CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

1. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON LA CONTRATACIÓN.

El Instituto Nacional de Vías (INVIAS) es un establecimiento público del orden nacional, adscrito al Ministerio de Transporte, cuyo objeto, conforme a lo dispuesto en el artículo 1 del Decreto 1292 de 2021, consiste en ejecutar las políticas, estrategias, planes, programas y proyectos de la infraestructura no concesionada de la Red Vial Nacional de carreteras primarias y terciarias, así como de la infraestructura férrea, fluvial, marítima y sus infraestructuras conexas, de acuerdo con los lineamientos del Ministerio de Transporte.

En concordancia con lo anterior, el Gobierno Nacional, mediante el Decreto 1008 de 2018, adoptó la Política de Gobierno Digital, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), como una estrategia transversal que hace parte del Modelo Integrado de Planeación y Gestión (MIPG). Esta política busca promover una gestión pública más eficiente y transparente, a través del uso de tecnologías que fortalezcan la gestión interna de las entidades, mejoren la experiencia ciudadana y soporten la toma de decisiones basada en datos.

En el marco de esta política, y en desarrollo del Decreto 1292 de 2021, se creó la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) del INVIAS, la cual tiene como función, entre otras, asesorar a la Dirección General y a las demás dependencias en materia de tecnologías de la información, definir lineamientos para la adquisición y funcionamiento de bienes tecnológicos, y propiciar la apropiación de las tecnologías por parte de los servidores públicos y ciudadanos.

La ciberseguridad se define como el conjunto de políticas, controles, procedimientos, tecnologías y prácticas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información y de los sistemas que la procesan, frente a amenazas de origen digital. En el contexto de las entidades del Estado, la ciberseguridad ha dejado de ser un componente accesorio de la gestión tecnológica para convertirse en una función estratégica indispensable para la continuidad de la operación institucional y la protección del patrimonio público digital. La evolución de las amenazas cibernéticas ha transformado radicalmente el panorama de riesgo de las entidades públicas colombianas, exigiendo capacidades de defensa que superen el modelo tradicional basado únicamente en dispositivos de protección perimetral que operan de manera aislada y sin supervisión activa.
Esta necesidad institucional no es una apreciación discrecional de la Oficina de Tecnologías de la Información y las Comunicaciones — OTIC, sino que encuentra respaldo directo en el marco normativo que el Estado colombiano ha desarrollado progresivamente en materia de seguridad digital. Es por ello que, el Documento CONPES 3854 de 2016 estableció la Política Nacional de Seguridad Digital, actualizada posteriormente mediante el Documento CONPES 3995 de 2020; el Decreto 338 de 2022 fortaleció la gobernanza de la seguridad digital del país; y la Resolución 500 de 2021 adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI), fundamentado en la norma internacional ISO/IEC 27001 y en el NIST Cybersecurity Framework como referentes técnicos

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

complementarios. El desarrollo detallado de este marco normativo, y de las características técnicas que de él se derivan para el operador del servicio, se presenta más adelante en este estudio, una vez descritas la trayectoria de la entidad y las herramientas que componen el Centro de Operaciones de Seguridad.

El Instituto Nacional de Vías, en su condición de establecimiento público del orden nacional adscrito al Ministerio de Transporte, ha desarrollado a lo largo de más de diez años un proceso progresivo y sostenido de fortalecimiento de su infraestructura de ciberseguridad, materializado en sucesivos contratos orientados principalmente a la protección perimetral de su red y a la protección de los equipos de usuario final, cuya revisión cronológica detallada permite comprender con precisión el punto de madurez tecnológica en el que se encuentra actualmente la entidad.

En el año 2014, el INVIAS suscribió el contrato de prestación de servicios No. 2059 con la firma Comware S.A., cuyo objeto consistió en la adquisición de una solución integral de seguridad perimetral destinada a proteger la red LAN y WAN de la entidad, por un valor de quinientos setenta y un millones cuatrocientos cincuenta y cuatro mil ciento noventa pesos ($571.454.190) incluido el impuesto al valor agregado. Como resultado de la ejecución de este contrato, el contratista entregó a la entidad dos dispositivos de seguridad perimetral de la marca Palo Alto Networks, modelo 5020, configurados en esquema de alta disponibilidad es decir, con un equipo principal y un equipo de respaldo operando de manera simultánea, de forma que la falla de uno de ellos no comprometiera la continuidad de la protección perimetral, así como un dispositivo adicional Palo Alto Networks modelo M-100 Panorama, destinado a la administración centralizada de dichos firewalls, y dos dispositivos de conmutación (switches) de la marca Avaya, modelo ERS-4826GTS, necesarios para la conectividad de la solución dentro de la red de la entidad.

El contrato incluyó adicionalmente servicios profesionales de soporte técnico en sitio prestados directamente por la firma Comware S.A., así como servicios de soporte técnico de fábrica proporcionados por la casa matriz Palo Alto Networks, por un período de treinta y seis (36) meses, que culminó el 2 de febrero de 2018. Este contrato constituyó el punto de partida de la infraestructura de seguridad perimetral basada en tecnología Palo Alto Networks que la entidad ha mantenido y progresivamente modernizado hasta la actualidad, y evidenció desde ese momento la decisión institucional de adoptar un fabricante de reconocida trayectoria internacional en el segmento de firewalls de nueva generación.

Ante la revisión efectuada en el año 2018 sobre el estado de obsolescencia tecnológica de la infraestructura instalada en el centro de datos de la entidad, se identificó que los equipos adquiridos en 2014 se aproximaban al final de su ciclo de vida útil y de soporte de fabricante, por ello en el año 2019 el INVIAS suscribió el contrato de prestación de servicios No. 1904 con la firma Cayses S.A.S., cuyo objeto consistió en la adquisición de infraestructura de seguridad perimetral actualizada para proteger la red LAN y WAN de la entidad, por un valor de trescientos cincuenta y tres millones de pesos ($353.000.000) incluido IVA.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

Como resultado de este contrato, el contratista entregó e instaló en el centro de datos principal de la entidad dos equipos firewall Palo Alto Networks modelo PA-3250, operando uno en rol principal y el otro en rol de respaldo, utilizando interfaces de conectividad de datos SFP+ en configuración de agregación de enlaces (link aggregation) contra los switches de core de la entidad y contra los proveedores de conectividad, con capacidad de enlace agregado de hasta veinte gigabits por segundo (20 Gbps).

De manera adicional, y en un hito particularmente relevante para la evolución de la arquitectura de seguridad del INVIAS, este contrato incorporó la instalación de una máquina virtual Palo Alto Networks modelo VM-100, en rol standalone desplegada directamente en la nube pública de Microsoft Azure, extendiendo por primera vez la protección perimetral de la entidad más allá de su infraestructura física local, hacia el manejo de tráfico y la microsegmentación de los recursos privados que el INVIAS ya empezaba a desplegar en dicho entorno de nube. El servicio de soporte de fábrica asociado a esta renovación tuvo vigencia hasta el 14 de diciembre de 2022.

Al aproximarse el vencimiento de dicho soporte de fábrica, en el año 2022 el INVIAS suscribió el contrato de prestación de servicios No. 1663, nuevamente con la firma Cayses S.A.S., cuyo objeto consistió en la renovación de suscripciones y soporte para la solución de ciberseguridad de la entidad, por un valor de trescientos ochenta y seis millones trescientos dieciocho mil pesos ($386.318.000) incluido IVA, mediante el cual se extendió la vigencia del licenciamiento de los firewalls Palo Alto Networks hasta el 27 de diciembre de 2023. Un año después, en el año 2023, el INVIAS suscribió el contrato de prestación de servicios No. 5100, también con la firma Cayses S.A.S., cuyo objeto consistió específicamente en modernizar la solución de ciberseguridad de la entidad en lo relacionado con la seguridad perimetral del fabricante Palo Alto, por un valor de quinientos cuarenta y seis millones novecientos noventa mil trescientos cincuenta y nueve pesos ($546.990.359) incluido IVA, extendiendo nuevamente la vigencia del licenciamiento hasta el 27 de diciembre de 2024.

Al finalizar dicho período de licenciamiento y soporte el 28 de diciembre de 2024, y ante la necesidad de incorporar nuevas funcionalidades de ciberseguridad que trascendieran el alcance de las renovaciones anteriores, en el año 2025 el INVIAS suscribió el contrato de prestación de servicios No. 1353 con la sociedad Grupo Microsistemas Colombia S.A.S. identificada comercialmente como GMS, cuyo objeto comprendió la renovación e implementación de nuevas funcionalidades en ciberseguridad y la adquisición de componentes tecnológicos para la implementación de servicios de conectividad SD-WAN para la entidad, por un valor de mil setecientos setenta y seis millones seiscientos veintidós mil cuarenta y tres pesos ($1.776.622.043) incluido IVA, el más significativo, en términos de inversión, de toda la serie histórica de contratos de ciberseguridad de la entidad. Este contrato incorporó equipos de nueva generación, sustancialmente superiores en capacidad de procesamiento a los modelos PA-3250 previamente instalados: dispositivos modelo PA-1420 en arquitectura on-premise para la sede principal de la entidad, y firewalls virtuales modelo VM-300 desplegados en la nube pública de Microsoft Azure, en reemplazo de la máquina virtual VM-100 de generación anterior.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

De manera adicional, y por primera vez en la trayectoria de contratación de la entidad, este contrato incorporó subsistemas especializados complementarios a la seguridad perimetral tradicional: un subsistema de análisis de superficie de ataque, orientado a identificar de manera proactiva la exposición externa de los activos digitales de la entidad; un subsistema de firewall de aplicaciones web con protección contra ataques de denegación de servicio distribuido operado en modalidad de nube (WAF DDoS Cloud); un subsistema de conectividad SD-WAN, destinado a optimizar y asegurar el tráfico de datos entre la sede central y las direcciones territoriales de la entidad distribuidas en el territorio nacional; y un subsistema de cómputo forense, orientado a dotar a la entidad de capacidad técnica para el análisis y salvaguarda de evidencia digital ante eventuales incidentes de seguridad en las estaciones de trabajo de la sede central y de las territoriales.



Figura 9. Línea de tiempo de la contratación de seguridad perimetral. Valores expresados en millones de pesos. Fuente: elaboración propia con base en el texto suministrado.

