes y servicios prestados, de acuerdo con las especificaciones Técnicas, el Pliego de Condiciones y la Oferta presentada
5. Dar a conocer al DEPARTAMENTO cualquier reclamación que indirecta o directamente pueda tener algún efecto sobre el objeto del Contrato o sobre sus obligaciones.
6. Comunicarle al DEPARTAMENTO cualquier circunstancia política, jurídica, social, económica, técnica, ambiental o de cualquier tipo, que pueda afectar la ejecución del Contrato.
7. Elaborar, suscribir y presentar al DEPARTAMENTO las respectivas Actas parciales las cuales deben estar aprobadas por el supervisor del Contrato, según corresponda.
8. Suministrar tanto en calidad, cantidad, como en tiempo, todos los equipos. Herramientas materiales y demás elementos necesarios para la ejecución del contrato.
9. Realizar por su cuenta y riesgo, todos los ensayos exigidos por ley y los que sean requeridos por la entidad y el supervisor y demás pruebas que se soliciten para verificar la calidad de los materiales y demás elementos necesarios para la ejecución del contrato.
10. Realizar los subcontratos necesarios, quedando claro que no existe ningún tipo de vínculo laboral del personal con DEPARTAMENTO
11. Presentar para aprobación del supervisor, actas parciales y final de la ejecución del contrato.
12. Responder por toda clase de demandas, reclamos o procesos que instaure el personal o los subcontratistas.
13. Responder por los gastos e impuestos que legalmente haya lugar para la legalización y ejecución del contrato, de conformidad con la normatividad que rige la materia.
14. Otorgar las pólizas dentro de los términos establecidos por la ENTIDAD.
15. Allegar los documentos requeridos para la legalización e iniciación del contrato, dentro del término establecido por la entidad.
16. Presentar la documentación requerida para acreditar el personal exigido en el pliego de condiciones, para la revisión y aprobación de la supervisión de la ENTIDAD como requisito de ejecución del contrato.

17. Atender en forma permanente la dirección de la ejecución del contrato, o mantener al frente del mismo un supervisor, el cual debe ser aceptado por el DEPARTAMENTO.
18. Ejecutar el contrato dando cumplimiento a las actividades, revisadas y aprobadas por el supervisor del DEPARTAMENTO.
19. Responder por todo daño que se cause a bienes, al personal que se utilice y a terceros en la ejecución del contrato, siempre que los mismos sean imputables al contratista.
20. Garantizar las normas de seguridad industrial para la ejecución del contrato en los siguientes aspectos: 1) Elementos de seguridad industrial para todo el personal que intervenga en la ejecución del contrato, 2) Manipulación de equipos, herramientas, combustibles y todos los elementos que se utilicen para cumplir el objeto y 3) Todo el contenido de seguridad industrial debe acogerse a las normas vigentes.
21. Realizar la señalización de los lugares y maniobras peligrosas, avisos y carteles expresivos de las normas adoptadas.
22. Responder por la buena calidad de los materiales y elementos utilizados en el objeto del contrato.
23. Aceptar el control y acatar las órdenes e instrucciones del supervisor del contrato.
24. El Contratista proveerá las condiciones de seguridad necesarias, para que el Supervisor, el departamento y los entes de control puedan inspeccionar las actividades ejecutadas en cualquier momento durante la ejecución del contrato, sin costo adicional para El Contratante.
25. Cumplir con las normas y especificaciones técnicas.
26. Ejecutar el objeto contractual observando el plan de calidad, con el fin de desarrollar acciones planificadas para la ejecución en debida forma del proyecto. El plan de calidad para el fin del contrato es el documento que refleja la aplicación de criterios de calidad al proyecto específico.
27. Hacer un archivo del contrato, el cual debe estar a disposición del DEPARTAMENTO y de los entes de control.
    a) Presentar informes mensuales, los cuales deberán ser aprobados por el supervisor.
    b) Acreditación, de acuerdo con lo establecido en el inciso segundo del artículo 41 de Ley 80 de 1993, adicionado mediante el artículo 23 de la Ley 1150 de 2007, que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios al Servicio Nacional de Aprendizaje - SENA, Instituto Colombiano de Bienestar Familiar - ICBF y las cajas de compensación familiar, cuando corresponda.
28. Presentar informe final, el cual deberá ser aprobado por el supervisor y contener como mínimo:
    a) Resumen de actividades y desarrollo de la ejecución del contrato.
29. Las obligaciones específicas contempladas en el anexo técnico adjunto al presente estudio previo.
30. Las demás inherentes al contrato para su ejecución en debida forma, así como las contenidas en el Pliego de Condiciones y que no hayan sido incluidas en los numerales anteriores.

23. ANEXOS AL PRESENTE DOCUMENTO.

- Los mencionados en los apartados del contenido.

En consecuencia, se:

CONCLUYE QUE:

Resulta procedente iniciar los trámites inherentes al proceso de selección de contratista en la modalidad de LICITACIÓN PÚBLICA para la contratación del **PRESTACIÓN DE SERVICIO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, MONITOREO DE INCIDENTES DE SEGURIDAD Y ATENCIÓN CORRECTIVA A INCIDENTES DE LA GOBERNACIÓN DE SANTANDER, EN EL MARCO DEL PROYECTO DE IMPLEMENTACIÓN DE ACCIONES PARA EL ASEGURAMIENTO TECNOLÓGICO Y LA TRANSFORMACIÓN DIGITAL EN EL DEPARTAMENTO DE SANTANDER.** para lo cual se atenderán los parámetros establecidos en el presente estudio previo, sin embargo, la prioridad y condiciones del mismo serán establecidas según instrucciones del señor Gobernador de Santander.

ORIGINAL FIRMADO

SHIRLEY PAOLA CASTELLANOS MARTINEZ
Secretaria TIC del Departamento de Santander

Proyecto aspectos Jurídicos: Lizeth Stefany Bohorquez Pedraza – Abog Sec TIC
Proyectó Estudios del Sector : Jaime Palacios – Contratista Oficina Contratación
Proyectó Aspectos Técnicos: Carolina Toledo Bueno – Directora de Gobierno Digital (E)
Estructuradora del Proyecto: Astrid Victoria Cárdenas Chicangana- Ingeniera de Sistemas -CPS

ANEXO
FICHA TÉCNICA DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD
GOBERNACIÓN DE SANTANDER

OBJETO CONTRACTUAL

OBJETO: PRESTAR EL SERVICIO INTEGRAL DE TELECOMUNICACIONES, SEGURIDAD DIGITAL, SOPORTE TÉCNICO Y ADQUISICIÓN E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE NETWORKING I PARA LA GOBERNACION DE SANTANDER DE ACUERDO CON LOS REQUERIMIENTOS TÉCNICOS DEFINIDOS

Las características descritas en este anexo corresponden a los requisitos consignados en las nueve secciones de la ficha técnica ajustada. La columna de verificación se deja como espacio de diligenciamiento contractual; no constituye declaración de cumplimiento comprobado.

1. 1. PROTECCIÓN DE APLICACIONES Y PORTALES WEB – SERVICIO EN LA NUBE (Relación item 1)

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	Implementar y operar un servicio administrado de seguridad de aplicaciones web en la nube para tres (3) sitios web públicos de la entidad, incluyendo puesta en funcionamiento, parametrización, monitoreo, soporte y actualizaciones durante el plazo contractual.		
2	El servicio deberá permitir la incorporación y protección efectiva de tres (3) aplicaciones o sitios web públicos, cada uno con configuración de dominio, políticas de seguridad y certificados TLS según corresponda.		
3	La solución deberá contemplar un volumen agregado de transferencia de al menos trescientos (300) GB mensuales entre los tres sitios protegidos. El contratista deberá acreditar que el plan comercial y sus condiciones de uso admiten dicho volumen.		
4	La capacidad inicial contratada para los tres portales será de al menos veinticinco (25) Mbps compartidos; antes de la puesta en producción, el contratista deberá validar que cubre el tráfico real y los picos operativos de la entidad y gestionar la ampliación necesaria sin interrupción del servicio.		
5	La solución deberá incorporar un firewall de aplicaciones web con inspección de tráfico HTTP/HTTPS y mecanismos de prevención de amenazas contempladas por OWASP, incluyendo inyección SQL, XSS, inclusión de archivos, manipulación de parámetros, acceso indebido y otras amenazas de aplicación.		
6	Se deberán aplicar actualizaciones periódicas de firmas, indicadores y mecanismos de detección de amenazas, incluidos patrones novedosos y actividades anómalas, durante toda la vigencia del servicio.		
7	El servicio deberá ofrecer mitigación de ataques de denegación de servicio de red y de aplicación, incluyendo L3/L4 y L7, y ataques HTTP/HTTPS, con controles de tasa, reputación y bloqueo según políticas.		
8	Se deberá incluir una red de distribución de contenidos (CDN) que permita la distribución y aceleración de contenido cacheable, con política de caché configurable, manejo de certificados y purga o invalidación según funciones del servicio.		
9	El servicio deberá incluir detección y mitigación avanzada de tráfico automatizado malicioso, bots, abuso de credenciales y automatización de solicitudes; deberá soportar políticas de desafío, mitigación o bloqueo.		
10	La protección deberá contar con análisis adaptativo del tráfico y mecanismos de detección de anomalías mediante analítica o aprendizaje automático para contribuir a la reducción de falsos positivos.		
11	Deberá permitir políticas por direcciones IP, rangos, reputación, geolocalización, métodos HTTP, rutas, patrones de solicitudes, límites por frecuencia y listas de autorización y bloqueo.		

ID	REQUISITO TÉCNICO	SI	NO
12	Deberá permitir la protección de aplicaciones publicadas mediante HTTPS y protocolos web modernos, utilizando certificados digitales válidos y configuraciones criptográficas seguras.		
13	La solución deberá operar delante de los servidores de origen mediante un esquema de protección cloud compatible con la publicación DNS y el enrutamiento a los orígenes, sin exigir la instalación de un dispositivo WAF físico en la entidad.		
14	Deberá permitir gestión de orígenes y opciones de continuidad del servicio disponibles en el plan contratado; cualquier balanceo global o conmutación automática se acreditará expresamente según la modalidad contratada.		
15	Deberá ofrecer registros de eventos, alertas, tableros e informes sobre tráfico, ataques bloqueados, mitigación DDoS y actividad de bots; los mecanismos de integración o exportación al monitoreo central se documentarán durante la implementación.		
16	Deberá permitir integrar o exportar eventos de seguridad al sistema de monitoreo y correlación de la entidad mediante los mecanismos soportados, incluyendo especificación de formato, periodicidad, límites y costos si corresponden.		
17	La retención de registros deberá ajustarse a lo definido en el pliego. Si el servicio no cuenta nativamente con el plazo requerido, el contratista deberá entregar un mecanismo de exportación o conservación externa que cumpla el requisito.		
18	El contratista deberá configurar perfiles, políticas, excepciones controladas, usuarios administradores, alertas y procedimientos para minimizar falsos positivos y evitar afectación innecesaria de la operación.		
19	Previo a la recepción, deberán verificarse para los tres portales la inspección HTTPS, el bloqueo de amenazas de prueba, mecanismos de bots, reglas de acceso, eventos, funcionamiento CDN y activación de protección DDoS conforme al servicio contratado.		
20	El servicio deberá incluir soporte técnico especializado, actualizaciones y acompañamiento del contratista durante la vigencia contractual, con canales, horarios, escalamiento y tiempos de atención conforme al acuerdo de niveles de servicio.		
21	Se entregarán documento de arquitectura, inventario de dominios y orígenes, configuración de políticas, actas de pruebas, procedimientos de administración, escalamiento, respaldo de configuraciones cuando aplique y capacitación al personal designado.		
	Características mínimas de la solución WAF		
22	La capacidad inicial contratada para los tres portales será de al menos veinticinco (25) Mbps compartidos; antes de la puesta en producción, el contratista deberá validar que cubre el tráfico real y los picos operativos de la entidad y gestionar la ampliación necesaria sin interrupción del servicio.		
23	El servicio deberá permitir la incorporación y protección efectiva de tres (3) aplicaciones o sitios web públicos, cada uno con configuración de dominio, políticas de seguridad y certificados TLS según corresponda.		
24	Se deberá incluir una red de distribución de contenidos (CDN) que permita la distribución y aceleración de contenido cacheable, con política de caché configurable, manejo de certificados y purga o invalidación según funciones del servicio.		
25	El servicio deberá ofrecer mitigación de ataques de denegación de servicio de red y de aplicación, incluyendo L3/L4 y L7, y ataques HTTP/HTTPS, con controles de tasa, reputación y bloqueo según políticas.		
26	La retención de registros deberá ajustarse a lo definido en el pliego. Si el servicio no cuenta nativamente con el plazo requerido, el contratista deberá entregar un mecanismo de exportación o conservación externa que cumpla el requisito.		
	Funcionalidades de Web Application Firewall:		
27	Debe tener soporte nativo de HTTP/2		
28	El servicio deberá admitir tráfico web moderno, incluida la compatibilidad de protocolos HTTP/HTTPS soportados por los portales protegidos.		