Año	Contrato	Contratista	Valor	Alcance principal
2014	2059	Comware S.A.	$571.454.190	PA-5020, Panorama M-100, switches y soporte por 36 meses.
2019	1904	Cayses S.A.S.	$353.000.000	PA-3250 en alta disponibilidad y VM-100 en Microsoft Azure.
2022	1663	Cayses S.A.S.	$386.318.000	Renovación de suscripciones y soporte hasta diciembre de 2023.
2023	5100	Cayses S.A.S.	$546.990.359	Modernización de la solución de seguridad perimetral.
2025	1353	GMS	$1.776.622.043	PA-1420, VM-300, superficie de ataque, WAF/DDoS Cloud, SD-WAN y cómputo forense.

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

De manera paralela a esta evolución continua de su seguridad perimetral, el INVIAS ha mantenido desde el año 2017 una solución de protección de punto final (endpoint) basada en la plataforma Sophos, gestionada a través de una serie igualmente extensa de contratos sucesivos con la firma Grupo Microsistemas Colombia S.A.S. En el año 2017, mediante el contrato de prestación de servicios No. 1311, por un valor de sesenta y seis millones novecientos cincuenta y cuatro mil novecientos pesos ($66.954.900) incluido IVA, se adquirió e implementó por primera vez esta solución de protección de nueva generación para equipos de usuario final y servidores, desplegando inicialmente el software antivirus Sophos en mil doscientos (1.200) usuarios y ciento veinte (120) equipos de tipo servidor, e incorporando desde ese momento capacidades de Detección y Respuesta en Endpoint (EDR).

En el año 2018, mediante el contrato de prestación de servicios No. 1297 por valor de setenta y ocho millones noventa y nueve mil novecientos pesos ($78.099.900), se renovó dicho licenciamiento, extendiendo su vigencia hasta el 3 de diciembre de 2019. En el año 2019, mediante el contrato de prestación de servicios No. 1972 por valor de ciento setenta y seis millones cien mil pesos ($176.100.000), se adquirió una ampliación de la solución de protección para equipos de usuario final, extendiendo la vigencia del licenciamiento hasta el 3 de diciembre de 2021. En el año 2021, mediante el contrato de prestación de servicios No. 2157 por valor de doscientos tres millones novecientos ochenta y cinco mil seiscientos treinta y cinco pesos ($203.985.635), se renovó nuevamente la solución endpoint de nueva generación, extendiendo su vigencia hasta el 28 de diciembre de 2022. En el año 2022, mediante el contrato de prestación de servicios No. 1693 por valor de doscientos veintiocho millones nueve mil novecientos cincuenta pesos ($228.009.950), se efectuó una nueva renovación, con vigencia hasta el 31 de diciembre de 2023.

En el año 2023, mediante el contrato de prestación de servicios No. 5084 por valor de trescientos cincuenta y ocho millones seiscientos cuarenta y dos mil doscientos pesos ($358.642.200), cuyo objeto se orientó específicamente a la adquisición y renovación del derecho de uso de actualizaciones y soporte de productos antivirus, se extendió la vigencia del licenciamiento hasta el 28 de diciembre de 2024, incrementando en esa vigencia la cantidad de licencias a dos mil quinientas (2.500) — dos mil trescientas (2.300) tipo usuario y doscientas (200) tipo servidor — correspondientes a Sophos Intercept X Advanced with XDR y Sophos Central Phish Threat. En el año 2024, mediante el contrato de prestación de servicios No. 4364 por valor de trescientos sesenta y nueve millones treinta y tres mil doscientos ochenta y ocho pesos ($369.033.288), se renovó nuevamente dicho licenciamiento, extendiendo su vigencia hasta el 28 de diciembre de 2025. Y finalmente, en el año 2025, mediante el contrato de prestación de servicios No. 2036 por valor de trescientos diecinueve millones quinientos ochenta y seis mil cuatrocientos pesos ($319.586.400), se renovó el licenciamiento ajustándolo a mil ochocientas (1.800) licencias — mil seiscientas (1.600) tipo usuario y doscientas (200) tipo servidor —, ajuste justificado en la depuración reciente de identidades y estaciones registradas en la plataforma de Directorio Activo de la entidad, con vigencia hasta el 30 de diciembre de 2025.



Figura 10. Línea de tiempo de la contratación de protección de punto final. Valores expresados en millones de pesos. Fuente: elaboración propia.

Año	Contrato	Contratista	Valor	Alcance principal
2017	1311	GMS	$66.954.900	Implementación inicial de Sophos para usuarios y servidores.
2018	1297	GMS	$78.099.900	Renovación hasta diciembre de 2019.
2019	1972	GMS	$176.100.000	Ampliación de la solución endpoint.
2021	2157	GMS	$203.985.635	Renovación hasta diciembre de 2022.
2022	1693	GMS	$228.009.950	Renovación hasta diciembre de 2023.
2023	5084	GMS	$358.642.200	Actualizaciones y soporte hasta diciembre de 2024.
2024	4364	GMS	$369.033.288	Renovación hasta diciembre de 2025 (2.500 licencias).
2025	2036	GMS	$319.586.400	Ajuste a 1.800 licencias hasta el 30 de diciembre de 2025.

Nota: *Es importante tener en cuenta que la solución Sophos, no hace parte integral del proceso de contratación por las razones descritas como el resultado del ejercicio del estudio de mercado. Sin embargo, dada su importancia y teniendo en cuenta que la cobertura contratada es hasta el 28 de diciembre del 2026, el servicio SOC debe integrarse con esta solución en el marco de la detección de amenazas informáticas y establecidas en los requerimientos técnicos, establecidos en el documento Anexo 1 – Ficha técnica Ciberseguridad.*

La revisión detallada de esta doble línea de contratación, la de seguridad perimetral basada en Palo Alto Networks y la de protección de punto final basada en Sophos, evidencia de manera contundente que el Instituto Nacional de Vías ha mantenido, durante más de una década, un compromiso

institucional sostenido, consistente y creciente con el fortalecimiento de su ciberseguridad, materializado, según los valores relacionados en este documento, en una inversión acumulada aproximada de cinco mil cuatrocientos treinta y cuatro millones setecientos noventa y seis mil ochocientos sesenta y cinco pesos ($5.434.796.865) en estas dos líneas de contratación entre 2014 y 2025.

No obstante, un análisis igualmente riguroso de la naturaleza de todos estos contratos permite identificar un patrón estructural común a todos ellos: en la totalidad de los casos, el objeto contractual se centró en la adquisición o renovación de licenciamiento y soporte de fabricante sobre dispositivos y software específicos firewalls, antivirus, subsistemas complementarios, sin que en ningún momento de esta trayectoria la entidad haya contratado un servicio de monitoreo, correlación de eventos y respuesta continua, operado por un equipo humano especializado y dedicado, disponible las veinticuatro horas del día, es decir, sin que la entidad haya contado hasta la fecha con un Centro de Operaciones de Seguridad propiamente dicho, en los términos que se desarrollan más adelante en el presente estudio.

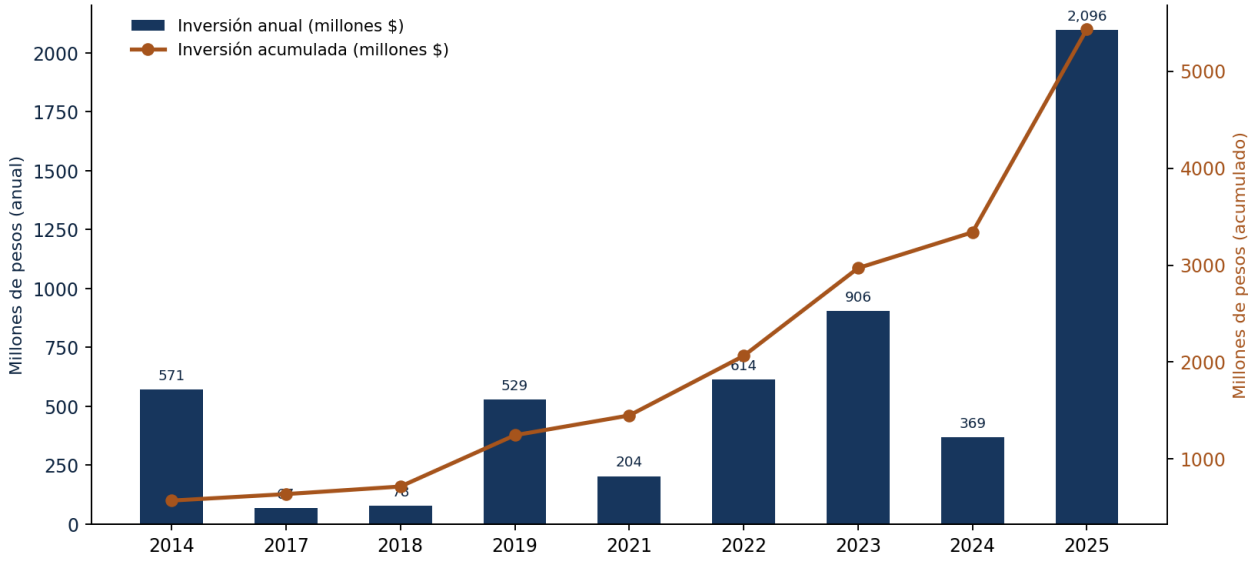


Figura 11. Inversión anual y acumulada calculada a partir de los valores relacionados en el documento. Fuente: elaboración propia.

Esta distinción resulta de la mayor relevancia práctica, pues implica que, no obstante la significativa inversión tecnológica realizada por la entidad a lo largo de una década, dicha inversión se ha concentrado en la adquisición de herramientas —los sentidos y los brazos ejecutores que se describen más adelante—, sin la incorporación simultánea del elemento humano especializado que interprete de manera continua la información que dichas herramientas generan, que correlacione

eventos entre las distintas plataformas adquiridas a lo largo de los años, y que ejecute con criterio experto las acciones de contención que la sofisticación de las amenazas actuales exige. En otras palabras: el INVIAS ha construido progresivamente, a lo largo de una década, un conjunto de herramientas de calidad creciente, pero sin el centro de operaciones que las active, las correlacione y las convierta en una capacidad de defensa efectivamente operativa.

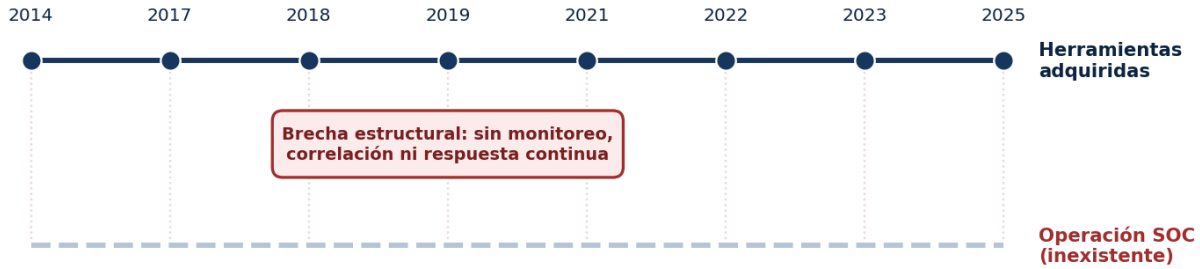


Figura 12. Brecha entre la adquisición de herramientas y la operación coordinada de un SOC. Fuente: elaboración propia.

Esta ausencia estructural de capacidad de monitoreo activo, correlación centralizada y respuesta especializada adquirió especial relevancia en el contexto de un incidente de ciberseguridad de alto impacto que afectó gravemente la infraestructura tecnológica del Instituto Nacional de Vías durante el mes de diciembre de 2025. Dicho incidente fue puesto formalmente en conocimiento de la Fiscalía General de la Nación mediante denuncia penal bajo número Único de Noticia Criminal 110016099382202500061 del 15 de diciembre de 2025 presentada por la entidad, por la presunta comisión de conductas punibles tipificadas en el Código Penal colombiano relacionadas con el acceso y la afectación no autorizada de sistemas informáticos, encontrándose actualmente en curso la investigación penal correspondiente ante dicha autoridad.

En atención a la reserva legal que ampara los detalles técnicos específicos del análisis forense practicado sobre el incidente, información que se encuentra sujeta a dicha investigación penal en curso y cuya divulgación pormenorizada en un documento de naturaleza pública como el presente estudio previo resultaría inapropiada e incluso jurídicamente inconveniente para los intereses de la entidad, el presente documento se limita a señalar, como hecho institucional documentado y fundamento de la necesidad que aquí se sustenta, que dicho incidente afectó de manera grave la disponibilidad de los servicios tecnológicos de la entidad, comprometió la continuidad de su

operación institucional durante un período significativo, y puso de manifiesto la necesidad de fortalecer las capacidades de monitoreo continuo, detección temprana, correlación centralizada de eventos y respuesta automatizada que un Centro de Operaciones de Seguridad, en los términos extensamente descritos en el presente estudio, está diseñado específicamente para proveer.

Es en este punto donde converge la totalidad del análisis desarrollado hasta ahora, para arrojar una conclusión ineludible sobre la necesidad institucional que el presente proceso de contratación busca satisfacer. El INVIAS cuenta, como se ha documentado extensamente, con una infraestructura de seguridad perimetral y de protección de endpoints robusta, actualizada y de reconocida trayectoria en el mercado, fruto de una inversión sostenida durante más de una década.

Sin embargo, dicha infraestructura opera en la actualidad, en esencia, como un conjunto de sensores y controles automatizados sin el centro nervioso que los active de manera coordinada: sin un SIEM que correlacione en tiempo real los eventos generados simultáneamente por los firewalls Palo Alto, la solución de protección de endpoints, el WAF y demás ya adquiridos por la entidad; sin un SOAR que automatice la respuesta ante los patrones de amenaza que dicha correlación permitiría identificar; sin un servicio de inteligencia de amenazas que anticipe las campañas dirigidas específicamente contra el sector público colombiano y contra entidades responsables de infraestructura crítica nacional como lo es el INVIAS; sin una plataforma de gestión de vulnerabilidades que evalúe de manera continua y sistemática el estado de exposición de la totalidad de su infraestructura híbrida; sin una solución de control de acceso a la red que segmente de manera efectiva su infraestructura y limite la capacidad de un atacante de desplazarse lateralmente una vez logrado un acceso inicial; y, sobre todo, sin el equipo humano especializado, organizado en niveles de experiencia progresiva y disponible de manera ininterrumpida las veinticuatro horas del día, que interprete con criterio experto la información generada por todas estas herramientas y ejecute, cuando la situación lo exija, las acciones de contención que la magnitud de un incidente de seguridad como el ocurrido en diciembre de 2025 demanda con la urgencia que su naturaleza impone.



Figura. Capacidad objetivo del Centro de Operaciones de Seguridad para el INVIAS. Fuente: elaboración propia.

Para el cumplimiento de este objeto misional, el INVIAS se soporta en un ecosistema tecnológico integral que comprende su centro de datos propio, los entornos de virtualización, los sistemas de información institucionales, los servicios desplegados en la nube pública en Azure, dispositivos de seguridad perimetral, los equipos de cómputo que operan tanto en la sede principal en Bogotá D.C., como en la sede Fontibón y veintiséis (26) direcciones territoriales distribuidas en el territorio nacional. La totalidad de este ecosistema tecnológico constituye simultáneamente el activo estratégico que garantiza el cumplimiento de los objetivos institucionales del INVIAS y la superficie de exposición que debe protegerse frente a las amenazas cibernéticas propias del entorno digital actual. En efecto, contar con una infraestructura tecnológica robusta, confiable y de alto rendimiento no es suficiente por sí sola si no está acompañada de capacidades igualmente robustas de monitoreo, detección y respuesta ante eventos de seguridad, capacidades que, como se desarrolla a continuación, se materializan a través de un Centro de Operaciones de Seguridad.

Dentro de este ecosistema, la protección del Proyecto Vías Inteligentes ITS – VIITS tiene especial relevancia por su relación directa con la gestión vial nacional. VIITS es el Sistema Inteligente de Transporte del Instituto y hace presencia en veintisiete (27) departamentos y aproximadamente seis mil (6.000) kilómetros de la red vial nacional. Ha procesado más de cien millones de datos provenientes de sus tres subsistemas: Orden Público y Seguridad, Monitoreo de Tránsito y Monitoreo de Infraestructura. Estas características permiten dimensionar la necesidad de preservar la disponibilidad, integridad y confidencialidad de la información que soporta su operación.

La información de estos subsistemas se captura mediante cámaras de detección automática de incidentes y videovigilancia, escáneres de inspección no intrusiva, sistemas de velocidad y pesaje dinámico, conteos fijos y móviles, controladores de galibo, paneles de mensajería variable e instrumentación geotécnica en zonas y puntos críticos. Todos estos dispositivos operan sobre infraestructura de campo con conectividad propia y convergen en el Centro de Control y Monitoreo Vial —CCMV— y en su Data Center. Los datos se almacenan y procesan en una plataforma híbrida con data lake, y su operación se realiza desde estaciones de trabajo y servidores que también requieren protección.

A su vez, el sistema se interconecta con el Ministerio de Transporte, la ANSV, la Superintendencia de Transporte, la ANI, la DIJIN, el SINITT, el RNDC y el RUNT, y apoya a la Policía Nacional, el Ejército Nacional y la Armada Nacional en el cumplimiento del Programa de Seguridad en Carreteras Nacionales. Por tanto, la información generada por VIITS trasciende el ámbito interno del Instituto y sirve de soporte para la coordinación y la toma de decisiones de otras entidades del Estado.

De acuerdo con las Resoluciones 3966 de 2000, 228 de 2013 y 1859 de 2014 del Ministerio de Transporte, VIITS y todos sus componentes deben operar los 365 días del año de forma ininterrumpida. La necesidad de monitoreo de seguridad debe guardar correspondencia con esa operación permanente, de manera que la protección de la información y de los recursos tecnológicos que la soportan acompañe la prestación continua de los servicios del proyecto.

Para cumplir su misionalidad, el Proyecto VIITS depende de la infraestructura tecnológica del Instituto que lo soporta de manera directa o indirecta. Esta comprende las redes y los servicios de comunicaciones, los centros de datos y los servicios en la nube, los servidores y los entornos de virtualización, los sistemas de información y las bases de datos, los mecanismos de respaldo, las estaciones de trabajo, las plataformas de seguridad y los demás recursos mediante los cuales el Instituto recibe, procesa, almacena, protege y distribuye la información del proyecto.

En consecuencia, la disponibilidad, integridad y confidencialidad de VIITS dependen de la seguridad del conjunto de estos elementos. El compromiso de cualquiera de ellos puede interrumpir la operación del proyecto o afectar la información que genera, aun cuando el evento se origine fuera de su perímetro físico. Por esta razón, se prevé que el Instituto pueda incorporar al monitoreo, durante la ejecución, la infraestructura adicional que se requiera para proteger el cumplimiento de

la misionalidad de VIITS, dentro de las capacidades contratadas.

Esta interdependencia permite relacionar los antecedentes de ciberseguridad descritos con la necesidad específica de proteger VIITS. La experiencia de diciembre de 2025 evidenció que la infraestructura tecnológica de la entidad enfrenta amenazas reales; a su vez, la incorporación de dispositivos de campo amplía la superficie de exposición que debe ser vigilada. Un incidente que comprometa el proyecto podría afectar, además del funcionamiento del INVIAS, la seguridad vial, el orden público y la información utilizada por otras entidades del Estado para adoptar decisiones. De ahí la necesidad de integrar las herramientas existentes con una capacidad permanente de análisis, correlación y respuesta, cuya operación se desarrolla a continuación.

Centro de Operaciones de Seguridad: conocido universalmente por sus siglas en inglés SOC, de Security Operations Center es la unidad organizacional, tecnológica y humana especializada cuyo propósito es proveer visibilidad continua, ininterrumpida y correlacionada sobre el estado de seguridad de la totalidad de la infraestructura tecnológica de una organización, con capacidad de detectar comportamientos anómalos, analizar su naturaleza y alcance, y ejecutar acciones de respuesta y contención antes de que una amenaza logre comprometer los activos críticos de la entidad. A diferencia de un modelo de seguridad tradicional, basado en dispositivos de protección que operan de manera autónoma sin supervisión activa, un firewall que bloquea tráfico según reglas predefinidas, un antivirus que compara archivos contra una base de firmas conocidas, el SOC introduce el elemento que ninguna herramienta automatizada puede replicar por completo: el criterio experto humano, aplicado de manera continua, para interpretar patrones complejos, distinguir actividad legítima de actividad maliciosa sofisticada, y tomar decisiones de contención bajo presión durante un incidente activo.