ID	REQUISITO TÉCNICO	SI	NO
29	Deberá soportar interoperabilidad con OpenAPI 3.0		
30	Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de vírus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica		
31	El servicio deberá permitir administrar políticas de reputación, firmas y amenazas actualizadas, aplicadas a los sitios protegidos.		
32	Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no		
33	Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial		
34	Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formulários y lo que se espera de cada campo		
35	El perfil aprendido de forma automática debe de poder ser ajustado		
36	Tener la capacidad de creación de firmas de ataques customizables		
37	La solución deberá contar con mecanismos de mitigación de automatización maliciosa y bots, según las políticas contratadas.		
38	Tener la capacidad de proteción contra ataques del tipo Botnet		
39	Tener la capacidad de proteción contra ataques del tipo Browser Exploit Against SSL/TLS (BEAST)		
40	La solución debe tener funcionalidad de proteción contra ataques como acceso por fuerza bruta		
41	Debe soportar detección de ataques de Clickjacking		
42	Debe soportar detección de ataques de cambios de cookie		
43	Identificar y proteger contra ataques del tipo Credit Cart Theft		
44	Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF)		
45	La solución debe tener funcionalidad de proteción contra ataques como cross site scripting (XSS)		
46	Debe tener proteción contra ataques de Denial of Service (DoS);		
47	Tener la capacidad de proteción contra ataques del tipo HTTP header overflow		
48	Tener la capacidad de proteción contra ataques del tipo Local File inclusion (FLI)		
49	Deberá mitigar ataques de denegación de servicio dirigidos a la aplicación web mediante las capacidades de la plataforma distribuida.		
50	Tener la capacidad de proteción contra ataques del tipo Remote File Inclusion (RFI)		
51	Tener la capacidad de proteción contra ataques del tipo Server Information Leakage		
52	Proteción contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection);		
29	Tener la capacidad de proteción contra ataques del tipo Malformed XML		
53	Identificar y prevenir ataques del tipo Low-rate DoS		
54	Prevención contra Slow POST attack		
55	Proteger contra ataques Slowloris		
56	La solución deberá mitigar ataques de denegación de servicio de red y de aplicación mediante los mecanismos contratados y documentados.		
57	Tener la capacidad de proteción contra ataques del tipo Forms Tampering		
58	La solución debe tener funcionalidad de proteción contra ataques de manipulación de campos ocultos		
59	Tener la capacidad de proteción contra ataques del tipo Directory Traversal		
60	Tener la capacidad de proteción del tipo Access Rate Control		
61	Identificar y proteger contra Zero Day Attacks		
62	La mitigación de DDoS volumétrico deberá prestarse mediante la infraestructura distribuida del servicio cloud, sin exigir mecanismos propios de un dispositivo local.		

ID	REQUISITO TÉCNICO	SI	NO
63	Permitir configurar reglas de bloqueo a métodos HTTP no deseados		
64	Permitir que se configuren reglas de limite de upload por tamaño del archivo		
65	Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de direción IP correspondientes a cada país		
66	Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado		
67	Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en direción IP de origen		
68	Permitir la liberación temporal o definitiva (white-list) de direciones IP bloqueadas por tener originado ataques detectados por la solución		
69	Debe permitir añadir, automaticamente o manualmente, en una lista de bloqueo, las direciones IP de origen, según la base de IP Reputation		
70	La solución deberá disponer de controles de abuso de autenticación y mitigación de solicitudes automatizadas cuando tales funciones estén disponibles en la modalidad contratada.		
71	Tener la capacidad de prevención contra pérdida de información (DLP), bloqueando la pérdidade información del encabezado HTTP		
72	La solución deberá permitir detectar alteraciones sospechosas y generar alertas de integridad o cambios en el sitio; la recuperación automática de contenidos requerirá un mecanismo específico contratado.		
73	Tener la funcionalidad de antivírus integrada para inspeción de tráfico y archivos, sin la necesidad de instalación de otro equipo		
74	Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado		
75	El servicio deberá gestionar el tráfico HTTPS seguro y la terminación TLS compatible con la publicación de los portales.		
76	La solución podrá terminar conexiones TLS conforme a las políticas de cifrado aprobadas por la entidad.		
77	La solución deberá soportar versiones vigentes y seguras de TLS, evitando requerir protocolos obsoletos e inseguros.		
78	La solución debe tener la capacidad de almacenar certificados digitales de CA's		
79	La solución debe de ser capaz de generar CSR para ser firmado por una CA		
80	La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL		
81	La solución debe contener las firmas de robôs conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de contról de acceso, así como resetear dichas conexiones		
82	La solución debe de tener un sistema de bloque con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación debe de ser actualizado automaticamente.		
83	La solución deberá contemplar controles de disponibilidad del origen y limitación de solicitudes, de acuerdo con las capacidades del plan contratado.		
84	La solución debe permitir la customización o reenvío de solicitaciones y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location		
85	La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).		
86	La solución debe de tener la capacidad de definir restrición a determinados métodos HTTP		
87	La solución debe tener la capacidad de proteger contra detección de campos ocultos		
88	Permitir que se configuren firmas customizadas de ataques y DLP, a través de expresiones regulares		

ID	REQUISITO TÉCNICO	SI	NO
89	Deberá poder utilizar informes de vulnerabilidades como insumo para ajustar las políticas de protección de aplicaciones, cuando las funciones contratadas lo permitan.		
90	Deberá permitir parametrizar reglas de protección a partir de vulnerabilidades detectadas y evidencias de riesgo.		
91	La entidad podrá realizar verificaciones periódicas de seguridad de los portales mediante herramientas complementarias contratadas.		
92	Se entregarán reportes de eventos de seguridad, amenazas detectadas y bloqueos por aplicación protegida.		
93	Soportar redireción y reescritura de requisiciones y respuestas HTTP		
94	Permitir redireción de requisiciones HTTP para HTTPS		
95	Permitir reescribir la línea URL del encabezado de una requisición HTTP		
96	Permitir reescribir el campo HOST del encabezado de una requisición HTTP		
97	Permitir reescribir el campo REFERER del encabezado de una requisición HTTP		
98	Permitir redirigir requisiciones para otro website		
99	Permitir enviar respuesta HTTP 403 Forbidden para requisiciones HTTP		
100	Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redireción HTTP de un servidor web		
101	Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web		
102	Permitir añadir el campo X-Forwarded-For para identificación de la direción IP real del cliente cuando en modo proxy reverso		
103	La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL y origen de la petición y, si necesario, aplicar una tasa específica de velocidad (rate limit).		
104	La solución debe de soportar combinación de contról de acceso y autenticación utilizando mecanismos como HTML Form, Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas y integración de los usuários de la aplicación		
105	Se deberá incluir una red de distribución de contenidos (CDN) que permita la distribución y aceleración de contenido cacheable, con política de caché configurable, manejo de certificados y purga o invalidación según funciones del servicio.		
106	Se deberán aplicar actualizaciones periódicas de firmas, indicadores y mecanismos de detección de amenazas, incluidos patrones novedosos y actividades anómalas, durante toda la vigencia del servicio.		
	Admnistración y Gestion de la Plataforma		
106	La administración deberá realizarse mediante interfaz segura de gestión, con control de acceso para operadores autorizados.		
107	El servicio deberá contar con medidas de disponibilidad y continuidad propias de su arquitectura cloud; las funciones de redundancia de origen se acreditarán según plan contratado.		
108	Deberá contar con API por medio del método RESTful sobre HTTPS.		
109	La solución deberá contar con dashboards, que muestren como mínimo información en tiempo real del tráfico, Historia de Ataques, sesiones por política e información del sistema.		
110	Deberá permitir la administración diferenciada de políticas para los tres portales protegidos.		
111	La solución deberá proporcionar consola web segura para administrar políticas, eventos y configuraciones.		
112	Debe soportar administración por interfaz web segura HTTPS.		
113	La administración se efectuará por interfaces seguras habilitadas por el proveedor del servicio; no se exigirá Telnet.		
114	El sistema ofrecerá medios documentados para la gestión y configuración de políticas, según capacidades de la plataforma.		
115	El sistema dispondrá de documentación y ayuda administrativa para la operación de las políticas.		

ID	REQUISITO TÉCNICO	SI	NO
116	El panel deberá mostrar información del estado de protección, tráfico, ataques y configuración de las aplicaciones protegidas.		
117	La consola deberá permitir conocer la vigencia de la suscripción, capacidad contratada y estado de la protección.		
118	La administración deberá poder realizarse por consola web y/o API disponibles en el servicio, sin exigir CLI de appliance.		
119	La plataforma deberá facilitar métricas del consumo de servicio y de los eventos de seguridad por aplicación.		
120	Deberá permitir consultar estadísticas y capacidad de uso del servicio, según los informes disponibles.		
121	Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados		
122	Dede proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de requisición HTTP en tiempo real y los últimos logs de eventos del sistema		
123	El panel deberá facilitar estadísticas de tráfico HTTP/HTTPS, ataques y eventos por aplicación.		
124	Deberá visualizar el estado de las aplicaciones protegidas y las políticas activas, sin exigir interfaces de red físicas.		
125	La configuración de administración de la solución debe permitir la utilización de perfiles		
126	El contratista deberá documentar y respaldar la parametrización de reglas mediante mecanismos de exportación soportados.		
127	El resguardo de configuraciones y credenciales deberá realizarse de forma segura y bajo control de acceso.		
128	El contratista deberá entregar copia documental de la configuración disponible en el servicio contratado.		
129	La recuperación de políticas deberá atender a los mecanismos de respaldo y restauración disponibles en la plataforma.		
130	El servicio incorporará actualizaciones administradas sin exigir pruebas de firmware local en memoria RAM.		
131	Las actualizaciones y continuidad del servicio se regirán por los procesos de operación de su infraestructura cloud.		
132	Los mecanismos de monitoreo e integración deberán estar documentados y disponibles mediante interfaces seguras.		
133	La solución deberá generar alertas de seguridad y permitir su transmisión a los canales e integraciones soportados.		
134	La plataforma deberá conservar y/o exportar registros de seguridad conforme a la política de retención definida contractualmente.		
135	Cuando el plazo de retención nativo sea insuficiente, el contratista deberá habilitar conservación externa o exportación verificable.		
136	La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías		
137	La solución debe tener datos analíticos conteniendo la localización geográfica de los clientes web		
138	La solución debe tener datos analíticos, siendo posible visualizar el total de ataques y porcentaje de cada país de origen, el volumen total de tráfico en bytes y porcentaje de cada país de origen, y el total de accesos (hits) y porcentaje de cada país de origen		
139	Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario		
140	La integración mediante API se efectuará conforme a las funciones y límites de acceso habilitados en el servicio.		
141	Las funciones de gestión deberán protegerse mediante autenticación segura de administradores y roles autorizados.		
142	Las funciones administrativas deberán disponer de controles de autenticación y autorización documentados.		

ID	REQUISITO TÉCNICO	SI	NO
143	Deberán mantenerse credenciales administrativas y certificados bajo controles apropiados.		
144	Los accesos de administración se asignarán mediante identidades y permisos autorizados por la entidad.		
145	Cuando esté disponible, la consola podrá integrarse con el servicio de identidad corporativo conforme al plan.		
146	La gestión de acceso deberá aplicar autenticación segura sin exigir protocolos heredados específicos.		
147	La solución deberá permitir asignar roles o perfiles para segregar tareas de operación y administración.		
148	Debe soportar CAPTCHA y Real Browser Enforcement (RBE)		
149	Deberá soportar autenticación reforzada de cuentas administrativas según las capacidades de la plataforma.		
	Administración y Gestión de la Plataforma		
150	La solución deberá incluir los servicios de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, realizada por ingenieros certificados por el proveedor de la solución de los equipos. El contratista deberá presentar las respetivas certificaciones del grupo de trabajo asignado expedidas por el proveedor de la solución de los equipos.		
151	La implementación estará a cargo de personal idóneo y certificado, con experiencia acreditable en seguridad de aplicaciones web y servicios cloud, conforme a los perfiles exigidos por la entidad.		
	Plan de Trabajo		
152	El contratista deberá presentar máximo dos (2) días hábiles luego de firmada el acta de inicio las hojas de vida y certificaciones del personal que realizará la implementación y el plan de trabajo detallado en el cual se describa el componente de diseño de la seguridad perimetral incluyendo los equipos que actualmente cuenta la entidad, adicionalmente se debe tener en cuenta los procesos/actividades inherentes para alcanzar el objeto de la solución, explicando claramente el número de días de la actividad y profesionales dedicados para desarrollar cada actividad relacionada en el cronograma, que incluya, entre otros, actividades, fechas de inicio y terminación, hitos y ruta crítica. La secuencia y duración de cada una de las actividades debe estar discriminada en semanas. Este plan de trabajo será de obligatorio cumplimiento durante la ejecución del contrato, previa aprobación del Supervisor del Contrato.		
	Garantia Y Soporte		
153	El oferente deberá prestar el servicio de soporte para apertura de casos de cualquier criticidad a través de una mesa de Ayuda, vía telefónica o vía correo electrónico. Por ambos medios la atención de incidentes estará disponible en horario 7x24x365.		
154	El contratista deberá registrar, gestionar y hacer seguimiento a cualquier incidente reportado por el la Entidad, además durante la atención inicial del caso se determinará su criticidad y la metodología para su resolución.		
155	Niveles de Atención que debe prestar el contratista: * Un primer nivel de atención con Agente Nivel I de la Mesa de Ayuda a través de la ejecución de un checklist, en conjunto con la Entidad, y la validación del respectivo problema. * Si la incidencia no es resuelta se deberá asignar un Ingeniero de Soporte de Nivel II para proceder con la atención remota o en sitio del incidente. * Si la incidencia persiste, el Ingeniero de Soporte de Nivel II procederá a gestionar la apertura de un ticket con el TAC del proveedor de la solución para dar pronta solución al incidente.		
156	El soporte requerido para la solución ofertada deberá ser provisto por el contratista durante el tiempo de garantía ofrecido.		
157	El contratista deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la Entidad así lo requiera), este soporte deberá ser suministrado por personal especializado en la herramienta.		
	Transferencia de Conocimiento		

ID	REQUISITO TÉCNICO	SI	NO
158	El contratista deberá realizar transferencia de conocimiento durante mínimo cuatro (4) horas a tres (3) ingenieros del Grupo de TIC, designados por el Supervisor del contrato, orientada a la instalación, configuración, parametrización y puesta en marcha de la solución, que brinde el conocimiento necesario para la administración y operación del hardware y software de la solución de seguridad implementada.		
159	La transferencia de conocimiento se podrá realizar durante la instalación, configuración, parametrización y puesta en funcionamiento la solución.		
160	Previo al inicio de actividades, el contratista deberá hacer entrega del documento de Plan de Transferencia de conocimiento en el cual se debe describir el mecanismo a utilizar para dicha actividad, de tal manera que se logre efectuar un aprovechamiento óptimo del software, de los equipos y de la tecnología.		
	DOCUMENTACION		
161	El contratista debe adjuntar los folletos, catálogos u hojas de especificaciones técnicas de los productos y servicios ofrecidos.		
162	El contratista debe documentar todos los procedimientos realizados para la instalación, configuración y parametrización de cada una de las funcionalidades implementadas y entregarlos en medio magnético e impreso, una vez revisados y aprobados por el Supervisor del contrato.		
163	Al finalizar la puesta en funcionamiento de la solución contratada, debe entregar en medio magnético e impreso, la documentación que permita la eficiente administración del firewall, como mínimo incluir: * Manual de procedimientos de administración y operación de los appliances. * Documento de descripción de la configuración de appliance y parámetros de configuración inicial de todo el software instalado. * Documentación de la topología de la solución implementada.		