El concepto de SOC surgió como evolución natural de los primeros equipos de respuesta a incidentes informáticos (los llamados CERT o CSIRT, por sus siglas en inglés) que empezaron a formarse a finales de la década de 1980, cuando las organizaciones comprendieron que la interconexión de redes generaba una superficie de exposición que ningún dispositivo aislado podía cubrir por sí solo. Con el paso de las décadas, y especialmente a partir de la masificación de internet, la nube pública, la movilidad empresarial y, más recientemente, la proliferación de dispositivos conectados (IoT), el volumen y la sofisticación de los eventos de seguridad que una organización debe procesar diariamente crecieron exponencialmente, haciendo inviable que un equipo de tecnología generalista, sin especialización ni dedicación exclusiva, pudiera identificar de manera oportuna las señales débiles que preceden a un compromiso de seguridad grave. El SOC nace precisamente para resolver ese problema: concentrar en un equipo dedicado, apoyado en tecnología especializada, la función de vigilancia permanente que la complejidad moderna de las amenazas exige.

Un SOC maduro se sostiene sobre tres pilares que deben operar de manera simultánea y coordinada: las personas, los procesos y la tecnología. Ninguno de estos tres pilares, por sí solo, constituye un SOC, es su integración funcional la que genera la capacidad real de defensa.

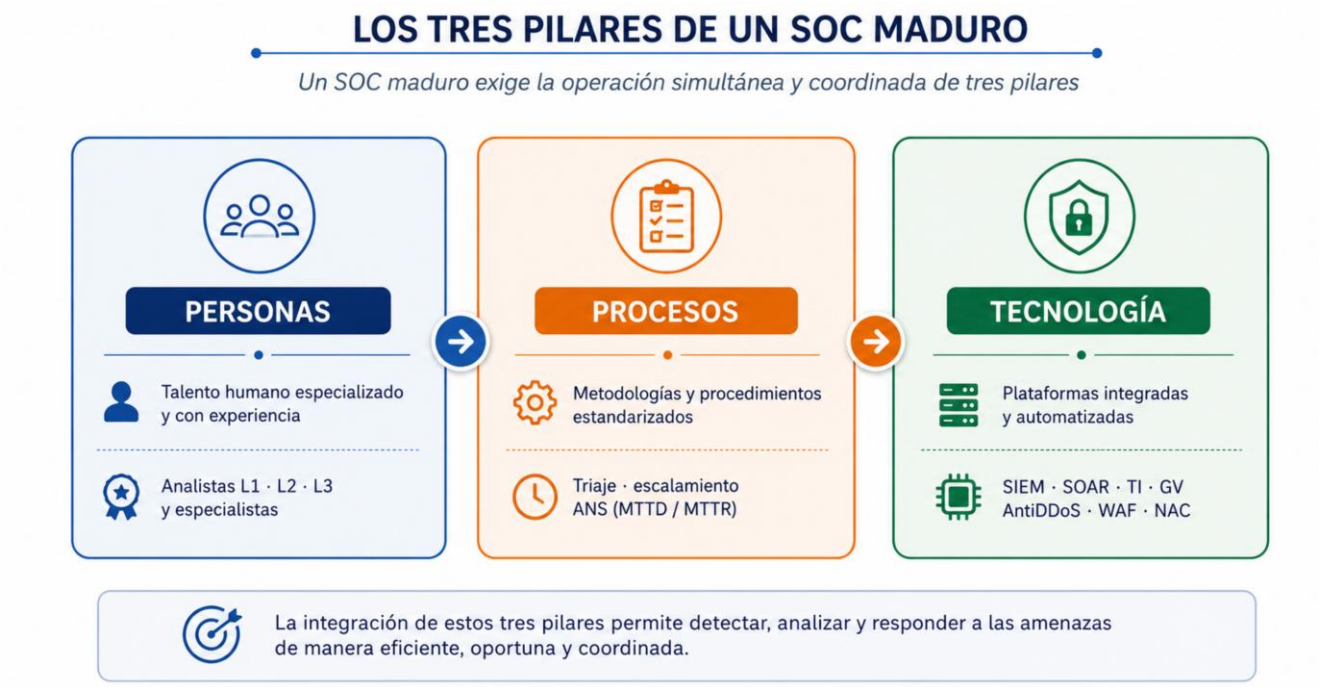


Figura 1. Pilares fundamentales de un Centro de Operaciones de Seguridad. Fuente: elaboración propia.

El pilar de las personas comprende un equipo de analistas de ciberseguridad organizados en niveles de experiencia y responsabilidad progresiva, comúnmente denominados Nivel 1 (L1), Nivel 2 (L2) y Nivel 3 (L3), complementados por especialistas de mayor profundidad técnica en áreas específicas. Los analistas de Nivel 1 constituyen la primera línea de defensa operativa: revisan de manera continua, durante toda su jornada de turno, las alertas generadas por las plataformas tecnológicas del SOC, aplicando criterios de triaje para determinar rápidamente si una alerta corresponde a un falso positivo (actividad legítima erróneamente marcada como sospechosa), por ejemplo un administrador de sistemas realizando un mantenimiento programado que genera un patrón de acceso inusual o si, por el contrario, presenta indicios suficientes para ameritar una investigación más profunda. La velocidad y precisión de este primer filtro es determinante: un SOC que reciba miles de alertas diarias sin un triaje eficiente termina generando lo que la industria denomina "fatiga de alertas", fenómeno mediante el cual los analistas, abrumados por el volumen de notificaciones, pierden progresivamente su capacidad de identificar señales genuinamente críticas entre el ruido.

Los analistas de Nivel 2 reciben los casos escalados por el Nivel 1 y ejecutan una investigación de mayor profundidad, correlacionando información proveniente de múltiples fuentes, registros de acceso, tráfico de red, comportamiento de endpoints, indicadores de amenaza para reconstruir la

línea de tiempo del evento, determinar su alcance real dentro de la infraestructura, e identificar si se trata de un incidente aislado o de una campaña más amplia. Es en este nivel donde se toman las primeras decisiones sustantivas de contención, como el aislamiento temporal de un equipo sospechoso o el bloqueo de una dirección IP de origen.

Los analistas de Nivel 3, con la mayor experiencia y especialización técnica del equipo, asumen la gestión de los incidentes de mayor severidad: ataques de ransomware en curso, amenazas persistentes avanzadas (APT, por sus siglas en inglés) que indican la presencia sostenida de un actor malicioso dentro de la red, o fugas de información sensible. Estos analistas lideran técnicamente la respuesta al incidente, coordinan las acciones de erradicación de la amenaza, y cuando la naturaleza del caso lo exige, ejecutan procedimientos de análisis forense digital — la disciplina que permite reconstruir, con rigor metodológico y preservando la cadena de custodia de la evidencia, qué ocurrió exactamente, cómo ingresó el atacante, qué sistemas comprometió y qué información pudo haber sido afectada, información que resulta indispensable tanto para la remediación técnica como para eventuales procesos disciplinarios, contractuales o penales derivados del incidente.

A este esquema de analistas por niveles se suman perfiles especializados que operan de manera transversal: el ingeniero de plataformas, responsable de la administración, configuración y optimización continua de las herramientas tecnológicas del SOC; el especialista en inteligencia de amenazas, encargado de investigar activamente el panorama de amenazas relevante para el sector y el perfil de riesgo específico de la organización; y el especialista en gestión de vulnerabilidades, responsable de la identificación y priorización sistemática de debilidades técnicas en la infraestructura.

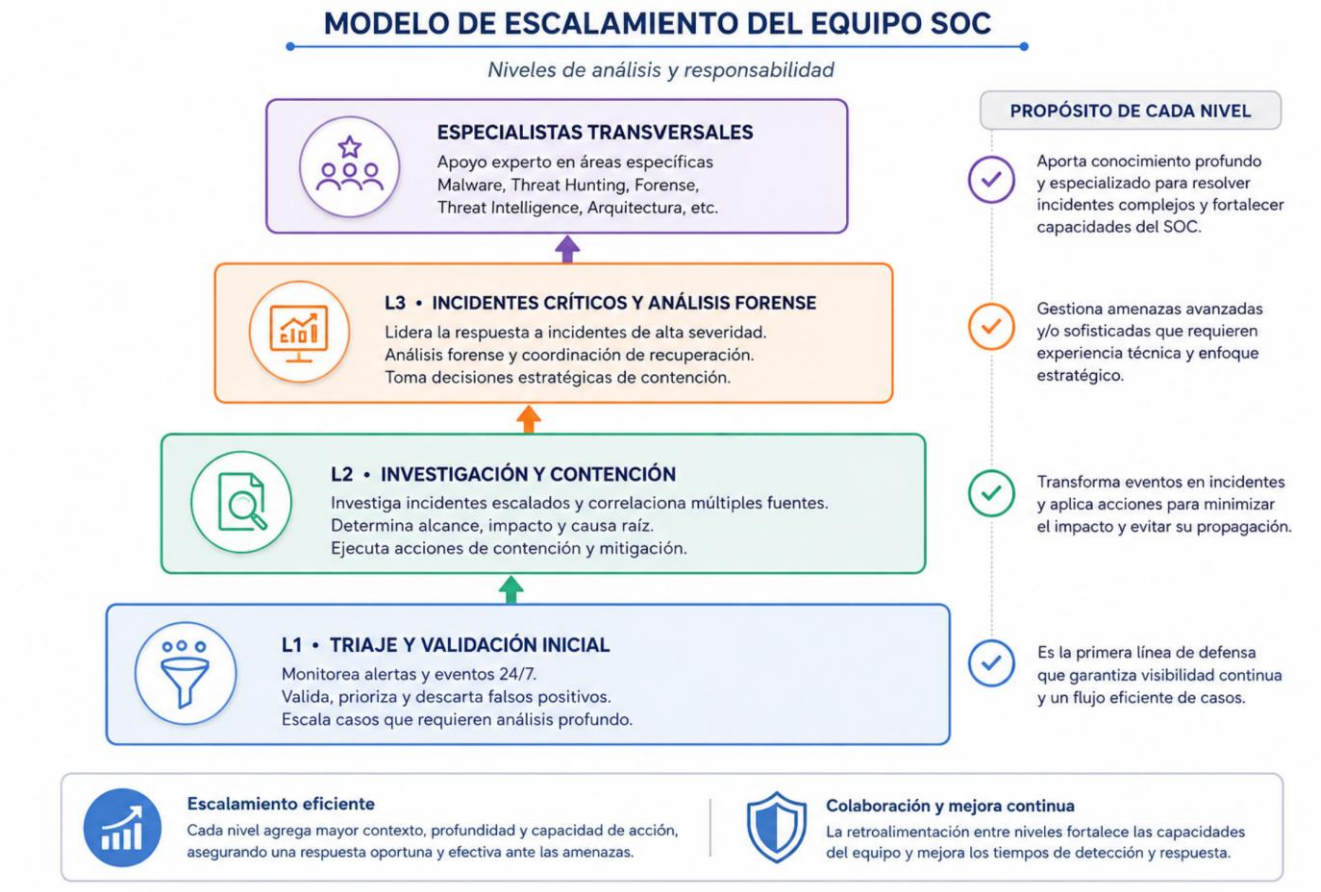


Figura 2. Modelo de escalamiento del equipo humano del SOC. Fuente: elaboración propia.

El pilar de los procesos: comprende el conjunto de procedimientos formales, documentados y estandarizados que rigen la operación diaria del SOC, garantizando que la calidad de la respuesta ante un incidente no dependa del criterio individual de quien esté de turno en un momento dado, sino de una metodología consistente, repetible y auditable. Estos procesos definen, entre otros aspectos: la matriz de clasificación de eventos según su criticidad (habitualmente clasificados en niveles como crítico, alto, medio y bajo, en función del impacto potencial sobre la confidencialidad, integridad o disponibilidad de la información y de la criticidad del activo afectado); los protocolos de escalamiento entre los distintos niveles de analistas y hacia las instancias directivas de la organización cuando la severidad del incidente lo amerita; los Acuerdos de Nivel de Servicio (ANS), que establecen los tiempos máximos permitidos entre la ocurrencia de un evento y su detección (comúnmente medido como MTTD, Mean Time To Detect) y entre la detección y la contención

efectiva (MTTR, Mean Time To Respond), diferenciados según la severidad del incidente; los procedimientos de documentación de cada caso gestionado, que generan un registro histórico auditable; y los mecanismos de comunicación con la organización cliente, incluyendo la periodicidad y el contenido de los informes ejecutivos y operativos.



Figura 3. Ciclo operativo continuo del SOC y métricas de detección y respuesta. Fuente: elaboración propia.

El pilar de la tecnología comprende el conjunto de plataformas especializadas que actúan, de manera figurada, como los sentidos y los brazos ejecutores del centro de operaciones recolectando información de toda la infraestructura, correlacionando eventos que de manera aislada pasarían desapercibidos, y en muchos casos ejecutando de forma automatizada las acciones de contención necesarias. A continuación, se describe en detalle cada una de estas herramientas, su función específica y el beneficio concreto que aporta a una entidad como el INVIAS.



Figura 4. Arquitectura funcional de las capacidades tecnológicas del SOC. Fuente: elaboración propia.

La primera y más determinante de estas plataformas es el **Sistema de Gestión de Información y Eventos de Seguridad**, conocido universalmente por sus siglas **SIEM**. El SIEM actúa como el cerebro correlacionador del SOC: recolecta de manera continua registros de actividad denominados técnicamente "logs" o eventos provenientes de la totalidad de los componentes de la infraestructura tecnológica de la organización, incluyendo servidores, estaciones de trabajo, dispositivos de red, firewalls perimetrales, aplicaciones institucionales, servicios en la nube, sistemas de autenticación y correo electrónico. Dado que cada una de estas fuentes genera sus registros en formatos distintos y con estructuras de datos propias, la primera función del SIEM es la normalización: transformar toda esta información heterogénea en un modelo de datos común que permita su análisis conjunto. Una vez normalizada la información, el SIEM aplica reglas de correlación lógicas que identifican patrones de comportamiento a partir de la combinación de múltiples eventos individuales que, vistos de manera aislada, no representarían ninguna anomalía.

El ejemplo clásico que ilustra este principio es el siguiente: un único intento fallido de inicio de sesión no constituye, por sí mismo, ningún indicio de amenaza cualquier usuario puede equivocarse al digitar su contraseña. Sin embargo, cientos de intentos fallidos de inicio de sesión, originados desde decenas de direcciones IP distintas ubicadas en países diferentes, ocurridos en un lapso de pocos minutos, y seguidos de un inicio de sesión exitoso desde una de esas direcciones, constituye un patrón que revela con alta probabilidad un ataque de fuerza bruta o de relleno de credenciales (credential stuffing) que culminó en un compromiso exitoso de la cuenta. Ningún dispositivo aislado ni el servidor de autenticación, ni el firewall, ni el antivirus del equipo afectado tiene, por sí solo, la visibilidad necesaria para identificar este patrón; solo un sistema que correlacione la información de todas las fuentes simultáneamente puede hacerlo.

Para el INVIAS, contar con un SIEM significa transformar la información dispersa que hoy generan sus treinta y uno (31) dispositivos de seguridad perimetral, sus servidores, su entorno de virtualización y sus servicios en la nube de Microsoft Azure y Microsoft 365, en una sola fuente de verdad correlacionada, capaz de revelar patrones de ataque que hoy, sin dicha correlación, permanecen invisibles hasta que el daño ya se ha materializado.

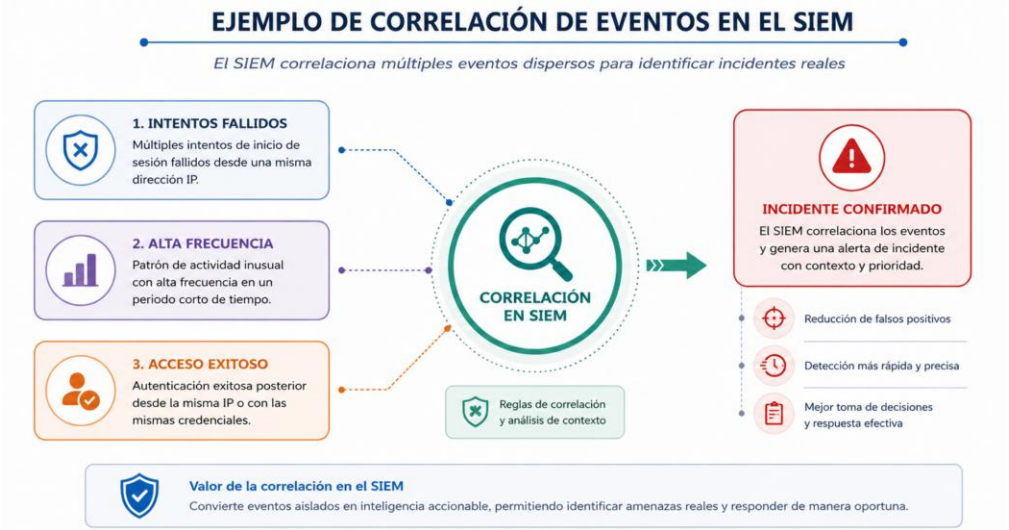


Figura 5. Ejemplo de correlación de múltiples eventos para identificar un incidente de alta confianza.

Fuente: elaboración propia.

La segunda plataforma es la de **Orquestación, Automatización y Respuesta de Seguridad, conocida por sus siglas SOAR.** Si el SIEM es el cerebro correlacionador, el SOAR constituye los brazos ejecutores del SOC. Una vez que el SIEM identifica una amenaza y los analistas la confirman como legítima, el SOAR permite ejecutar de manera automatizada, mediante flujos de trabajo

predefinidos denominados "playbooks", las acciones de contención correspondientes: aislar de la red un equipo comprometido, bloquear una dirección IP maliciosa en el firewall perimetral, deshabilitar una cuenta de usuario cuyas credenciales fueron comprometidas, o revocar sesiones activas sospechosas. La automatización de estas acciones reduce drásticamente el tiempo que transcurre entre la confirmación de una amenaza y su contención efectiva — un intervalo que, ejecutado manualmente por un analista que debe acceder a cada consola por separado, puede tomar minutos u horas, mientras que un playbook automatizado lo ejecuta en segundos.

El SOAR incorpora además un módulo de gestión del ciclo de vida de los incidentes, conocido como IRP (Incident Response Platform), que documenta de manera estructurada cada caso desde su apertura hasta su cierre, registrando las acciones ejecutadas, los tiempos de cada etapa, y las lecciones aprendidas, generando así la trazabilidad y el historial auditable indispensable para la mejora continua del SOC y para la rendición de cuentas ante la entidad contratante. Para el INVIAS, la implementación de un SOAR significa la diferencia entre que la contención de una amenaza dependa de que un analista humano ejecute manualmente, bajo presión y en tiempo real, una secuencia de pasos en múltiples consolas distintas, o que dicha secuencia se ejecute de manera automática, consistente y sin margen de error humano, en el instante mismo en que la amenaza es confirmada.

La tercera capacidad corresponde al servicio de inteligencia de amenazas, conocido en inglés como Threat Intelligence. Esta capacidad provee al SOC información actualizada, contextualizada y accionable sobre las tácticas, técnicas y procedimientos (TTPs, según la nomenclatura del marco internacional MITRE ATT&CK) que utilizan los actores de amenaza a nivel global, así como indicadores de compromiso concretos — direcciones IP maliciosas conocidas, dominios utilizados en campañas de phishing, hashes de archivos identificados como malware — que permiten al SIEM y a las demás plataformas del SOC bloquear proactivamente estas amenazas antes de que impacten la infraestructura, en lugar de esperar a detectarlas únicamente cuando ya han iniciado su actividad maliciosa dentro de la red.