2. 2. Sistema de Gestión de Información y Eventos de Seguridad (SIEM) (Security Information and Event Management SIEM) (Relación item 2)

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO		
1	El sistema de correlacionador de eventos deberá soportar la totalidad de las licencias adquiridas y permitir la integración correcta con los demás dispositivos de la infraestructura de la Entidad.		
2	Suministro de una plataforma del tipo Next Generation - Security Information and Event Manager (SIEM) que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la Entidad, así como monitorear las disponibilidades de los servicios y las plataformas TI.		
3	(1) Un dispositivo (appliance Fisico de propósito específico) de la misma referencia, debidamente licenciados para el cubrimiento de los requerimientos del presente anexo. Los dispositivos serán instalados en el data.center de la Entidad. No se aceptan soluciones en nube, ni que los logs de eventos deban salir en ningún momento de la entidad.		
4	Los componentes que integran la solución no deben aparecer en listas end-of-life ó end-of-sale del fabricante.		
5	La plataforma debe Colectar los eventos de seguridad de múltiples marcas para lo cual se debe incluir el licenciamiento necesario para esto.		
6	La plataforma debe tener la capacidad de comportarse como una herramienta del tipo “base de datos de la gestión de configuración” o CMDB.		
7	La plataforma debe monitorear los cambios en los archivos de configuración de los servidores que la Entidad defina.		
8	La plataforma debe contar con licenciamiento a suscripción y Actualizaciones Periódicas de Software (EPS) , asegurando el acceso y las actualizaciones continuas sin necesidad de renovaciones adicionales.		
	CARACTERISTICAS MINIMAS		
9	Cantidad de dispositivos a correlacionar: 150		
10	Cantidad de eventos por segundo: 3000		

ID	REQUISITO TÉCNICO		
11	La solución debe contar con un sistema de bases de datos hibrida, lo que quiere decir que esté basado en NoSQL (BigData) y SQL, no se aceptan soluciones basadas únicamente en motores de bases de datos del tipo SQL, esto con el fin de asegurar que la solución soporte grandes volúmenes de datos sin afectar la estabilidad de la solución.		
12	Por temas de estrategia TI de la Entidad, se requiere que la solución cuente con características “Multitenencia” o multi- tenancy.		
13	La plataforma al ser un SIEM de nueva generación Debe contar con características conjuntas de NOC y SOC, por lo cual Debe realizar:		
14	Actualización constante de la base de datos de contextos, configuraciones, software instalado y servicios corriendo de los dispositivos monitoreados.		
15	Análisis constante el desempeño de las aplicaciones lo cual permita realizar un triage de la seguridad.		
16	Visor personalizado de log de tráfico.		
17	Herramienta de búsqueda sobre los logs de tráfico.		
18	Para garantizar que el futuro contrarista tenga las mejores prácticas en sus actividades de implementación y soporte, el futuro contratista deberá estar certificado en la normas ISO27001:2013 e ISO 20000-1:2018.		
19	El oferente también debe pertenecer a grupos de respuesta como CSIRT.		
	CARACTERISTICAS DE MONITOREO Y DISPONIBILIDAD		
20	Debe tener la capacidad de Colectar las versiones del software instalado en los dispositivos monitoreados, almacenado en un repositorio de versiones.		
21	Debe contar con la característica de detección automática de los cambios en la configuración de red de las plataformas monitoreadas.		
22	Debe contar con la característica de detección automática de cambios en el software instalado en las plataformas monitoreadas.		
23	Debe contar con la característica de detección automática en cambios en archivos y carpetas, de las plataformas Windows y Linux monitoreadas, donde se detalle el “Quien” y el “Que”.		
24	Debe contar con la característica de detección automática basada en agente, de cambios en el registro de los sistemas Windows monitoreados.		
25	Debe contar con la característica de Monitoreo del sistema vía SNMP, WMI y PowerShell.		
26	Debe contar con la característica de Monitoreo de aplicaciones vía JMX, WMI y PowerShell.		
27	Debe contar con la característica de Monitoreo de Hipervisor tales como VMWARE.		
28	Debe poder Monitorear plataformas de almacenamiento tales como EMC, NetAPP, etc, a nivel de desempeño y uso de almacenamiento.		
29	Debe poder Monitorear sistemas del tipo Directorio Activo y Exchange basado en WMI y PowerShell.		
30	La solución propuesta debe permitir el escaneo periódico de los archivos contenidos en el dispositivo con el agente instalado.		
31	Debe poder Monitorear motores de Bases de datos SQL Server, Oracle, MySQL entre otras vías JDBC.		
32	Debe poder Monitorear Infraestructura VoIP vía IPSLA, SNMP, CDR y CMR.		
33	Debe realizar Análisis del desempeño y flujo de las aplicaciones vía NetFlow, Sflow, Cisco AVC y NBAR.		
34	La solución propuesta debe poder evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos.		
35	Debe tener la capacidad de definir métricas definidas por el usuario.		
36	Debe tener la Capacidad de detectar desviaciones de una línea base de la infraestructura monitoreada.		
37	Debe tener la Capacidad de monitorear dispositivos del entorno tales como Liebert UPS, HVAC, FPC y APC.		
38	Debe monitorear las caídas y reinicios de los sistemas vía Ping, SNMP, WMI, así como análisis del reinicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage.		

ID	REQUISITO TÉCNICO		
39	Debe hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace		
40	route y puertos TCP/UDP genéricos.		
41	Debe hacer detección de comportamiento anómalo de usuarios usando técnicas de machine learning.		
	PROTOCOLOS DE CONEXIÓN		
42	Web – HTTP/HTTPS,		
43	DNS, FTP/SCP, Generic TCP/UDP, ICMP, IMAP4, JDBC, LDAP, POP3, POP3S		
44	SMTP, SOAP, SSH, Telnet/SSH, SNMP, WMI, JMX.		
	CARACTERISTICAS DE ANALISIS SEGURO		
45	Debe soportar la Correlación de Eventos de múltiples fuentes, tales como Firewalls, UPS, Servidores, estaciones de trabajo entre otros.		
46	Debe soportar Correlación cruzada de eventos.		
47	Integración por medio de API's con fuentes de información externa sobre amenazas, tales como Dominios de Malware, IPs, URLs, Hash y Nodos de Tor.		
48	Integración Nativa con fuentes de información de terceros tales como ThreatStream, CyberArk, SANS y Zeus.		
49	de los laboratorios de inteligencia del fabricante, por el período de soporte contratado.		
50	Capacidad de hacer Monitoreo de la Integridad de Archivos o FIM basada en agente Windows.		
51	Debe tener la capacidad de modificar los parsers por medio de interface gráfica, sin que esta modificación afecte la colección de logs o genere caídas en los servicios de la solución.		
52	Debe permitir la creación de Parsers customizados a partir de platillas XML.		
53	Debe tener la capacidad de Colectar logs de forma segura, desde dispositivos remotos.		
54	Debe contar con un framework de notificación de incidentes el cual Debe estar basado en políticas.		
55	Debe tener la capacidad de ejecutar scripts de remediación cuando un incidente ocurra. Debe contar con scripts de remediación predefinidos que involucren al menos las plataformas de Firewall de Nueva Generación con las que cuenta la Entidad, además de la capacidad de definir scripts nuevos.		
56	Debe contar con un sistema propio de tickets.		
57	Debe tener la capacidad de integrarse con sistemas de tickets externos en caso que la Entidad lo requiera, dicha integración deberá ser por API.		
58	Debe ser capaz de detectar anomalías en la línea base definida.		
59	La detección de incidentes deberá ser en tiempo real anterior al almacenamiento del evento, utilizando técnicas del tipo "Correlación Distribuida".		
60	Debe contar con una consola de visualización de logs y eventos correlacionados la cual cuente con un sistema para el filtrado de los mismos por medio de condiciones Boleanas.		
61	Debe poder realizarse filtros por medio de expresiones regulares.		
62	El reporte de incidentes debe poder ser priorizado por los servicios críticos.		
63	Debe permitir la identificación dinámica de usuarios.		
	CARACTERISTICAS DE ADMINISTRACION Y REPORTES		
64	La plataforma deberá poder ser administrada vía HTTPS.		
65	La plataforma deberá tener una consola del tipo dashboard en la cual se pueda personalizar varios tipos de gráficas y tablas, lo cual permita tener una visión global de los incidentes de seguridad.		
66	La comunicación de los módulos debe ser asegurada por temas de confidencialidad por medio de HTTPS.		
67	Debe contar con un módulo para el cálculo de los SLA.		
68	Debe contar con un dashboard que permita identificar en un mapa los incidentes y su ubicación geográfica.		
69	Debe contar con un módulo para administrar las políticas de correlación.		

ID	REQUISITO TÉCNICO		
70	Debe contar con un módulo para la administración de los agentes, el cual debe recibir datos de uno o varios colectores de software en caso de ser requerido, cuyos recursos de software serán suministrados por la Entidad con las siguientes características máximas: 2 vCPU, 6 GB en RAM, 240 GB en disco.		
71	Deberá contar con un módulo de administración para la característica de “base de datos de la gestión de configuración” o CMDB, sin requerir de software o hardware adicional.		
72	La plataforma debe tener un gran número de reportes predefinidos y deberá permitir crear reportes customizados.		
	LUGAR DE INSTALACION		
70	Centro de datos de la Entidad, en el ambiente de FISICO que se designe por parte de la Gobernación.		
71	un (1) año con servicio de soporte y mantenimiento en sitio, incluyendo repuestos, licencias, actualizaciones y configuraciones.		
72	Se debe hacer mantenimiento del sistema semestralmente durante el tiempo de la garantía.		
73	En caso de daño del SIEM debe cambiarse por otro nuevo y actualizado. El tiempo máximo de atención por una falla es de 12 horas y el de reparación o sustitución es de 10 dias.		
74	El SIEM con las licencias adquiridas se entregarán debidamente instalados y operativos y se realizarán los trabajos de mantenimiento correspondientes en el datacenter de la Entidad en la ciudad de Bogotá D.C.,		
75	En la oferta quedan incluidos todos los costos de transporte, logística, instalación y garantías necesarios, los impuestos a que haya lugar, así como el mantenimiento.		
	SERVICIOS PROFESIONALES		
76	La solución deberá incluir los servicios de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, realizada por ingenieros certificados por el fabricante de los equipos. El contratista deberá presentar las respetivas certificaciones del grupo de trabajo asignado expedidas por el fabricante de los equipos.		
77	La implementación de este proyecto será exclusiva para empresas que pertenezcan al nivel máximo de membresía del fabricante y que formen parte del programa de socios de servicios preferentes (EPSP).		
	IMPLEMENTACION		
4	Planeación de cada una de las actividades con el fin de disminuir los tiempos de afectación en el servicio.		
5	Presentar diseño de seguridad perimetral de acuerdo a buenas prácticas y recomendaciones del fabricante integrando los dispositivos de seguridad con los que actualmente cuenta la entidad, este será evaluado y aprobado por el supervisor de contrato.		
6	Presentar el diseño de Políticas de Seguridad para ser evaluado y aprobado por el líder de infraestructura y el supervisor del contrato.		
7	Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.		
8	Implementación de la solución de acuerdo a las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura.		
9	Pruebas de Servicio de las plataformas ofertadas.		
10	Puesta en Producción de las plataformas ofertadas.		
11	Estabilización de las plataformas ofertadas.		
12	Entrega a satisfacción de la entidad.		
13	Dentro de los servicios se debe tener en cuenta el diseño, Instalación, configuración y puesta en producción de los dispositivos de seguridad que actualmente cuenta la Entidad, así como la entrega a satisfacción de los mismos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para el cliente.		

ID	REQUISITO TÉCNICO		
14	La entidad requiere la implementación y puesta en marcha de las plataformas ofertadas, así como la configuración de políticas, objetos y demás configuraciones a que haya lugar para dejar las misma totalmente operativas y a satisfacción de la entidad, así como realizar pruebas de detección de cada una para validar su correcta configuración de acuerdo a las buenas prácticas de implementación del fabricante.		
15	El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, Entre otros) requerida para que el personal asignado al proyecto, pueda cumplir sus funciones.		
	GARANTIA Y SOPORTE		
16	El oferente deberá prestar el servicio de soporte para apertura de casos de cualquier criticidad a través de una mesa de Ayuda, vía telefónica o vía correo electrónico. Por ambos medios la atención de incidentes estará disponible en horario 7x24x365.		
17	El contratista deberá registrar, gestionar y hacer seguimiento a cualquier incidente reportado por el la Entidad, además durante la atención inicial del caso se determinará su criticidad y la metodología para su resolución.		
18	Niveles de Atención que debe prestar el contratista: * Un primer nivel de atención con Agente Nivel I de la Mesa de Ayuda a través de la ejecución de un checklist, en conjunto con la Entidad, y la validación del respectivo problema. * Si la incidencia no es resuelta se deberá asignar un Ingeniero de Soporte de Nivel II para proceder con la atención remota o en sitio del incidente. * Si la incidencia persiste, el Ingeniero de Soporte de Nivel II procederá a gestionar la apertura de un ticket con el TAC del fabricante para dar pronta solución al incidente.		
19	El soporte requerido para la solución ofertada deberá ser provisto por el contratista durante el tiempo de garantía ofrecido.		
20	El contratista deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la Entidad así lo requiera), este soporte deberá ser suministrado por personal especializado en la herramienta.		
	TRANSFERENCIA DE CONOCIMIENTO		
21	El contratista deberá realizar transferencia de conocimiento durante mínimo cuatro (4) horas a tres (3) ingenieros del Grupo de TIC, designados por el Supervisor del contrato, orientada a la instalación, configuración, parametrización y puesta en marcha de la solución, que brinde el conocimiento necesario para la administración y operación del hardware y software de la solución de seguridad implementada.		
22	La transferencia de conocimiento se podrá realizar durante la instalación, configuración, parametrización y puesta en funcionamiento la solución.		
23	Previo al inicio de actividades, el contratista deberá hacer entrega del documento de Plan de Transferencia de conocimiento en el cual se debe describir el mecanismo a utilizar para dicha actividad, de tal manera que se logre efectuar un aprovechamiento óptimo del software, de los equipos y de la tecnología.		
	DOCUMENTACION		
24	El contratista debe adjuntar los folletos, catálogos u hojas de especificaciones técnicas de los productos y servicios ofrecidos.		
25	El contratista debe documentar todos los procedimientos realizados para la instalación, configuración y parametrización de cada una de las funcionalidades implementadas y entregarlos en medio magnético e impreso, una vez revisados y aprobados por el Supervisor del contrato.		