Esta capacidad incluye adicionalmente el monitoreo de la huella digital externa de la organización, es decir, el rastreo sistemático de la información que sobre la entidad circula públicamente en internet y, de manera más sensible, en foros clandestinos y mercados de la denominada dark web, donde con frecuencia se comercializan credenciales robadas, accesos comprometidos o información filtrada de organizaciones específicas, así como la ejecución periódica de ejercicios de búsqueda proactiva de amenazas, conocidos como threat hunting, mediante los cuales analistas especializados examinan deliberadamente la infraestructura en busca de indicios de compromisos que no hayan activado ninguna alerta automática, partiendo de la premisa realista de que un atacante sofisticado puede permanecer oculto dentro de una red durante semanas o meses antes de ser detectado por medios convencionales. Para una entidad como el INVIAS, que administra infraestructura vial de carácter nacional y por tanto constituye un objetivo de interés para actores que buscan afectar infraestructura crítica del Estado, contar con inteligencia de amenazas actualizada significa anticipar campañas dirigidas específicamente al sector público colombiano antes de que se materialicen contra su propia infraestructura.

La cuarta capacidad tecnológica es la gestión de vulnerabilidades, que comprende el descubrimiento continuo de la totalidad de los activos tecnológicos de la organización — sean estos conocidos o desconocidos previamente por el equipo de tecnología, un fenómeno frecuente en entornos que han crecido de manera orgánica durante años —, la evaluación permanente de dichos activos en busca de vulnerabilidades técnicas (fallas de software documentadas públicamente, conocidas como CVE) y de configuraciones inseguras, y la priorización sistemática de la remediación con base en el riesgo real que cada vulnerabilidad representa para la infraestructura específica de la entidad, considerando factores como si la vulnerabilidad está siendo activamente explotada por atacantes a nivel mundial, la criticidad del activo afectado, y la existencia o no de un parche disponible.

Esta capacidad se complementa con la ejecución periódica de pruebas de penetración, mediante las cuales especialistas éticos simulan de manera controlada las técnicas que emplearía un atacante real, con el fin de identificar de manera proactiva las brechas de seguridad explotables antes de que un actor malicioso las descubra por su cuenta. Para el INVIAS, esta capacidad resulta especialmente crítica considerando la naturaleza híbrida de su infraestructura que combina un centro de datos propio con cargas de trabajo desplegadas en la nube pública de Microsoft Azure y sedes departamentales distribuidas en todo el territorio nacional, escenario en el cual la ausencia de visibilidad continua sobre el estado de vulnerabilidad de cada uno de estos entornos representa, precisamente, el tipo de brecha que actores maliciosos buscan y explotan.

En la capa de protección perimetral, un SOC de nivel corporativo se apoya en tres soluciones especializadas adicionales. La primera es el sistema de mitigación de ataques de denegación de servicio distribuido, conocido por sus siglas AntiDDoS, que protege la disponibilidad de los servicios institucionales expuestos a internet frente a intentos deliberados de saturar el ancho de banda de la red o la capacidad de procesamiento de los servidores mediante volúmenes masivos de tráfico malicioso generado simultáneamente desde miles de orígenes distintos un tipo de ataque que, de no ser mitigado en tiempo real, puede dejar fuera de servicio los portales y aplicaciones institucionales durante horas o días.

La segunda es el firewall de aplicaciones web, conocido por sus siglas WAF, que protege específicamente las aplicaciones institucionales expuestas a internet frente a los vectores de ataque más comunes contra este tipo de sistemas inyección de código malicioso en formularios web, intentos de acceso no autorizado a bases de datos a través de vulnerabilidades de la aplicación, o el aprovechamiento de fallas de programación para tomar control del servidor, vectores que un firewall perimetral tradicional, diseñado para inspeccionar tráfico de red genérico, no está en capacidad de identificar con la misma precisión que una herramienta especializada en el análisis del tráfico específico de aplicaciones web.

El WAF actualmente en operación en el INVIAS corresponde al fabricante Imperva, incorporado a la infraestructura de la entidad mediante el contrato de prestación de servicios No. 1353 de 2025 con Grupo Microsistemas Colombia S.A.S., descrito en la cronología de contratación del presente

estudio. Desde su implementación, esta plataforma ha acumulado políticas de seguridad, reglas de protección personalizadas para las aplicaciones institucionales del INVIAS y un historial de eventos y ajustes que reflejan el comportamiento específico del tráfico de la entidad. La continuidad de este mismo fabricante en el presente proceso de contratación no obedece a una preferencia comercial, sino a una justificación técnica de continuidad: migrar hacia un fabricante distinto obligaría a reconfigurar desde cero las políticas de protección ya afinadas, implicaría la pérdida del historial de eventos acumulado, y expondría a las aplicaciones institucionales expuestas a internet a una ventana de vulnerabilidad durante el período de transición. Esta continuidad tecnológica encuentra sustento en que la renovación o ampliación de bienes y servicios previamente contratados resulta procedente cuando busca garantizar la continuidad operativa, preservar la coherencia tecnológica y mantener el nivel de madurez alcanzado por una solución que ya se encuentra implementada y en funcionamiento dentro de la entidad.

La tercera es la solución de Control de Acceso a la Red, conocida por sus siglas NAC, que verifica la identidad y evalúa la postura de seguridad de cualquier dispositivo que intente conectarse a la red institucional sea este un equipo de cómputo corporativo, un dispositivo personal de un visitante, o un dispositivo de Internet de las Cosas como una cámara de videovigilancia o un sensor ambiental antes de permitirle el acceso, y que adicionalmente segmenta la red institucional en función del perfil de riesgo de cada dispositivo, de manera que, si un atacante logra comprometer un dispositivo de bajo privilegio, encuentre barreras efectivas que le impidan desplazarse lateralmente hacia los sistemas críticos de la organización.

Capas complementarias. AntiDDoS protege la disponibilidad; el WAF protege las aplicaciones web; y el NAC verifica, perfila y segmenta los dispositivos antes y durante su acceso a la red.

Finalmente, un SOC operado bajo modalidad de servicio gestionado requiere de dos componentes adicionales que garantizan su puesta en marcha y su sostenibilidad operativa en el tiempo: un proceso formal de implementación y despliegue, que instala, configura e integra entre sí la totalidad de las plataformas descritas, adaptándolas a la infraestructura específica de la organización y transfiriendo el conocimiento operativo necesario al equipo interno de tecnología; y una bolsa de horas especializadas prepagadas, que garantiza la disponibilidad inmediata de capacidad técnica de alto nivel de especialistas en respuesta a incidentes críticos, análisis forense digital, pruebas de penetración avanzadas o gestión de crisis para ser desplegada bajo demanda ante situaciones que superen el alcance de la operación rutinaria del SOC, sin que la organización deba iniciar un proceso de contratación adicional precisamente en el momento en que más urgentemente necesita dicha capacidad.

Descrito lo que es un SOC y las herramientas tecnológicas que lo componen, resulta necesario detenerse en las características cualitativas que distinguen a un SOC verdaderamente maduro y efectivo de uno meramente nominal, es decir, en aquellos atributos que determinan si el conjunto

de plataformas y personas descrito anteriormente funciona realmente como un ecosistema de defensa cohesionado, o si, por el contrario, opera como un conjunto de herramientas yuxtapuestas sin verdadera integración funcional entre sí.

La primera característica determinante es el grado de integración nativa entre las plataformas tecnológicas que componen el núcleo del SOC. Esta consideración conduce a un criterio de arquitectura ampliamente documentado y reconocido por la industria global de ciberseguridad: la reducción de la heterogeneidad tecnológica innecesaria y, principalmente, la exigencia de interoperabilidad verificable entre las plataformas centrales el SIEM, el SOAR, la inteligencia de amenazas, la gestión de vulnerabilidades y los controles perimetrales especializados, mediante modelos de datos compartidos, interfaces documentadas, conectores soportados y capacidades de automatización efectivamente probadas.

Esta característica no responde en modo alguno a una preferencia hacia una marca comercial determinada, sino a una consideración técnica objetiva, verificable y ampliamente documentada en la literatura especializada sobre operación de centros de seguridad: cuando las plataformas de un SOC provienen de fabricantes distintos entre sí, la comunicación entre ellas depende necesariamente de conectores desarrollados por terceros, o de integraciones construidas a la medida, que deben traducir la información generada en el formato propietario de un fabricante al formato propietario de otro. Cada una de estas traducciones constituye, simultáneamente, una oportunidad de pérdida de contexto en la información transmitida, una fuente de latencia adicional en la propagación de alertas e inteligencia entre plataformas, y un punto adicional de falla que debe mantenerse, actualizarse y probarse de manera independiente cada vez que cualquiera de los fabricantes involucrados modifica su plataforma, fenómeno que la industria ha denominado "fatiga de integración", y que se traduce en la práctica en que los equipos de seguridad terminan invirtiendo una porción significativa de su tiempo operativo en mantener funcionando las conexiones entre herramientas, en lugar de dedicar ese tiempo al análisis efectivo de amenazas.

Esta misma heterogeneidad de fabricantes se traduce, en la operación diaria de un SOC, en la necesidad de que los analistas deban monitorear simultáneamente múltiples consolas de administración independientes para vigilar una misma infraestructura práctica que la industria conoce coloquialmente como "swivel-chair operations", en referencia a la necesidad de que el analista gire físicamente su silla y su atención de una pantalla a otra para intentar correlacionar manualmente información que las herramientas, por provenir de orígenes distintos, no logran correlacionar automáticamente entre sí.

Esta fragmentación operativa incrementa sustancialmente el riesgo de fatiga de alertas ya mencionado, y constituye uno de los factores humanos más documentados en el análisis retrospectivo de fallas de detección ocurridas en incidentes de seguridad de gran escala a nivel mundial. Por el contrario, cuando las plataformas centrales de un SOC operan dentro de un ecosistema interoperable y debidamente soportado, pueden compartir un modelo de datos común, una taxonomía uniforme para la clasificación de eventos y activos, y mecanismos de comunicación estables y documentados, lo cual permite que la inteligencia de amenazas identificada en cualquier

punto del ecosistema se propague de manera instantánea hacia todos los demás componentes, que las acciones de contención se ejecuten sin depender de interfaces de programación externas cuya disponibilidad y comportamiento pueden variar de manera independiente al resto del sistema, y que exista un único responsable operativo y contractual frente a la organización evitando el escenario, frecuente en arquitecturas que combinan múltiples fabricantes sin necesidad técnica que lo justifique, en el cual, ante una falla de integración entre dos herramientas, cada proveedor involucrado atribuye la responsabilidad al otro, dilatando la solución del problema precisamente en el momento en que la organización más requiere que su ecosistema de defensa opere sin fricciones.