ID	REQUISITO TÉCNICO		
26	Al finalizar la puesta en funcionamiento de la solución contratada, debe entregar en medio magnético e impreso, la documentación que permita la eficiente administración del firewall, como mínimo incluir: * Manual de procedimientos de administración y operación de los appliances. * Documento de descripción de la configuración de appliance y parámetros de configuración inicial de todo el software instalado. * Documentación de la topología de la solución implementada.		

3. 3. MONITOREO DE MARCA (Relación item 3)

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	Los equipos de ciberseguridad de todo el mundo luchan contra la escasez de talento, la gestión de miles de incidentes y la presión de las ciberamenazas que cada vez afectan más la rentabilidad y dañan la reputación de las empresas. Además, los incidentes relacionados con la fuga de datos, la piratería en línea y los fraudes digitales, como el phishing, exigen aún más tiempo de los equipos en los procesos operativos para su tratamiento y eliminación.		
2	La solución ofertada deberá permitir la escalabilidad y la automatización de la gestión de ciberamenazas, con el propósito de fortalecer las capacidades del equipo de seguridad de la información en la identificación, análisis y respuesta oportuna frente a riesgos que puedan afectar los activos digitales de la Entidad. La plataforma deberá proporcionar capacidades de Inteligencia de Ciberamenazas (Cyber Threat Intelligence), permitiendo el monitoreo continuo y la correlación de información proveniente de diferentes fuentes, incluyendo la superficie de Internet (Surface Web), así como la Deep Web y Dark Web, con el fin de identificar oportunamente amenazas, exposición de información, suplantaciones, campañas maliciosas y otros eventos que puedan comprometer la seguridad de la Entidad. Así mismo, deberá contar con mecanismos automatizados para la gestión y solicitud de retiro (takedown) de contenidos maliciosos o fraudulentos, disponibles de manera continua (24x7), así como con servicios especializados de análisis e investigación de amenazas que complementen las capacidades tecnológicas de la plataforma y permitan una respuesta eficiente frente a incidentes de seguridad.		
	FRAUDES DIGITALES		
3	Phishing, perfiles falsos en redes sociales, aplicaciones falsas, malware y nombres de dominio similares		
	FUGA DE DATOS		
4	Fuga de tarjetas de crédito, exposición de credenciales corporativas, fuga de bases de datos, exposición de código		
	PIRATERIA ONLINE		
5	Producto falso o venta irregular, piratería de contenidos y falsificación NFT		
	EJECUTIVOS & VIP		
6	Perfil de red social falso, con tecnología FaceMatch, fuga de información personal, fuga de credenciales, fuga de números de teléfono y fuga de tarjetas de crédito		
	DEEP & DARK WEB		
7	Monitoreo de grupos y foros no indexados, mediante capacidades de Inteligencia de Ciberamenazas (Cyber Threat Intelligence) y servicios especializados de investigación y análisis de amenazas cibernéticas, con el fin de identificar oportunamente riesgos, actividades maliciosas y posibles exposiciones que puedan afectar los activos de información de la Entidad.		
	PLATAFORMAS SaaS		

ID	REQUISITO TÉCNICO	SI	NO
8	La plataforma SaaS más intuitiva con usuarios ilimitados para aliviar a los equipos de ciberseguridad Optimice la gestión de equipos multidisciplinarios: * Ciberseguridad * Marketing * Ami-fraude * Protección de dalos * Juridico		
	TAKEDOWN		
9	Elimine fraudes y contenidos maliciosos con el takedown más eficaz del sector 99% de éxito: * Primera notificacldn en mlnutos * Norificación 24X7, para plataformas de todo el mundo * Verificación autométlca del contenldo * Transparencia en todo el proceso: realice el acompafiamiento en ticmpo real * Reportes de reputaclén: reduclmos la exposlclén a! fraude notificando a los principales actores de scguridad del mercado, como antivirus, asociaciones y grupos antlfraude, para mltlgar los lmpactos. * El 70% del contenido se elimina en la primera notificación		
	REDUZCA EL MTTC (MEAN TIME TO CONTAIN) CON LAS AUTOMACIONES DE LA PLATAFORMA		
10	Cree reglas inteligentes para detectar incidentes en menos tiempo, claslficar y tratar las amenazas en tiempo real.		
	GARANTICE EL TRATAMIENTO CORRECTO DE LOS DATOS Y REDUZCA EL RIESGO LEGAL Y DE REPUTACIÓN		
11	Las detecciónes almacenan evidencias de las amenazas detectadas incluso después de su eliminación * Screenshot de la páglna donde esté a amenaza* * HTML de la página * Información del domlnlo (Whois) *En mas del 98% de los casos		
	THREAT INSPECTOR		
12	La herramienta debe contar con Threat inspector, una tecnología única de inteligencia artificial que va más allá de la detección. Con esta función, las amenazas se analizan y clasifican con un algoritmo propio, teniendo en cuenta el nivel de riesgo, de dicha amenaza, y permitiendo automatizaciones inteligentes, como: * Score de riesgo * Semejanza de logotipo * Tecnologia FaceMatch para identificar ejecutivos con el análisis de semeíanza de resto * Filtro por idiomas para detección inteligente clasificando contenidos del mundo entero		
	TAKEDOWN WARRANTY		
13	Una exclusividad de Axur que demuestra el compromiso de eliminar los contenidos inapropiados durante un máximo de 15 días. Durante este periodo, si una página vuelve a aparecer, solicitamos su eliminación sin coste adiciona		
	COMPROMISO DE PRIVACIDAD		
14	Elimine los perfiles falsos de las redes sociales sin compartir su acceso personal. Datos seguros y privacidad garantizada		
	TRACKING TOKENS		
15	Proteja sus bases de datos y mitigue riesgos con LGPD: * Identificación * Seguimiento * Notificación de fugas * Control de procedencia * Mejora en la respuesta a incidentes		

ID	REQUISITO TÉCNICO	SI	NO
	INTEGRACIONES		
16	La plataforma debe contar con una API estable, dinámica y flexible, con una documentación actualizada y extremadamente completa, permitiendo realizar varias integraciones con aplicaciones externas como: * SIEM * SOAR * DMARC * Sistemas de ticketing * Fuentes de otras herramentas (Phishtank, Domain Tools) y otras.		

4. 4. EDR(ENDPOING DETECTION AND RESPONSE) (Relación item 4)

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	Adquisición de un sistema de detección y respuesta de punto final (EDR por sus siglas en inglés), que permita a la entidad fortalecer la postura de seguridad de los dispositivos finales en la misma.		
	GENERALIDADES		
2	Suministro de una solución de detección de punto final que cubra eventos de pre-ejecución y post-ejecución para prevención antimalware, investigación y respuesta a eventos.		
3	Los componentes que integran la solución no deben aparecer en listas end-of-life ó end-of-sale del fabricante.		
4	La solución debe brindar detección en tiempo real, contención y respuesta a ciber amenazas.		
5	La solución debe ser validada para cumplimiento de PCI DSS y HIPAA.		
6	La solución debe estar como recomendada por NSS Labs en el informe de Advanced Endpint Protection para el año 2019 y su equivalente para el año 2020, o certificada por AV Test.		
7	La solución debe contar con soporte técnico por parte del fabricante por un periodo de 1 año en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono.		
	CARACTERISTICAS MINIMAS DE DESEMPEÑO		
8	Numero de endpoints a proteger: 900		
9	Rendimiento de Servidores a Proteger: 100		
10	La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows (32 bits y 64 bits) XP SP2 / SP3, 7, 8, 8.1 y 10		
11	La solución propuesta debe ser compatible con los siguientes sistemas operativos de servidor: Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 y 2019		
12	La solución propuesta debe ser compatible con las siguientes versiones de macOS: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15)		
13	La solución propuesta debe ser compatible con los siguientes sistemas operativos: Versiones de Linux: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, Servidor 18.04.1 y 18.04.2, 64 bits		
14	La solución propuesta debe ser compatible con los siguientes sistemas operativos: entornos de Infraestructura de escritorio virtual (VDI) en VMware y Citrix. VMware Horizons 6 y 7, y Citrix XenDesktop 7		
15	La solución propuesta debe tener un consumo máximo de 120 MB de RAM		
16	La solución propuesta debe tener un consumo promedio de CPU de menos del 2%.		
17	La solución propuesta debe consumir menos de 40 MB de espacio en disco		
18	La solución propuesta debe tener protección "Anti Tamper" o "AntiViolation" en su agente		

ID	REQUISITO TÉCNICO	SI	NO
19	La solución propuesta debe funcionar sin depender de firmas hash locales para amenazas conocidas para detectar archivos maliciosos.		
20	La solución propuesta debe registrar en tiempo real la información del proceso y la información adicional, como determinar el usuario asociado con los eventos.		
21	La solución propuesta debe tener la opción de solicitar una contraseña para desinstalar el agente de la estación de trabajo.		
22	La solución propuesta debe admitir la instalación masiva utilizando herramientas como MS System Center, JAMF y Satellite.		
	CARACTERISTICAS DE PROTECCION Y DETECCIÓN		
23	Funcionalidad de Antivirus de nueva generación basado en aprendizaje de máquina (Machine Learning).		
24	El agente que se instale en los endpoint de la solución propuesta debe poder trabajar detrás de un proxy		
25	La solución debe poder descubrir y hacer seguimiento a aplicaciones y dispositivos IoT.		
26	La solución propuesta debe poder funcionar en modalidad "offline" fuera de línea sin que el Agente se encuentre conectado a la red empresarial		
27	La solución debe proveer enriquecimiento de datos con CVE y clasificación de aplicaciones.		
28	La solución debe brindar control sobre dispositivos USB.		
29	La solución propuesta debe poder Incorporar inteligencia de amenazas en el esquema de detección.		
30	La solución propuesta debe tener la capacidad de recibir actualizaciones diarias de inteligencia		
31	La solución propuesta debe identificar actividad maliciosa conocida y no conocida.		
32	La solución propuesta debe tener la capacidad para cargar indicadores de compromisos (IOC) tales como IP, dominio, nombre de archivo, hash de archivo, etc.) para la búsqueda de amenazas		
33	La solución de be contar con capacidades de búsqueda de drecciones IP de destino.		
34	La solución propuesta debe detectar las conexiones establecidas en la red desde el dispositivo protegido.		
35	La solución propuesta debe ser capaz de evitar la ejecución de archivos maliciosos.		
36	La solución propuesta debe bloquear el tráfico malicioso de la filtración de datos (fuga de datos)		
37	La solución propuesta debe bloquear el tráfico de comunicación malicioso hacia C&C (Comando y Control)		
38	La solución propuesta debe tener la capacidad de categorizar los eventos detectados en diferentes categorías (Ej: Malicioso, Sospechoso, No concluyente, Probablemente Seguro)		
39	La solución debe proveer políticas proactivas para permitir la reducción de la superficie de ataque.		
40	La solución propuesta debe poder configurarse en modo de monitoreo de tal manera que no se realice ningún tipo de bloqueo pero se grabe toda actividad maliciosa.		
41	La solución propuesta debe permitir el escaneo periódico de los archivos contenidos en el dispositivo con el agente instalado para todos o un grupo de los agentes desplegados.		
42	La solución propuesta debe detectar cambios realizados por procesos maliciosos en las claves de registro de la estación de trabajo		
43	La solución propuesta debe poder frenar brechas de seguridad e intentos de ransomware en tiempo real		
44	La solución propuesta debe poder evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos		
	CARACTERISTICAS DE RESPUESTA Y CONTENCIÓN		
45	Clasificación automática de eventos.		

ID	REQUISITO TÉCNICO	SI	NO
46	La solución propuesta debe permitir la creación de excepciones de eventos basados en direcciones IP, aplicaciones y protocolos		
47	La solución propuesta debe permitir el bloqueo automático de un dispositivo en el que se encontró una actividad causada por malware		
48	La solución propuesta debe permitir el bloqueo de actividades realizadas por archivos maliciosos		
49	Remediación automática (notificar a los usuarios, aislar el dispositivo, remediar el dispositivo, abrir tiquete).		
50	Remediación manual de eventos.		
51	Debe tener la capacidad de obtener instantáneas de memoria (volcados) que permitan realizar análisis forenses		
52	Debe tener la capacidad de abrir tickets en plataformas de administración como ServiceNow		
53	Debe almacenar los metadatos generados por los dispositivos para que se utilicen para la investigación forense.		
54	La solución debe permitir hacer investigación automatizada con interrupción mínima para el usuario.		
55	La solución propuesta debe la capacidad para restaurar la configuración de llaves de registro basada en la clasificación de actividad predefinida		
56	Debe poder teeminar un proceso basado en su clasificación.		
57	La solución debe brindar visibilidad completa de la cadena de ataque.		
58	Debe tener la capacidad de eliminar un archivo según su clasificación		
59	Debe tener la capacidad de aislar dispositivos infectados de la red		
60	Debe permitir la limpieza automática de dispositivos y revertir modificaciones maliciosas mientras se mantiene la disponibilidad del dispositivo afectado.		
61	Debe tener la capacidad de restringir automáticamente el acceso del dispositivo a la red de acuerdo con la clasificación de la actividad detectada		
62	La solución propuesta debe proporcionar múltiples mecanismos de protección, incluida como la terminación de un proceso, eliminación de un archivo malicioso, el bloqueo de una conexión de red		
63	Debe identificar y prevenir los intentos de escalación de privilegio		
64	La solución propuesta debe permitir la reducción de las superficies de ataque utilizando políticas proactivas de comunicación basadas en el riesgo de acuerdo a CVE y la calificación o reputación que puede tener una aplicación		
65	La solución propuesta debe tener la capacidad para prevenir la comunicación a través de la red de cualquier aplicación no autorizada		
66	La solución propuesta debe poder detectar e identificar todas las aplicaciones en los dispositivos que se comunican en la red.		
67	La solución propuesta debe tener la capacidad para crear políticas que tengan la capacidad de prevenir la comunicación de aplicaciones de acuerdo a la versión de la aplicación instalada		
68	Debe tener la capacidad de detectar estaciones de trabajo y servidores en la red organizacional que no estén protegidos con un agente EDR		
69	La solución propuesta debe tener la capacidad para descubrir aplicaciones vulnerables que se estén comunicando a través de la red		
70	Debe tener la capacidad de realizar un parche virtual, restringiendo el acceso de comunicación a las aplicaciones que son vulnerables		
71	La solución debe estar en capacidad de integrarse con la solución de protección de amenazas avanzadas con la que cuenta la entidad, para inspección de archivos ejecutables.		
72	La solución debe estar en capacidad de integrarse con la solución de SIEM con la que cuenta la entidad.		
	CARACTERISTICAS ADICIONALES		
73	El oferente debe incluir los servicios profesionales para el despliegue de la solución en premisas.		
74	La consola de administración debe permitir la visualización de eventos grabados en dispositivos que requieren atención.		