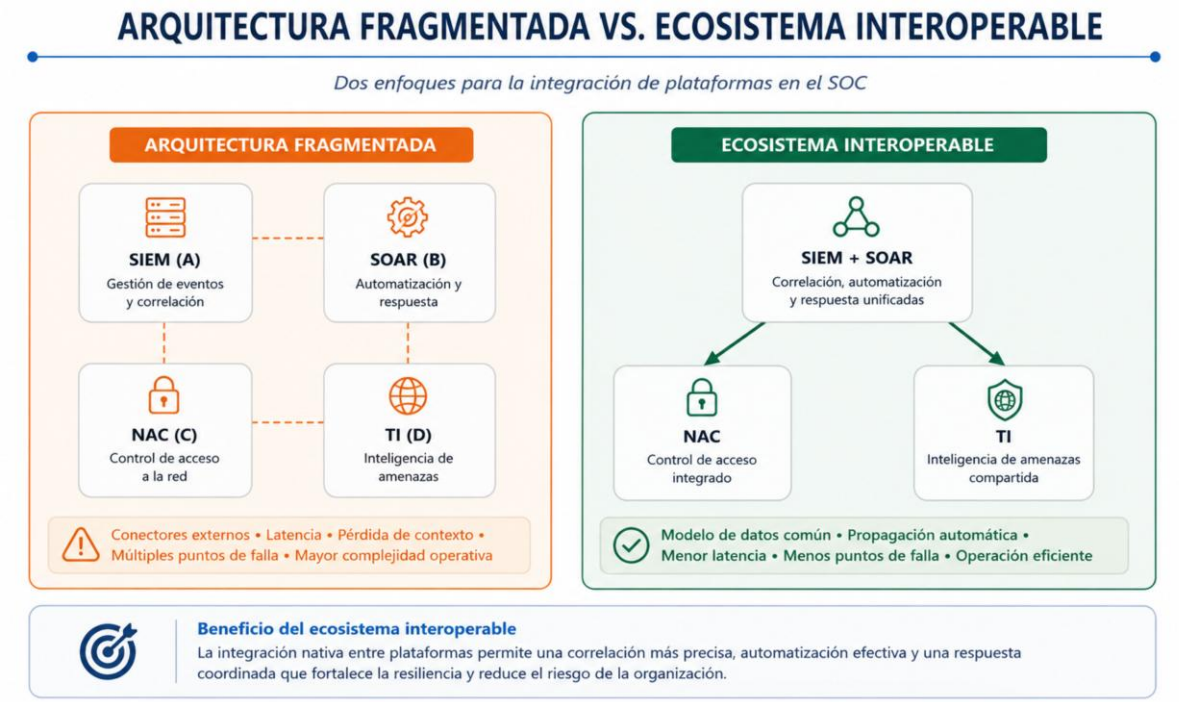


Figura 6. Comparación entre una arquitectura fragmentada y un ecosistema interoperable. Fuente: elaboración propia.

Criterio de neutralidad tecnológica. La necesidad de integración debe traducirse en condiciones objetivas y medibles de interoperabilidad, soporte, desempeño y automatización, evitando que el requisito dependa exclusivamente de la identidad del fabricante.

Una segunda característica igualmente determinante es la trayectoria y experiencia comprobada del operador del SOC en la implementación y gestión efectiva de las plataformas tecnológicas que integra. La ciberseguridad gestionada es, ante todo, una disciplina de ejecución: la disponibilidad de tecnología de última generación resulta insuficiente si el equipo humano que la opera carece de la experiencia práctica necesaria para configurarla correctamente, afinar sus reglas de detección conforme a la infraestructura específica de cada cliente, y responder con criterio experto ante los incidentes reales que dicha tecnología permite identificar. Un SOC operado por un equipo con trayectoria demostrada y con certificaciones vigentes de los fabricantes de las plataformas que administra ofrece garantías objetivas de que el conocimiento técnico requerido para extraer el máximo valor de dichas herramientas efectivamente existe dentro de la organización operadora, y no depende de un aprendizaje que se construya de manera improvisada durante la ejecución misma del servicio, con el riesgo correspondiente para la entidad que contrata dicho servicio precisamente para proteger su infraestructura más crítica.

Una tercera característica de un SOC de clase mundial, con frecuencia subestimada, pero de enorme relevancia práctica, es la pertenencia o articulación operativa de su equipo con la comunidad internacional coordinada por el FIRST — Forum of Incident Response and Security Teams. FIRST es la organización internacional decana y de mayor reconocimiento mundial en materia de respuesta a incidentes de seguridad informática, cuya idea se remonta a 1989 y que fue fundada en 1990, como respuesta a la necesidad de mejorar la coordinación entre los equipos de respuesta a incidentes que surgieron después de los primeros eventos de propagación masiva en internet. Actualmente, FIRST agrupa a más de ochocientos (800) equipos de respuesta a incidentes de seguridad — denominados técnicamente CERT o CSIRT provenientes de más de ciento diez (110) países alrededor del mundo, entre entidades gubernamentales, académicas, organismos multilaterales y empresas del sector privado de todas las industrias.

El propósito central de FIRST es fomentar la cooperación y la coordinación efectiva entre sus miembros en materia de prevención de incidentes, estimular una reacción rápida y coordinada frente a amenazas activas que trasciendan las fronteras de una sola organización o de un solo país, y promover el intercambio confiable de información sensible sobre amenazas entre sus miembros y la comunidad global de ciberseguridad. Para cumplir este propósito, FIRST no se limita a ser un espacio de encuentro informal, sino que ha desarrollado y mantiene activamente estándares técnicos de adopción prácticamente universal en la industria de la ciberseguridad a nivel mundial. El más relevante de estos estándares es el Common Vulnerability Scoring System (CVSS), el sistema de puntuación numérica de severidad de vulnerabilidades informáticas que constituye hoy el lenguaje común mediante el cual se comunica el nivel de criticidad de una vulnerabilidad, y que es utilizado por prácticamente la totalidad de las plataformas de gestión de vulnerabilidades disponibles en el mercado mundial, incluyendo la contemplada dentro de un SOC de nivel corporativo. FIRST mantiene además el Traffic Light Protocol (TLP), un protocolo estandarizado de clasificación y manejo de información sensible de inteligencia de amenazas que asigna colores (rojo, ámbar, verde y claro) a la información compartida entre organizaciones para señalar de manera inequívoca el nivel de restricción con que debe tratarse cada dato, protocolo que resulta indispensable para que distintas organizaciones puedan intercambiar entre sí inteligencia sensible

sobre amenazas activas con la confianza suficiente de que dicha información no será divulgada más allá de lo autorizado por quien la comparte.

La pertenencia a esta comunidad, o la articulación operativa demostrable con miembros de la misma, resulta relevante por al menos tres razones prácticas y verificables. En primer lugar, un equipo con articulación a la comunidad FIRST tiene acceso a canales de intercambio de inteligencia de amenazas que, por su propia naturaleza, no se encuentran disponibles públicamente ni a través de canales comerciales ordinarios incluyendo alertas tempranas sobre campañas de ataque activas identificadas por otros equipos miembros en cualquier parte del mundo, que con frecuencia terminan afectando posteriormente a organizaciones de otros países y sectores una vez que la técnica del atacante se replica o se comercializa entre distintos grupos criminales.

En segundo lugar, dado que Colombia registra antecedentes de participación de su ente coordinador nacional en esta comunidad desde 2013 y que ColCERT figura actualmente como equipo miembro de FIRST, un equipo operador de SOC con articulación equivalente facilita sustancialmente la coordinación técnica directa con dicho ente coordinador nacional ante incidentes que, por su naturaleza, magnitud o impacto sobre infraestructura crítica del Estado, deban ser escalados a dicha instancia, coordinación que resulta considerablemente más ágil cuando ambas partes comparten un mismo marco de referencia técnica, un mismo protocolo de clasificación de información sensible (el TLP ya mencionado), y canales de confianza previamente establecidos, que cuando dicha coordinación debe construirse desde cero en medio de un incidente activo.

En tercer lugar, el propio proceso de admisión a FIRST que exige la evaluación exhaustiva de la madurez operativa, los procedimientos formales documentados, y la capacidad técnica real del equipo postulante, evaluación que no se limita a una declaración de intención sino que es verificada activamente por el comité de membresía de la organización, que constituye en sí mismo un indicador objetivo, independiente y verificable de la idoneidad técnica de un equipo de respuesta a incidentes, comparable en su rigor a las certificaciones técnicas individuales que se exigen a los analistas del SOC, pero aplicado a nivel organizacional.



Figura 7. Relación entre FIRST, ColCERT y el operador del SOC. Fuente: elaboración propia.

Una cuarta característica indispensable de un SOC de clase mundial es su alineación con los marcos normativos y los estándares técnicos internacionales que rigen la gestión de la seguridad de la información, tanto a nivel global como en el ordenamiento jurídico colombiano específicamente aplicable a las entidades del Estado. En el plano internacional, la norma técnica ISO/IEC 27001 constituye el estándar de mayor reconocimiento y adopción mundial para los Sistemas de Gestión de Seguridad de la Información, estableciendo un marco sistemático mediante el cual una organización identifica, evalúa y trata los riesgos de seguridad de la información a los que está expuesta, a través de un ciclo continuo de mejora que abarca la totalidad de sus procesos, activos de información y controles técnicos y organizacionales.

Que el operador del SOC — o el alcance organizacional dentro del cual se presta el servicio — cuente con certificación ISO/IEC 27001 vigente y verificable no es un formalismo administrativo, sino la evidencia de que dicha organización ha sido auditada externamente y de manera independiente respecto del cumplimiento de un conjunto extenso y riguroso de controles de seguridad que abarcan desde la gestión de accesos hasta la continuidad del negocio, pasando por la gestión de incidentes, la criptografía, la seguridad física y la gestión de proveedores.

De manera complementaria a la norma ISO, el NIST Cybersecurity Framework, desarrollado originalmente por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (National Institute of Standards and Technology), se ha consolidado como un marco de referencia técnica de amplia adopción para estructurar de manera integral las capacidades de una organización frente al ciclo de vida completo de la gestión del riesgo cibernético.