ID	REQUISITO TÉCNICO	SI	NO
75	La consola de administración de la solución debe permitir ver el estado de los agentes instalados.		
76	La consola de administración debe permitir la activación y desactivación remota del agente instalado en los dispositivos.		
77	La consola de administración debe permitir la creación de grupos organizativos en los que cada grupo pueda tener reglas de protección independientes de los demás.		
78	La consola de administración debe permitir la auditoría de los cambios realizados por los administradores / operadores. Estas auditorías se pueden descargar a un archivo en formato CSV		
79	Capacidad para integrarse con el Servicio del fabricante para el monitoreo, detección de alertas, gestión de incidentes de la solución propuesta		
80	El oferente debe incluir un servicio de monitoreo de amenazas directo del fabricante con cubrimiento 7x24x365.		
81	La consola de administración de la solución propuesta debe permitir la integración con "Active Directory" para garantizar el cumplimiento de los requisitos de la política de contraseñas de la empresa.		
82	La consola de administración de la solución propuesta debe permitir el uso de autenticación de doble factor (2FA) para acceder a la misma		
83	La consola de administración de la solución propuesta debe permitir el uso de roles granulares para los administradores		
84	La consola de administración de la solución propuesta debe permitir la gestión a través de Full Restful API		
85	La solución propuesta debe poder ser gestionada completamente en nube sin requerimiento de servicios en las premisas, con posibilidad de arquitectura hibrida utilizando servicios en las premisas complementadas con otras en nube.		
86	La solución debe poder brindar protección a las estaciones finales tanto cuando se encuentran conectadas a la red corporativa de la entidad, como fuera de ella.		
	SERVICIOS PROFESIONALES		
88	La solución deberá incluir los servicios de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, realizada por ingenieros certificados por el fabricante de los equipos. El contratista deberá presentar las respetivas certificaciones del grupo de trabajo asignado expedidas por el fabricante de los equipos.		
89	La implementación de este proyecto será exclusiva para empresas que pertenezcan al nivel máximo de membresía del fabricante y que formen parte del programa de socios de servicios preferentes (EPSP).		
	PLAN DE TRABAJO		
90	El contratista deberá presentar máximo dos (2) días hábiles luego de firmada el acta de inicio las hojas de vida y certificaciones del personal que realizará la implementación y el plan de trabajo detallado en el cual se describa el componente de diseño de la seguridad perimetral incluyendo los equipos que actualmente cuenta la entidad, adicionalmente se debe tener en cuenta los procesos/actividades inherentes para alcanzar el objeto de la solución, explicando claramente el número de días de la actividad y profesionales dedicados para desarrollar cada actividad relacionada en el cronograma, que incluya, entre otros, actividades, fechas de inicio y terminación, hitos y ruta crítica. La secuencia y duración de cada una de las actividades debe estar discriminada en semanas. Este plan de trabajo será de obligatorio cumplimiento durante la ejecución del contrato, previa aprobación del Supervisor del Contrato.		
	DISEÑO		
91	Los diseños de la solución a implementar deberán ser revisados y aprobados por el supervisor del contrato. Si el Supervisor lo considera pertinente podrá solicitar nuevos diseños que se ajusten a las necesidades de la Entidad.		
	IMPLEMENTACION		
92	Planeación de cada una de las actividades con el fin de disminuir los tiempos de afectación en el servicio.		

ID	REQUISITO TÉCNICO	SI	NO
93	Presentar diseño de seguridad perimetral de acuerdo a buenas prácticas y recomendaciones del fabricante integrando los dispositivos de seguridad con los que actualmente cuenta la entidad, este será evaluado y aprobado por el supervisor de contrato.		
94	Presentar el diseño de Políticas de Seguridad para ser evaluado y aprobado por el líder de infraestructura y el supervisor del contrato.		
95	Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.		
96	Implementación de la solución de acuerdo a las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura.		
97	Pruebas de Servicio de las plataformas ofertadas.		
98	Puesta en Producción de las plataformas ofertadas.		
99	Estabilización de las plataformas ofertadas.		
100	Entrega a satisfacción de la entidad.		
101	Dentro de los servicios se debe tener en cuenta el diseño, Instalación, configuración y puesta en producción de los dispositivos de seguridad que actualmente cuenta la Entidad, así como la entrega a satisfacción de los mismos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para el cliente.		
102	La entidad requiere la implementación y puesta en marcha de las plataformas ofertadas, así como la configuración de políticas, objetos y demás configuraciones a que haya lugar para dejar las misma totalmente operativas y a satisfacción de la entidad, así como realizar pruebas de detección de cada una para validar su correcta configuración de acuerdo a las buenas prácticas de implementación del fabricante.		
103	El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, Entre otros) requerida para que el personal asignado al proyecto, pueda cumplir sus funciones.		
104	La implementación de este proyecto será exclusiva para empresas que pertenezcan al nivel máximo de membresía del fabricante y que formen parte del programa de socios de servicios preferentes (EPSP).		
	GARANTIA Y SOPORTE		
105	El oferente deberá prestar el servicio de soporte para apertura de casos de cualquier criticidad a través de una mesa de Ayuda, vía telefónica o vía correo electrónico. Por ambos medios la atención de incidentes estará disponible en horario 7x24x365.		
106	El contratista deberá registrar, gestionar y hacer seguimiento a cualquier incidente reportado por el la Entidad, además durante la atención inicial del caso se determinará su criticidad y la metodología para su resolución.		
107	Niveles de Atención que debe prestar el contratista: * Un primer nivel de atención con Agente Nivel I de la Mesa de Ayuda a través de la ejecución de un checklist, en conjunto con la Entidad, y la validación del respectivo problema. * Si la incidencia no es resuelta se deberá asignar un Ingeniero de Soporte de Nivel II para proceder con la atención remota o en sitio del incidente. * Si la incidencia persiste, el Ingeniero de Soporte de Nivel II procederá a gestionar la apertura de un ticket con el TAC del fabricante para dar pronta solución al incidente.		
108	El soporte requerido para la solución ofertada deberá ser provisto por el contratista durante el tiempo de garantía ofrecido.		
109	El contratista deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la Entidad así lo requiera), este soporte deberá ser suministrado por personal especializado en la herramienta.		
	TRANSFERENCIA DE CONOCIMIENTO		

ID	REQUISITO TÉCNICO	SI	NO
109	El contratista deberá realizar transferencia de conocimiento durante mínimo cuatro (4) horas a tres (3) ingenieros del Grupo de TIC, designados por el Supervisor del contrato, orientada a la instalación, configuración, parametrización y puesta en marcha de la solución, que brinde el conocimiento necesario para la administración y operación del hardware y software de la solución de seguridad implementada.		
110	La transferencia de conocimiento se podrá realizar durante la instalación, configuración, parametrización y puesta en funcionamiento la solución.		
111	Previo al inicio de actividades, el contratista deberá hacer entrega del documento de Plan de Transferencia de conocimiento en el cual se debe describir el mecanismo a utilizar para dicha actividad, de tal manera que se logre efectuar un aprovechamiento óptimo del software, de los equipos y de la tecnología.		
	DOCUMENTACIÓN		
112	El contratista debe adjuntar los folletos, catálogos u hojas de especificaciones técnicas de los productos y servicios ofrecidos.		
113	El contratista debe documentar todos los procedimientos realizados para la instalación, configuración y parametrización de cada una de las funcionalidades implementadas y entregarlos en medio magnético e impreso, una vez revisados y aprobados por el Supervisor del contrato.		
114	Al finalizar la puesta en funcionamiento de la solución contratada, debe entregar en medio magnético e impreso, la documentación que permita la eficiente administración del firewall, como mínimo incluir: * Manual de procedimientos de administración y operación de los appliances. * Documento de descripción de la configuración de appliance y parámetros de configuración inicial de todo el software instalado. * Documentación de la topología de la solución implementada.		

5. 5. ANALISIS DE VULNERABILIDADES (Relación item 5)

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	La solución debe ser entregada como un servicio Software-as-a-Service (SaaS) en una nube propietaria del fabricante para todos sus servicios y aplicaciones requeridas en este documento. No se aceptan servicios brindados desde nubes de terceras partes.		
2	Todos los servicios de la plataforma deben estar disponibles bajo el mismo estándar de calidad de servicio 24x7x365 y garantizar 99,5% de disponibilidad.		
3	El oferente deberá ofrecer constante mantenimiento y actualización a la plataforma durante todo el periodo de tiempo que dure el contrato del servicio.		
4	Las actualizaciones del servicio deben ser transparentes para el administrador de la solución, sin afectar ninguno de los datos almacenados o servicios suministrados.		
5	Solo se admitirá 1 desconexión al trimestre durante un periodo de tiempo no mayor a 4 horas del servicio ofertado en ventanas de mantenimiento programadas y previamente notificadas.		

ID	REQUISITO TÉCNICO	SI	NO
6	La plataforma que brinda los servicios debe contar con las siguientes certificaciones: SSAE 18 SOC 2 FedRamp Moderate Privacy Shield Framework CloudStar PCI ASV ISO/IEC 27001: 2013 ISO/IEC 27017: 2015 ISO/IEC 27018: 2019 GDPR		
7	Toda comunicación entre componentes, transferencia y sincronización de datos de la solución debe estar cifrada de extremo a extremo, haciendo uso como mínimo de TLS 1.2, certificados firmados con RSA 2048 bits y algoritmo de firma SHA256.		
8	La solución se debe licenciar por IP o HOST y debe proveer capacidades de descubrimiento e inventario ilimitadas con acceso ilimitado a agentes, escáneres, sensores para contenedores, sensores de descubrimiento pasivo sin licenciamientos o costos adicionales.		
9	La solución debe ofrecerse licenciada para 800 IP/HOST para escaneo de vulnerabilidades, 800 HOST para Parcheo / Inventario, 2 URLS para escaneo de aplicaciones web		
10	Inventario de 1000 activos (servidores, estaciones de trabajo, dispositivos de telecomunicaciones, de redes, virtualizacion, nube)		
11	Descubrimiento de Vulnerabilidades para 80 servidores críticos		
12	La solución debe permitir descubrir, evaluar, priorizar e dientificar parches vulnerabilidades / configuraciones en toda la infraestructura de la red, incluyendo estaciones de trabajo, servidores, dispositivos de red, telecomunicaciones y seguridad, hipervisores, máquinas virtuales, orquestadores de contenedores, contenedores y nubes (Azure, GCP, AWS), brindando una única interfaz web de usuario para todos los activos, permitiendo la gestión centralizada de todos los componentes de la solución desde un único punto, sin necesidad de incurrir a consolas adicionales o componentes fuera de la misma para la administración de los servicios ofertados.		
13	La solucion debera contar con un API para la integracion con plataformas de terceros sin requerir licenciamiento adicional, hasta 2 llamados por suscripcion y 300 llamadas por hora		
14	La solución propuesta debe:		
15	Permitir enviar alertas en tiempo real acerca de las irregularidades en la red, identificar amenazas y supervisar los cambios inesperados que se produzcan en la misma.		
16	Enviar notificaciones para usuarios específicos y grupos de usuarios para el perfil de monitoreo o múltiples perfiles de monitoreo.		
17	Permitir personalizar el perfil de monitoreo asociado a una lista específica de criterios.		
18	Permitir que las alertas se pueden personalizar para con una amplia variedad de condiciones que afectan a los sistemas, certificados, vulnerabilidades, puertos, servicios y software. Cada regla debe permitir configurarse para detectar cambios generales comunes o ajustarse a circunstancias muy específicas.		
19	Permitir la asignación de diferentes destinatarios para cada alerta.		

ID	REQUISITO TÉCNICO	SI	NO
20	Enviar de alertas de monitoreo sobre vulnerabilidades, configuraciones incorrectas y otros parámetros definidos por el administrador de la solución, tales como: Activos con sistemas operativos no homologados Certificados expirados o por expirar Puertos abiertos Vulnerabilidades graves Tickets de remediación abiertos, resueltos o cerrados Software no homologado		
21	La solución debe:	☐ Sí ☐ No	
22	Incorporar un motor de calculo de riesgo, que automáticamente ayude a priorizar los activos.	☐ Sí ☐ No	
23	Realizar el calculo del riesgo de los activos teniendo en cuenta al menos las siguientes variables: Vulnerabilidades asociadas al activo Criticidad del activo Ubicación del activo Amenazas/Ataques asociados a las vulnerabilidades halladas Problemas configuración Controles compensatorios Certificados asociados al activo Obsolescencia del software	☐ Sí ☐ No	
24	Permitir priorizar acciones de remediación basándose en este cálculo de riesgo.	☐ Sí ☐ No	
25	Realizar un calculo de riesgo dinámico y no estático, contemplando variaciones en las amenazas o variables contempladas en el cálculo de riesgo a lo largo del tiempo, en el caso de que alguna variable cambie a lo largo del tiempo, esta misma debería modificar el cálculo de riesgo de la vulnerabilidad y el activo.	☐ Sí ☐ No	
26	Permitir crear flujos de trabajo automatizados para acciones de evaluación y remediación sin necesidad de código y mediante el uso de una interfaz grafica del tipo “drag and drop”, a traves de la integracion con un modulo de parchado nativo de la solucion	☐ Sí ☐ No	
27	Permitir la priorizacion de las parches a traves de un filtrado sencillo basado en etiquetas, nivel de riesgo del activo, nivel de criticidad del activo y criticidad de la vulnerabilidad	☐ Sí ☐ No	
28	Permitir agrupar la priorizacion de vulnerabilidades por activo, vulnerabilidad o parche a ser aplicado	☐ Sí ☐ No	
29	La solución propuesta debe:	☐ Sí ☐ No	
30	Proveer fuentes de inteligencia de amenazas en tiempo real y técnicas de aprendizaje automático, para brindar control al administrador sobre la evolución de las amenazas relacionadas con las vulnerabilidades halladas en los activos de la organización e identificar cuáles corregir primero.	☐ Sí ☐ No	
31	Permitir realizar consultas adhoc con múltiples variables y criterios, como clase de activo, tipo de vulnerabilidad, indicadores de amenazas en tiempo real, etiqueta del activo y sistema operativo, de modo que se pueda, por ejemplo, buscar todas las vulnerabilidades que tienen una clasificación de gravedad alta, son fáciles de explotar y fueron divulgadas en la última semana.	☐ Sí ☐ No	
32	Hacer una correlación en tiempo real de amenazas activas contra las vulnerabilidades detectadas en los activos corporativos.	☐ Sí ☐ No	

ID	REQUISITO TÉCNICO	SI	NO
33	Incluir indicadores de amenazas en tiempo real que ayuden a evaluar y priorizar las vulnerabilidades detectadas, categorizados de la siguiente forma: *Dia cero: vulnerabilidades para las que no hay un parche disponible y para las que se ha observado un ataque activo. *Exploit público: Vulnerabilidades cuyo mecanismo de explotación es conocido, para las que existe un código de explotación y está disponible públicamente. *Ataques activos: Vulnerabilidades que están siendo atacadas activamente. *Movimiento lateral: Vulnerabilidades que permiten que el atacante propague el ataque ampliamente a través de la red violada. *Fácil explotación: Vulnerabilidades que se pueden explotar fácilmente, que requieren pocas habilidades y pocos conocimientos *Perdida de datos: Vulnerabilidades cuyo exploit producirá una pérdida masiva de datos *Denegación de servicio: Vulnerabilidades cuyo payload podría sobrecargar o bloquear los sistemas comprometidos para que no estén disponibles de forma permanente o temporal. *Sin Parche: Vulnerabilidades para las que no hay una solución por parte del proveedor *Malware: Vulnerabilidades asociadas infecciones de malware *Kit de explotación: Vulnerabilidades para las que hay disponible un exploit kit	☐ Sí ☐ No	
34	La solución propuesta debe:	☐ Sí ☐ No	
35	Permitir la detección y creacion de un inventario de todos los activos conocidos y desconocidos que se conectan al entorno de TI híbrido global de la organización, incluidos los dispositivos y aplicaciones locales, móviles, estaciones de trabajo, servidores, dispositivos de red / telecomunicaciones / seguridad, nubes, contenedores, TO e IoT.	☐ Sí ☐ No	
36	Permitir descubrir dispositivos, aunque no sea permitido hacer ping o traceroute.	☐ Sí ☐ No	
37	Permitir generar vistas gráficas de los dispositivos descubiertos a través de visualizaciones de mapas de la red.	☐ Sí ☐ No	
38	Permitir descubrir todos los activos conectados a la red, incluso en segmentos con entornos aislados y en infraestructuras críticas.		
39	Permitir descubrir activos ofreciendo las siguientes alternativas: Escaneo pasivo de la red Escaneo activo de la red no autenticado Escaneo activo de la red autenticado Agente		
40	Ofrecer un inventario de activos que cubra como mínimo los siguientes puntos:		
41	Inventario de activos de la red local: Debe detectar todos los dispositivos y aplicaciones conectadas a la red, incluidos servidores, bases de datos, estaciones de trabajo, routers, dispositivos de seguridad y redes, impresoras y dispositivos IoT.		
42	Inventario de Certificados: Debe detectar y catalogar todos los certificados TLS/SSL digitales (internos y externos) de cualquier autoridad de certificación.		

ID	REQUISITO TÉCNICO	SI	NO
43	Inventario de Nube: Debe permitir supervisar los usuarios, instancias, redes, almacenamiento, bases de datos, ACL, ELB y sus relaciones para tener un inventario continuo de los recursos y activos en al menos las siguientes plataformas de nube pública: Amazon AWS Google Cloud Platform Microsoft Azure. Oracle Cloud (OCI)		
44	Inventario de Contenedores: Debe permitir descubrir y tener visibilidad de la infraestructura de contenedores activos o inactivos brindando información de imágenes, registros, contenedores asociados o creados a partir de la misma imagen y hosts / pods donde se encuentran.		
45	Inventario de dispositivos móviles: Debe permitir detectar y catalogar los dispositivos móviles, con todos los detalles de versionado de OS (Android, IOS, IpadOS) y hardware sobre el dispositivo, su configuración y las aplicaciones instaladas.		
46	La solución propuesta debe:		
47	Permitir recopilar información detallada del activo gestionado, la misma debe detallar al menos los siguientes datos para cada activo: Servicios en ejecución Software instalado Usuarios Puertos abiertos Versión de sistema operativo Hostname FQDN IP v4/v6 MAC Address Procesador Memoria Volúmenes de disco BIOS		
48	Permitir de forma automática clasificar los activos por familias tecnológicas, tipo de dispositivo, tipo de plataforma y fabricante. Automáticamente normalizar los nombres de los fabricantes de HW y SW con sus datos relevantes como nombre de las aplicaciones y versiones, para facilitar su posterior búsqueda en la solución.		
49	Permitir el etiquetado de activos para facilitar la identificación, generando etiquetas al menos utilizando los siguientes parámetros: Estática / manual. Palabras clave Dirección IP y rangos de IPs Segmento de Red Puertos abiertos ID de Vulnerabilidad especifica Groovy Scriptlet o Regex		
50	La solucion debe:		
51	Ejecutar escaneos de vulnerabilidades basados en: Sistemas Operativos Servicios WEB Puertos TCP y UDP Servicios Aplicaciones Bases de Datos		

ID	REQUISITO TÉCNICO	SI	NO
52	Como mínimo cubrir los sistemas operativos listados en la URL adjunta, bases de datos y aplicaciones (Definir con el cliente un listado de aplicaciones y sistemas operativos a cubrir para listar como un requerimiento mínimo).		
53	Detectar y analizar vulnerabilidades de al menos los siguientes sistemas operativos: Microsoft Windows UNIX LINUX MacOsx Cisco VMware		
54	Detectar y analizar vulnerabilidades en las principales versiones de Bases de Datos, al menos: Microsoft SQL Server MySQL Oracle Sybase		
55	Detectar y analizar vulnerabilidades en plataformas WEB, al menos: IIS Apache Tomcat		
56	Detectar y analizar vulnerabilidades por puertos y servicios como: TCP UDP		
57	Buscar vulnerabilidades en al menos las siguientes aplicaciones y/o plataformas: Adobe Apple HP McAfee Microsoft (Office, IIS, Exchange) Oracle Oracle Java VMware		
58	Permitir descubrir vulnerabilidades en la red ofreciendo las siguientes alternativas de escaneo Escaneo activo de la red no autenticado Escaneo activo de la red autenticado Agente		
59	Contar con un motor de analisis cuya tasa precisión para detección de vulnerabilidades del 99.99966% (six sigma) durante los últimos 10 años.		
60	Contar con una base de conocimiento de vulnerabilidades que sea actualizada semanalmente, asegurando la incorporación de al menos 20 CVEs a la misma y debe contar con al menos una base de conocimiento de 35.000 CVEs relacionados incluyendo tecnologías legadas y actuales.		
61	Admitir el soporte estándar de la industria para la puntuación de vulnerabilidades Common Vulnerability Scoring System (CVSS)		
62	Admitir el soporte estándar de la industria para la adición de detecciones personalizadas utilizando Open Vulnerability Assessment Language (OVAL).		
63	Permitir vincular las vulnerabilidades detectadas e indicar su relación con amenazas como Virus, Troyanos y Malware.		

ID	REQUISITO TÉCNICO	SI	NO
64	Contar con una base datos que relacione la mayoría de las vulnerabilidades con CVE y Bugtraq.		
65	Soportar integración para autenticación por con herramientas de bóvedas de contraseña líderes de la industria.		
66	Permitir la configuración del tipo de escaneo que se va a realizar, permitiendo como mínimo definir las siguientes configuraciones al definir el mismo: Configuración de puertos Consumo de ancho de banda y recursos (Alto, Medio, Bajo) Escaneo a dispositivos que no soportan ping o traceroute Evitar el purgado de datos de un dispositivo cuando se detecta un cambio en el sistema operativo Detección de balanceadores de carga Configuración de fuerza bruta a utilizar para los passwords Utilización de un header HTTP personalizado Ignorar ciertos paquetes		
67	Tener la capacidad de generar la evaluacion de las vulnerabilidades, estableciendo el nivel real de criticidad a traves del analisis de informacion relacionada con la vulnerabilidad y generar su propio score, usando criterios como: CVSS Score CISA known exploitable Exploit Code Maturity (ECM) Exploit Treding Threat Actor		
68	La solucion debe:		
69	Permitir la evaluación, informar y reportar problemas de configuración, en función de las referencias del estándar de industria Center of Internet Security (CIS).		
70	El fabricante debe estar certificado por CIS de forma oficial para entregar este nivel de controles.		
71	Ofrecer evaluación de configuraciones basado en el estándar de industria CIS Benchmark, dando cobertura de esta funcionalidad en las siguientes categorías: Sistemas operativos Software de servidor Proveedores de nube Dispositivos de red Software de escritorio		
72	Permitir la evaluación de certificados digitales (internos y externos) y configuraciones TLS en busca de problemas y vulnerabilidades de certificados brindando como resultado distintos grados de conformidad de acuerdo con los resultados de evaluación de su emisor, fecha de expiración, tipo de certificado, robustez del algoritmo y suite de cifrado utilizada.		
73	La solucion debe:		
74	Correlacionar de forma automática vulnerabilidades y parches para los hosts de la organización.		
75	Mapear automáticamente los parches con los CVE asociados a las vulnerabilidades detectadas.		
76	Permitir la identificacion de los parches sin necesidad de integrarse con herramienta adicionales		
77	La solución debe ofrecer la posibilidad de supervisar, gestionar y proteger dispositivos móviles Android, IOS, IpadOS		
78	La solucion debera:		
79	Tener la capacidad de renovar los certificados que caducan directamente desde la interfaz de usuario de la herramienta.		

ID	REQUISITO TÉCNICO	SI	NO
80	Permitir el envio de alertas cuando un certificado este proximo a vencer		
81	Permitir configurar las CA autorizada para evaluar si la CA que firma los certificados esta autorizada por la compania, de lo contratario debera generar alertas de los certificados no validos		
82	Metodologia de Analisis de Vulnerabilidades aplicable al proyecto Fase 1. PLANEACIÓN Definición del alcance. Objetivos de la prueba Activos involucrados. Fase 2: LIMITACIONES Y ALCANCES Tiempos de Ejecución Restricciones operativas y responsables. Canal de Comunicación y aprobación formal de actividades. Fase 3: RECONOCIMIENTO Recolección de Información relevante sobre los activos en evaluación. Técnicas de reconocimiento pasivo (Open Source Intelligence) y activo. Descubrimiento de posibles vectores de exposición. Fase 4: ANÁLISIS DE VULNERABILIDADES Escaneos automáticos y Revisión Manual de Debilidades Técnicas. Inspección de configuraciones, versiones ý exposición de servicios. Identificación y Documentación inicial de vulnerabilidades conocidas (CVE). Fase 5: VALIDACIÓN TÉCNICA DE HALLAZGOSRevisión Técnica para confirmar veracidad de hallazgos detectados. Clasificación de cada hallazgo según los criterios de criticidad (CVSS) e impacto potencial. Simulación no destructiva de condiciones vulnerales si se justifica (sin explotación activa). Fase 6: REPORTE FINAL Elaboración de Informe Técnico, actualización de Matriz de Vulnerabilidades (según aplique) con recomendaciones priorizadas. Asesoría y acompañamiento en remediación (si aplica).		

6. 6. SGSI

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	El proveedor deberá estar en la capacidad de brindar apoyo en el seguimiento a auditorías internas (bimestrales) y externas del SGSI, incluyendo la preparación de evidencias, gestión de hallazgos y atención de requerimientos de entes de control, con cobertura sobre el SGSI de la Gobernación de Santander.		
2	El proveedor deberá estar en la capacidad de apoyar la evaluación, mitigación y monitoreo de riesgos de seguridad de la información, incluyendo la gestión continua de indicadores y la actualización del análisis de riesgos conforme a nuevas amenazas y tecnologías, a nivel de sistemas, usuarios y activos de información.		

ID	REQUISITO TÉCNICO	SI	NO
3	El proveedor deberá estar en la capacidad de apoyar el desarrollo, actualización e implementación de políticas de seguridad de la información, alineadas con la norma ISO 27001:2022, incluyendo políticas de contraseñas, gestión de proveedores, uso aceptable, privacidad, aseguramiento de la información, mantenimiento, desarrollo seguro de software, gestión de cambios, continuidad del negocio (DRP) y plan operativo anual, con cobertura sobre el SGSI de la entidad.		
4	El proveedor deberá estar en la capacidad de apoyar la documentación y actualización de procedimientos operativos de seguridad, incluyendo respaldo de información, continuidad del negocio, gestión y seguimiento de incidentes, control de cumplimiento y mitigación de vulnerabilidades, aplicables a los sistemas informáticos de la entidad.		
5	El proveedor deberá estar en la capacidad de asistir en la elaboración y ejecución del plan de sensibilización en seguridad de la información, incluyendo el diseño y ejecución de una (1) campaña de sensibilización mensual dirigida al personal de la entidad.		
6	El proveedor deberá estar en la capacidad de ejecutar una (1) capacitación semestral en seguridad de la información, orientada a fortalecer las competencias del personal en el marco del SGSI.		
7	El proveedor deberá estar en la capacidad de ejecutar una (1) prueba de ingeniería social tipo phishing semestral, dirigida a hasta 1000 buzones de correo, con el fin de evaluar el nivel de concienciación de los usuarios frente a amenazas de seguridad.		
	METODOLOGIA SGSI		
8	El SGSI estará diseñado para cumplir con los requisitos establecidos en la norma ISO/IEC 27001:2022, asegurando que la protección de los activos de información esté alineada con las mejores prácticas globales. Los aspectos clave de esta alineación incluyen: • Análisis de Riesgos: El SGSI incorporará un análisis de riesgos detallado para identificar las vulnerabilidades y amenazas a los activos de información, en línea con los requisitos de la ISO/IEC 27001:2022. • Definición de Controles de Seguridad: Se implementarán controles de seguridad adecuados para mitigar los riesgos identificados, incluyendo controles físicos, lógicos y administrativos. • Gestión de Incidentes: Se establecerán procedimientos claros para la detección, respuesta y recuperación ante incidentes de seguridad. • Evaluación y Mejora Continua: El SGSI será evaluado y mejorado de forma periódica para garantizar su efectividad y adecuación a las necesidades cambiantes de la organización.		
9	El proveedor deberá ejecutar la implementación y/o fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), bajo un enfoque estructurado alineado con la norma ISO/IEC 27001:2022, contemplando las siguientes fases: * Fase 1: Análisis GAP Inicial (27001:2022) * Fase 2: Entrega Informe GAP y Socialización de resultados * Fase 3: Definir el alcance del SGSI * Fase 4: Identificación de Activos de información * Fase 5: Elaboración de inventario de activos de información * Fase 6: Identificación de Riesgos * Fase 7: Analisis de Riesgos * Fase 8: Elaboración de Matriz de Riesgos * Fase 9: Elaboración de matriz de aplicabiilidad para acoplamiento con la ISO 27001 * Fase 10: Elaboración de Políticas de Seguridad * Fase 11: Diseño de Controles * Fase 12: Elaboración de Plan de pruebas * Fase 13: Diseño de plan de mitigación y mejora continua (PHVA)		
10	El proveedor deberá estar en la capacidad de establecer y ejecutar un programa de auditorías internas del SGSI, orientado a verificar el cumplimiento continuo de la norma ISO/IEC 27001:2022.		

ID	REQUISITO TÉCNICO	SI	NO
11	El proveedor deberá ejecutar auditorías internas de forma periódica, con una frecuencia mínima anual, evaluando la eficacia del SGSI y la correcta implementación de los controles de seguridad.		
12	El proveedor deberá realizar la revisión y actualización de controles y procedimientos del SGSI, con base en los resultados de auditorías, identificando desviaciones y oportunidades de mejora.		
13	El proveedor deberá definir y gestionar Indicadores Clave de Desempeño (KPIs) del SGSI, tales como: * Número de incidentes de seguridad * Tiempo de respuesta y resolución de incidentes * Nivel de cumplimiento de controles de seguridad		
14	El proveedor deberá realizar el seguimiento a las acciones correctivas y planes de mejora, derivados de auditorías internas o externas, asegurando su cierre efectivo.		
15	El proveedor deberá garantizar la disponibilidad de la documentación del SGSI, incluyendo resultados de auditorías y evidencias, para procesos de revisión, auditoría externa o certificación.		
16	El proveedor deberá garantizar la documentación del proceso de auditoría, incluyendo hallazgos, desviaciones, acciones correctivas y su respectivo seguimiento, asegurando trazabilidad.		
17	El proveedor deberá estar en la capacidad de emplear herramientas de gestión de proyectos, que permitan la planificación, seguimiento y control de las actividades relacionadas con la implementación del SGSI.		
18	El proveedor deberá estar en la capacidad de implementar herramientas de gestión documental, que permitan la creación, almacenamiento, control de versiones y trazabilidad de la documentación del SGSI.		
19	El proveedor deberá garantizar que las herramientas utilizadas se encuentren alineadas con los objetivos del SGSI, contribuyendo al fortalecimiento de la confidencialidad, integridad y disponibilidad de la información.		
	PREMISAS Y CONDICIONES		
20	El proveedor deberá ejecutar el servicio considerando la disponibilidad de recursos humanos, tecnológicos y financieros por parte de la entidad para la implementación del SGSI.		
21	El proveedor deberá contemplar que la entidad garantice el acceso controlado a sistemas, activos de información y datos, necesarios para la ejecución de las actividades.		
22	El proveedor deberá considerar la participación activa de personal clave de la entidad, incluyendo áreas de TI, seguridad y operaciones, para el desarrollo del SGSI.		
23	El proveedor deberá ejecutar las actividades en entornos controlados y seguros, evitando afectar la operación de los sistemas en producción.		
24	El proveedor deberá contemplar que el SGSI será objeto de revisión y actualización periódica, conforme a cambios tecnológicos, regulatorios y de amenazas.		
25	El proveedor deberá considerar la existencia de mecanismos de monitoreo y registro de eventos de seguridad, que permitan la detección y gestión de incidentes.		
26	El proveedor deberá ejecutar el servicio bajo el entendimiento de que existe compromiso de la alta dirección en la implementación y sostenimiento del SGSI.		
27	El proveedor deberá garantizar que la ejecución del servicio se alinee con el cumplimiento de requisitos normativos y regulatorios aplicables en materia de seguridad de la información.		

7. 7. HERRAMIENTA DE PROTECCIÓN DE CORREO – PASARELA SMTP

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	Suministrar, instalar, configurar y poner en operación una solución de seguridad del correo electrónico en modalidad pasarela SMTP (gateway), para proteger el flujo de correo entrante y saliente de trescientos (300) buzones alojados en Microsoft 365 / Exchange Online, sin trasladar el alojamiento de buzones.		
2	La solución deberá proteger trescientos (300) buzones de correo electrónico de la entidad por medio de las políticas de flujo y conectores aplicables. El sistema de correo y el almacenamiento principal de mensajes permanecerán en la plataforma de correo existente.		
3	La solución deberá desplegarse como pasarela de protección de correo y permitir el encaminamiento del flujo mediante configuración de dominios, registros MX, conectores y reglas de transporte en el servicio de correo, según aplique.		
4	Deberá permitir inspeccionar mensajes entrantes y salientes en los flujos enrutados a través de la pasarela, conforme a las políticas de la entidad y las capacidades contratadas.		
5	Deberá realizar clasificación de correo no deseado y permitir su bloqueo, cuarentena o etiquetado con reglas configurables, listas de confianza y bloqueo, y administración de excepciones.		
6	Deberá inspeccionar mensajes y adjuntos para detectar y prevenir malware, empleando mecanismos de seguridad actualizables durante todo el periodo contratado.		
7	Deberá contar con mecanismos de detección y prevención de phishing, suplantación de remitente, dominios fraudulentos, enlaces maliciosos y amenazas de compromiso de correo corporativo.		
8	Deberá permitir aplicar y comprobar políticas y resultados de SPF, DKIM y DMARC, de acuerdo con las configuraciones soportadas y las políticas definidas por la entidad.		
9	Deberá incluir protección avanzada frente a amenazas de correo, análisis de URLs y archivos sospechosos y medidas de prevención frente a amenazas desconocidas, de acuerdo con el alcance contratado.		
10	Deberá soportar políticas de tipos de archivo, tamaño, contenido y tratamiento de archivos potencialmente maliciosos, incluyendo cuarentena y otras acciones de mitigación soportadas.		
11	Deberá contar con administración de cuarentena y mecanismos de consulta, liberación, eliminación o tratamiento de mensajes sujetos a roles y permisos.		
12	Deberá admitir reglas por dominio, remitente, destinatario, dirección IP, reputación y características del mensaje, con administración de perfiles, permisos y excepciones.		
13	Deberá generar bitácoras de recepción, clasificación, acciones aplicadas, entrega, cuarentena y administración, así como informes operativos y de incidentes.		
14	Deberá permitir la integración o exportación de eventos de seguridad al sistema de monitoreo de la entidad mediante formatos e interfaces compatibles, sujetos a las funciones contratadas.		
15	El contratista deberá verificar y documentar el dimensionamiento para 300 buzones según volumen de mensajes por día y en hora pico, tamaño medio de adjuntos, dominios y proyección de crecimiento.		
16	La implementación deberá contemplar mecanismos de continuidad del flujo SMTP, manejo de fallos, colas y recuperación según funcionalidades soportadas y arquitectura aprobada.		
17	Deberá proteger las comunicaciones administrativas y soportar cifrado TLS para los flujos SMTP compatibles, con configuración de certificados y políticas según capacidades de los extremos.		

ID	REQUISITO TÉCNICO	SI	NO
18	La inspección se aplicará al correo que efectivamente atraviese la pasarela SMTP. La inspección de mensajes internos o ya almacenados en Microsoft 365 mediante API no forma parte del alcance base, salvo contratación expresa y demostración técnica.		
19	Deberá incluir actualizaciones de seguridad, servicios de inteligencia y soporte especializado durante doce (12) meses, además de soporte y acompañamiento del contratista conforme al SLA contractual.		
20	Deberá comprobarse el flujo de entrada y salida, filtrado antispam, detección de mensajes de prueba, tratamiento de phishing y adjuntos, cuarentena, alertas, bitácoras y entrega de correo legítimo.		
21	El contratista entregará arquitectura, inventario de dominios, configuración de conectores, políticas, evidencias de pruebas, procedimientos de operación y escalamiento y transferencia de conocimiento.		
22	La pasarela deberá inspeccionar de forma configurable archivos comprimidos y contenido adjunto, dentro de los límites de análisis documentados.		
23	La profundidad de análisis de archivos comprimidos deberá corresponder a las funciones técnicas acreditadas de la solución, sin imponer un número de capas sin evidencia.		
24	Se deberán documentar las limitaciones y acciones permitidas frente a adjuntos cifrados o protegidos con contraseña.		
25	El servicio deberá permitir el análisis de formatos comprimidos soportados, conforme a sus políticas y capacidades.		
26	La solución deberá integrarse mediante flujo SMTP y conectores de Exchange Online con el servicio de correo alojado en Microsoft 365, sin exigir integración API de buzones.		
27	La pasarela deberá identificar y bloquear amenazas de archivos, URLs, malware y suplantación en los mensajes que atraviesen el flujo de correo protegido.		
28	El contratista deberá gestionar incidentes de seguridad del correo y su escalamiento dentro del esquema de soporte y atención acordado, sin asumir un servicio administrado de respuesta a incidentes no contratado.		
29	La solución deberá inspeccionar la totalidad de mensajes que efectivamente atraviesen la pasarela SMTP, sujetos a límites técnicos, políticas y excepciones documentadas.		
30	Deberá inspeccionar enlaces y mensajes entrantes y salientes dirigidos a través del gateway según las rutas implementadas.		
31	La disponibilidad del servicio deberá corresponder a la arquitectura implementada y a los compromisos de soporte y mantenimiento del equipo.		
32	Deberá incluir análisis estático y avanzado de amenazas, URL, adjuntos sospechosos, phishing, malware y ransomware según las capacidades del servicio contratado.		
33	Podrá configurarse control de contenido y prevención de fuga de información en el flujo SMTP, en la medida soportada por la licencia y el equipo.		
34	La solución se implementará mediante pasarela de seguridad de correo instalada en la infraestructura aprobada por la entidad y conectada a Microsoft 365.		
35	Deberá recibir actualizaciones periódicas de seguridad y motores antimalware mientras esté vigente el servicio contratado.		
36	La capacidad podrá ampliarse mediante actualización de licencias y/o infraestructura, conforme a las condiciones de crecimiento del servicio.		
37	La pasarela deberá aplicar políticas preventivas y bloquear o poner en cuarentena amenazas antes de entregar los mensajes a los buzones protegidos.		
38	Deberá integrarse con Microsoft 365 mediante registros DNS, conectores y reglas de transporte compatibles con el flujo SMTP.		

ID	REQUISITO TÉCNICO	SI	NO
40	La solución deberá interoperar con Microsoft 365 / Exchange Online a través de mecanismos de encaminamiento de correo soportados.		
41	La herramienta deberá disponer de mecanismos documentados de consulta, administración e integración de eventos, en el alcance disponible.		
42	La inspección de mensajes ya entregados y los mensajes internos de Microsoft 365 mediante API no se incluye en el alcance base; requerirá contratación y acreditación adicional si se solicita.		
43	La plataforma deberá poder exportar alertas o registros al sistema de monitoreo central de la entidad mediante interfaces soportadas.		
44	Deberá permitir el envío de eventos al SIEM conforme al mecanismo, formato y latencia de integración disponibles.		
45	El acceso administrativo deberá mantenerse protegido mediante controles de autenticación apropiados.		
46	La plataforma deberá permitir administración por perfiles y asignación de permisos de acuerdo con las funciones disponibles.		
47	La ampliación de funciones de protección se realizará, cuando se requiera, mediante capacidades y servicios adicionales compatibles con la solución.		
48	La transmisión de correo y la gestión administrativa deberán protegerse mediante protocolos seguros como TLS, según compatibilidad de los extremos.		
49	El manejo de certificados, claves y credenciales deberá ajustarse a las políticas de seguridad y protección de información de la entidad.		
50	La oferta deberá adjuntar documentación y certificaciones de seguridad aplicables a la solución y a los servicios contratados.		
51	La solución operará sobre infraestructura aprobada por la entidad, con procedimientos de continuidad, respaldo y recuperación documentados.		
52	Deberá incluir consola administrativa para consultar estados de mensajes, políticas, eventos, estadísticas e incidentes.		
29	la solución debe tener la opcion de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc.		
53	La solucion debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación		
54	El cliente debe estar en capacidad de personalizar los banners y las alertas de advertencia y traducirlos a otros idiomas como español, inglés y portugues		
55	La solucion debe tener una forma que el usuario reporte un presunto falso positivo o falso negativo para que la solucion la revise y de su veredicto		
56	La solución debe envíar informes y resúmenes de acciones a los usuarios		
57	El contratista deberá contar con procedimientos de gestión de incidentes y escalamiento especializado para eventos del correo protegido.		
58	Los servicios de respuesta especializados no incluidos en el licenciamiento deberán acreditarse de forma separada cuando sean requeridos por el pliego.		
59	La solución deberá contar con soporte técnico especializado y suscripciones de seguridad vigentes durante el plazo contratado, sin requerir marcas o referencias comerciales particulares.		
60	El contratista garantizará atención de incidentes conforme a los horarios y tiempos de atención acordados contractualmente.		
61	La solución deberá proteger trescientos (300) buzones de correo corporativo alojados en Microsoft 365 mediante pasarela SMTP.		
	Admnistración y Gestion de la Plataforma		

ID	REQUISITO TÉCNICO	SI	NO
62	La solución deberá incluir los servicios de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, realizada por ingenieros certificados por el proveedor de la solución de los equipos. El contratista deberá presentar las respetivas certificaciones del grupo de trabajo asignado expedidas por el proveedor de la solución de los equipos.		
63	La implementación será realizada por personal idóneo con experiencia acreditable en pasarelas de seguridad de correo y correo corporativo en la nube, de acuerdo con los requisitos del pliego.		
	Garantia Y Soporte		
65	El oferente deberá prestar el servicio de soporte para apertura de casos de cualquier criticidad a través de una mesa de Ayuda, vía telefónica o vía correo electrónico. Por ambos medios la atención de incidentes estará disponible en horario 7x24x365.		
66	El contratista deberá registrar, gestionar y hacer seguimiento a cualquier incidente reportado por el la Entidad, además durante la atención inicial del caso se determinará su criticidad y la metodología para su resolución.		
67	Niveles de Atención que debe prestar el contratista: * Un primer nivel de atención con Agente Nivel I de la Mesa de Ayuda a través de la ejecución de un checklist, en conjunto con la Entidad, y la validación del respectivo problema. * Si la incidencia no es resuelta se deberá asignar un Ingeniero de Soporte de Nivel II para proceder con la atención remota o en sitio del incidente. * Si la incidencia persiste, el Ingeniero de Soporte de Nivel II procederá a gestionar la apertura de un ticket con el TAC del proveedor de la solución para dar pronta solución al incidente.		
68	El soporte requerido para la solución ofertada deberá ser provisto por el contratista durante el tiempo de garantía ofrecido.		
69	El contratista deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la Entidad así lo requiera), este soporte deberá ser suministrado por personal especializado en la herramienta.		
	DOCUMENTACION		
70	El contratista debe adjuntar los folletos, catálogos u hojas de especificaciones técnicas de los productos y servicios ofrecidos.		
71	El contratista debe documentar todos los procedimientos realizados para la instalación, configuración y parametrización de cada una de las funcionalidades implementadas y entregarlos en medio magnético e impreso, una vez revisados y aprobados por el Supervisor del contrato.		
72	Al finalizar la puesta en funcionamiento de la solución contratada, debe entregar en medio magnético e impreso, la documentación que permita la eficiente administración de la plataforma de seguridad de correo electrónico, como mínimo incluir: * Manual de procedimientos de administración y operación de los appliances. * Documento de descripción de la configuración de appliance y parámetros de configuración inicial de todo el software instalado. * Documentación de la topología de la solución implementada.		

8. 8. ETHICAL HACKING

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	Ejecutar 1 prueba de Ethical Hacking semestral sobre 30 activos tecnológicos, incluyendo servidores físicos, servidores virtuales, dispositivos de seguridad (UTM) y aplicaciones, con el fin de identificar vulnerabilidades explotables y posibles vectores de ataque.		
2	Realizar 1 análisis de vulnerabilidades cuatrimestral sobre la infraestructura tecnológica de la Gobernación de Santander, incluyendo hasta 80 servidores y 800 estaciones de trabajo, con el fin de identificar vulnerabilidades, configuraciones inseguras y software desactualizado.		
	METODOLOGÍA PRUEBAS ETHICAL HACKING		
3	La prueba deberá ejecutarse bajo una metodología estructurada basada en estándares reconocidos como OWASP, PTES o EC-Council.		
4	El enfoque de la prueba deberá contemplar escenarios de evaluación tipo caja negra y caja gris, de acuerdo con el nivel de información suministrado por la entidad.		
5	La ejecución del servicio se realizará bajo un enfoque metodológico basado en buenas prácticas de Ethical Hacking, alineadas con estándares del EC-Council (CEH). Las actividades incluirán como mínimo las siguientes fases: * Reconocimiento * Escaneo y enumeración * Análisis de vulnerabilidades * Explotación controlada cuando aplique * Post-explotación limitada a la validación del impacto		
6	La explotación de vulnerabilidades se realizará de forma controlada y no intrusiva, únicamente cuando sea necesario para validar la existencia y el impacto del hallazgo.		
7	No se contempla la ejecución de pruebas destructivas o de alto impacto sobre la infraestructura, tales como: * Ataques de denegación de servicio (DoS / DDoS) * Pruebas de estrés que afecten la disponibilidad de los sistemas		
8	Todos los hallazgos deberán ser documentados con evidencia técnica, impacto y recomendaciones de mitigación.		
9	El proveedor deberá contar con un equipo de Ingenieros profesionales especializados en seguridad de la información y Ethical Hacking, responsables de la ejecución de las pruebas.		
10	El equipo deberá contar con certificaciones vigentes en seguridad informática, tales como CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), CompTIA Security+ u otras certificaciones equivalentes		
	METODOLOGÍA ANALISIS DE VULNERABILIDADES		
11	El proveedor deberá ejecutar el análisis de vulnerabilidades bajo una metodología estructurada, alineada con buenas prácticas y estándares reconocidos como NIST SP 800-115, OWASP y lineamientos del EC-Council (CEH), orientada a la identificación, validación y priorización de vulnerabilidades en la infraestructura tecnológica.		
12	El proveedor deberá realizar la validación manual de los hallazgos identificados, con el fin de eliminar falsos positivos y asegurar la precisión técnica de los resultados obtenidos.		
13	El proveedor deberá garantizar que los hallazgos identificados sean analizados y correlacionados en función del contexto técnico de los activos evaluados, permitiendo una interpretación adecuada del riesgo.		
14	El proveedor deberá clasificar las vulnerabilidades identificadas mediante un sistema de scoring basado en el estándar CVSS, considerando su nivel de criticidad, impacto potencial y facilidad de explotación.		

ID	REQUISITO TÉCNICO	SI	NO
15	El proveedor deberá garantizar que los hallazgos identificados sean analizados y correlacionados en función del contexto técnico de los activos evaluados, permitiendo una interpretación adecuada del riesgo.		
16	El proveedor deberá priorizar los hallazgos identificados en función de su nivel de riesgo, permitiendo a la entidad establecer planes de remediación efectivos.		
17	El proveedor deberá generar un informe técnico detallado, que incluya la descripción de las vulnerabilidades, evidencia técnica, clasificación de riesgo y recomendaciones de mitigación.		
18	El análisis de vulnerabilidades deberá limitarse a la identificación, validación y clasificación de hallazgos, sin contemplar la explotación activa de los mismos, salvo validaciones controladas cuando aplique.		

9. 9. ANALISIS DE CÓDIGO PRUEBAS SAST Y DAST SOBRE CÓDIGO FUENTE

1. Características mínimas y especificaciones requeridas

ID	REQUISITO TÉCNICO	SI	NO
1	Aplicar pruebas de seguridad antes del despliegue de software, mediante la ejecución de: * 5 revisiones de código fuente estático (SAST) * 5 revisiones de análisis dinámico de aplicaciones (DAST) * con el objetivo de identificar vulnerabilidades en etapas previas a producción.		
	METODOLOGÍA PRUEBAS SAST Y DAST SOBRE CÓDIGO FUENTE		
2	El análisis SAST deberá incluir revisión de código fuente orientada a la identificación de vulnerabilidades como: inyecciones, manejo inseguro de datos, exposición de credenciales y errores de validación.		
3	Las pruebas deberán permitir la identificación de vulnerabilidades asociadas al comportamiento de la aplicación, tales como fallas de autenticación, control de acceso, exposición de servicios y vulnerabilidades del OWASP Top 10.		
4	Los resultados deberán incluir clasificación de vulnerabilidades según su criticidad e impacto.		
5	La ejecución del servicio deberá realizarse bajo una metodología estructurada, alineada con estándares y buenas prácticas reconocidas, tales como OWASP, PTES y lineamientos del EC-Council (CEH), abarcando tanto pruebas de seguridad ofensiva como análisis de seguridad de aplicaciones (SAST y DAST).		
6	El proveedor deberá estar en la capacidad de ejecutar análisis de código fuente (SAST) sobre aplicaciones entregadas por la entidad, mediante el procesamiento de repositorios o carpetas que contengan el código fuente, siempre y cuando el volumen del mismo no supere las 800.000 líneas de código.		
7	El análisis deberá contemplar la identificación de vulnerabilidades de seguridad a nivel de código, incluyendo errores de validación, manejo inseguro de datos, exposición de credenciales y debilidades asociadas a buenas prácticas de desarrollo seguro.		
8	El proveedor deberá estar en la capacidad de ejecutar pruebas de análisis dinámico (DAST) sobre aplicaciones web en ejecución, mediante la conexión a entornos controlados definidos por la entidad, incluyendo ambientes de pruebas o preproducción.		
9	El proveedor deberá garantizar la ejecución del análisis de código fuente mediante un enfoque combinado de análisis automatizado y revisión manual experta, con el fin de identificar vulnerabilidades que no sean detectadas exclusivamente por herramientas.		
10	El proveedor deberá estar en la capacidad de realizar análisis de dependencias del software, identificando vulnerabilidades en librerías, componentes de terceros y frameworks utilizados por la aplicación.		

ID	REQUISITO TÉCNICO	SI	NO
11	El proveedor deberá garantizar la notificación inmediata de vulnerabilidades críticas, con el fin de que la entidad pueda tomar acciones oportunas de mitigación.		
12	El proveedor deberá generar un informe ejecutivo, que incluya el resumen de hallazgos, métricas de riesgo y análisis general del estado de seguridad de las aplicaciones.		
13	El proveedor deberá analizar el contexto de la arquitectura de la aplicación, incluyendo su estructura, componentes y flujos de información, con el fin de identificar riesgos asociados a la lógica de negocio.		

10. 10. REQUERIMIENTO DE PERSONAL SOC

1. Perfiles mínimos, cantidad y dedicación requerida

El contratista deberá disponer del personal relacionado a continuación para la prestación del servicio SOC durante la ejecución del contrato, de acuerdo con los perfiles, cantidades y porcentajes o condiciones de dedicación establecidos:

CARGO	CANT.	PERFIL PROFESIONAL	DEDICACIÓN
GERENTE DE PROYECTO	1	Ingeniero de Sistemas, informático, eléctrico, electrónico, de telecomunicaciones y/o afines. Especialista en gerencia de proyectos informáticos y/o de telecomunicaciones.	50 %
INGENIERO DE ASEGURAMIENTO TECNOLÓGICO	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines, con especialización y/o maestría en seguridad de la información y/o ciberseguridad.	100 %
INGENIERO DE ASEGURAMIENTO TECNOLÓGICO	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines, con especialización y/o maestría en seguridad de la información y/o ciberseguridad.	100%
INGENIERO DE PRUEBAS DE SEGURIDAD	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines.	A demanda, según requerimiento
INGENIERO DE PRUEBAS DE DESARROLLO SEGURO	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines.	A demanda, según requerimiento
COORDINADOR DE MONITOREO	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines.	100 %
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines.	100 %
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	1	Ingeniero de sistemas, electrónica, telemática, telecomunicaciones o afines.	100 %
ANALISTA DE MONITOREO SOC	1	Técnico o tecnólogo en las áreas de sistemas, telemática, telecomunicaciones o afines. Debe cubrir la jornada 7x24.	100 %
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	1	Ingeniero de Sistemas, informático, eléctrico, electrónico, de telecomunicaciones y/o afines. Especialista en seguridad de la información y/o seguridad informática.	100 %

2. NOTAS – REQUERIMIENTO DE PERSONAL SOC

Nota 1. Cumplimiento y disponibilidad del personal. El oferente deberá garantizar la disponibilidad, vinculación y asignación efectiva del personal requerido por la Entidad, de conformidad con los perfiles profesionales, cantidades, niveles de formación, experiencia, porcentajes de dedicación y

horarios establecidos en la presente ficha técnica. Así mismo, deberá asegurar que el personal asignado se encuentre disponible durante toda la vigencia del servicio, garantizando la continuidad de la operación y el cumplimiento de las actividades y responsabilidades propias de cada cargo.

Nota 2. Compromiso y acreditación del personal. El oferente deberá presentar, junto con su propuesta, una carta de compromiso suscrita por el representante legal, mediante la cual garantice el cumplimiento integral de los perfiles, cantidades y condiciones de dedicación del personal exigido por la Entidad. Así mismo, el oferente se comprometerá a presentar, dentro de los diez (10) días hábiles siguientes a la adjudicación del contrato, las hojas de vida, soportes académicos, certificaciones profesionales y demás documentos que acrediten el cumplimiento de los requisitos establecidos para cada perfil. La Entidad podrá verificar y validar la documentación presentada antes de autorizar la vinculación del personal a la ejecución del contrato.

Nota 3. Independencia del personal para la operación SOC. El personal relacionado en el presente apartado, correspondiente a la prestación del servicio SOC durante la ejecución del contrato, será adicional e independiente del equipo de trabajo exigido para las actividades de implementación, instalación, configuración, parametrización, puesta en funcionamiento y afinamiento de las soluciones tecnológicas objeto del contrato. En consecuencia, el contratista deberá garantizar la disponibilidad de ambos equipos de trabajo, sin que exista sustitución, duplicidad o afectación de las responsabilidades y dedicaciones exigidas para cada componente contractual.

Nota 4. Cobertura y continuidad del servicio de monitoreo SOC 7x24. El contratista deberá garantizar que el personal asignado al cargo de ANALISTA DE MONITOREO SOC asegure la cobertura permanente del servicio bajo un esquema de operación siete (7) días a la semana, veinticuatro (24) horas al día (7x24), durante los doce (12) meses de ejecución contractual. Para tal efecto, deberá disponer de la cantidad suficiente de analistas y establecer los turnos, relevos, descansos y mecanismos de reemplazo necesarios para garantizar la continuidad ininterrumpida del monitoreo, la identificación, gestión y escalamiento de eventos e incidentes de seguridad, sin generar interrupciones ni períodos de desatención del servicio. La cobertura 7x24 deberá garantizarse independientemente de las novedades administrativas, laborales, incapacidades, vacaciones o ausencias del personal asignado.