En su versión 2.0, publicada en 2024, el marco organiza dichas capacidades en seis funciones centrales: gobernar, identificar, proteger, detectar, responder y recuperar. La función de gobernar articula la estrategia, los roles, las políticas, la supervisión y la gestión del riesgo; identificar comprende el conocimiento de activos, amenazas y vulnerabilidades; proteger reúne los controles preventivos; detectar busca reconocer oportunamente eventos adversos; responder comprende la contención, comunicación y gestión del incidente; y recuperar orienta el restablecimiento de capacidades y la incorporación de mejoras. Un SOC de nivel corporativo debe demostrar cómo sus capacidades tecnológicas y operativas apoyan integralmente estas seis funciones, sin presentar la operación del SOC como sustituto de las responsabilidades institucionales de gobierno, continuidad y recuperación que permanecen a cargo de la entidad.



Figura 8. Funciones del NIST Cybersecurity Framework 2.0. Fuente: NIST CSF 2.0; representación gráfica de elaboración propia.

En el plano específicamente colombiano, el Estado ha desarrollado durante la última década un cuerpo normativo progresivo en materia de seguridad digital, que resulta directamente aplicable a las entidades públicas y que un SOC contratado por una de dichas entidades debe estar en capacidad de respaldar en su operación. El Documento CONPES 3854 de 2016, mediante el cual se estableció la Política Nacional de Seguridad Digital, constituyó el primer marco institucional del país orientado a que las múltiples partes interesadas: el Gobierno nacional y territorial, las

organizaciones públicas y privadas, los propietarios u operadores de infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil gestionaran de manera preventiva, y no meramente reactiva, el riesgo de seguridad digital asociado a sus actividades, incorporando plenamente las recomendaciones y mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), lo cual posicionó a Colombia como el primer país de América Latina en adoptar dicho estándar.

Sobre esta base, el Documento CONPES 3995 de 2020, que estableció la Política Nacional de Confianza y Seguridad Digital, actualizó y profundizó dicho marco con el objetivo de desarrollar la confianza digital del país mediante el fortalecimiento de las capacidades nacionales de seguridad digital y la actualización del marco de gobernanza correspondiente.

En desarrollo de estas políticas, el Ministerio de Tecnologías de la Información y las Comunicaciones expidió la Resolución 500 de 2021, mediante la cual estableció los lineamientos y estándares para la estrategia de seguridad digital del Estado colombiano, y adoptó el Modelo de Seguridad y Privacidad de la Información — MSPI, concebido como habilitador directo de la Política de Gobierno Digital del país.

El MSPI está diseñado para conducir a las entidades públicas hacia la preservación efectiva de la confidencialidad, la integridad y la disponibilidad de su información institucional, mediante la aplicación sistemática de un proceso de gestión del riesgo que brinde confianza verificable a la ciudadanía y a las demás partes interesadas sobre la adecuada gestión de dichos riesgos por parte del Estado y se encuentra, de manera explícita y documentada por el propio MinTIC, fundamentado directamente en los requisitos y controles de la norma internacional ISO/IEC 27001 ya descrita, adoptando adicionalmente el NIST Cybersecurity Framework como fuente de buenas prácticas complementarias para las entidades que buscan robustecer su postura de seguridad más allá de los requisitos mínimos.

Finalmente, el Decreto 338 de 2022, expedido por la Presidencia de la República, adicionó el Título 21 a la Parte 2 del Libro 2 del Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la Información y las Comunicaciones, con el propósito específico de fortalecer la gobernanza de la seguridad digital del país, creando para ello el Modelo y las instancias institucionales de Gobernanza de Seguridad Digital correspondientes. Es precisamente bajo el marco de gobernanza establecido por este decreto, y por la política que le antecede, que opera el Grupo de Respuesta a Emergencias Cibernéticas de Colombia — COLCERT, creado originalmente en el marco del Documento CONPES 3701 de 2011 como el ente coordinador nacional de los asuntos de ciberseguridad y ciberdefensa del país.

Un SOC de nivel corporativo que opere en Colombia debe estar en capacidad de articularse de manera efectiva con este ente coordinador nacional, tanto para efectos de reporte de incidentes de impacto significativo como para la recepción de alertas e inteligencia de amenazas de origen nacional relevantes para el sector público; esta capacidad de articulación se ve sustancialmente

facilitada, como ya se explicó, cuando el operador del SOC mantiene también vínculo con la comunidad internacional FIRST de la cual el COLCERT es miembro, con antecedentes de participación institucional registrados desde 2013 y una ficha de membresía vigente del equipo COLCERT.

En síntesis, un SOC que reúna de manera simultánea estas cuatro características de integración e interoperabilidad verificables que reduzcan la heterogeneidad tecnológica innecesaria, trayectoria y experiencia operativa comprobada, articulación con la comunidad internacional de respuesta a incidentes coordinada por FIRST, y alineación verificable con los estándares ISO/IEC 27001 y NIST, así como con el marco normativo colombiano de seguridad digital constituye el estándar de referencia frente al cual debe evaluarse la idoneidad de cualquier solución de ciberseguridad gestionada que aspire a proteger de manera efectiva la infraestructura tecnológica de una entidad del sector público colombiano.

Para VIITS, estas características adquieren una aplicación concreta: la integración e interoperabilidad permiten relacionar los eventos de los componentes que soportan el proyecto; la experiencia del operador aporta el conocimiento necesario para interpretar esos eventos y responder ante incidentes; la cooperación con comunidades de ciberseguridad facilita el intercambio oportuno de inteligencia de amenazas; y la alineación con ISO/IEC 27001 y el NIST Cybersecurity Framework 2.0 proporciona un marco de procesos auditables, gestión del riesgo y mejora continua. Su articulación permite que la tecnología, los procesos, el talento humano y las capacidades de cooperación se orienten a la protección sostenida de la operación misional.

La entidad dispone de herramientas robustas de seguridad perimetral, protección de endpoints, infraestructura tecnológica y servicios de nube, adquiridas y fortalecidas mediante inversiones realizadas durante varios años. Sin embargo, estas capacidades operan actualmente sin un componente central que consolide y correlacione la información generada, identifique comportamientos anómalos y permita coordinar oportunamente las acciones de respuesta.

Esta condición genera una brecha estructural entre la información producida por las herramientas de seguridad y la capacidad institucional para convertirla en alertas procesables, decisiones oportunas y acciones coordinadas de contención, brecha que dejó de representar un riesgo meramente hipotético con el incidente ocurrido los días 9 y 10 de diciembre de 2025, cuando fueron comprometidos componentes críticos de la infraestructura tecnológica del INVIAS, incluidos entornos de virtualización, sistemas de información, bases de datos y mecanismos de respaldo.

En este contexto, la contratación del servicio permitirá fortalecer la postura de seguridad digital de la entidad en cuatro dimensiones fundamentales. La primera es la centralización y correlación de los eventos generados por los dispositivos de seguridad perimetral, los servidores, los entornos de virtualización, los servicios desplegados en la nube, los endpoints y las demás fuentes incluidas dentro del alcance contractual, lo cual permitirá obtener una visión unificada del estado de seguridad de la infraestructura y facilitará la identificación de patrones, secuencias de comportamiento e

indicadores de compromiso que hoy podrían no detectarse mientras la información permanezca distribuida entre plataformas que operan de manera independiente.

La segunda es la implementación de capacidades de orquestación, automatización y respuesta —SOAR —, apoyadas en procedimientos y playbooks previamente definidos, que permitirán reducir los tiempos requeridos para analizar, escalar y contener determinados eventos de seguridad; aunque la respuesta automatizada no sustituye la valoración de los especialistas ni la toma de decisiones institucionales, sí permite ejecutar de manera inmediata acciones previamente autorizadas —bloqueo de indicadores maliciosos, aislamiento de dispositivos, suspensión de conexiones o enriquecimiento de alertas—, limitando la propagación de un ataque durante sus fases iniciales y disminuyendo la probabilidad de que alcance componentes críticos, como los entornos de virtualización, las bases de datos o los sistemas de respaldo.

La tercera es la integración de inteligencia de amenazas, gestión continua de vulnerabilidades y análisis de exposición, que permitirá identificar debilidades técnicas, configuraciones inseguras, activos vulnerables e indicadores relacionados con campañas dirigidas contra entidades públicas o infraestructuras críticas, facilitando la priorización de las acciones de remediación de acuerdo con el nivel de criticidad del activo, la probabilidad de explotación, la exposición efectiva y el impacto potencial sobre la operación institucional, superando así un enfoque exclusivamente reactivo.

Y la cuarta es la disponibilidad de personal especializado y de una bolsa de horas para atender situaciones críticas, que permitirá al INVIAS contar con apoyo técnico oportuno ante incidentes que superen su capacidad operativa ordinaria, reduciendo la dependencia de gestiones de emergencia realizadas durante la materialización de un incidente y permitiendo activar procedimientos de análisis, contención, erradicación y recuperación con mayor oportunidad, coordinación y trazabilidad.

La relevancia de esta contratación se relaciona directamente con la continuidad de la gestión pública, la protección de los activos de información, la disponibilidad de los sistemas institucionales y la capacidad del INVIAS para cumplir sus funciones misionales. El Instituto administra información, procesos y plataformas que soportan la gestión de la infraestructura vial nacional; en consecuencia, una interrupción prolongada de sus servicios tecnológicos puede afectar la operación administrativa, técnica, contractual y financiera de la entidad, generando impactos que trascienden su funcionamiento interno.

En particular, para el Proyecto VIITS, el servicio gestionado de SOC permitirá mantener el monitoreo constante y fortalecer la protección de la infraestructura tecnológica crítica para la movilidad, cuyos sensores, cámaras, plataformas de monitoreo, redes de comunicaciones, centros de control y servicios en la nube operan de manera interconectada. De este modo, la centralización y el análisis de los eventos de seguridad contribuirán a identificar oportunamente situaciones que puedan comprometer la continuidad del proyecto y a coordinar las acciones de respuesta correspondientes.

Asimismo, dado que los sistemas inteligentes de transporte dependen de información confiable para

la gestión del tránsito, la movilidad y la toma de decisiones, el SOC contribuirá a preservar la integridad y confiabilidad de la información vial mediante la detección de alteraciones o manipulación de datos y la protección de la información proveniente de sensores, dispositivos de campo y sistemas de monitoreo y control. Este beneficio se relaciona directamente con el uso de los datos del proyecto por parte del Instituto y de las entidades con las cuales se interconecta.

En este sentido, el aprovechamiento integrado de las capacidades existentes de seguridad perimetral, protección de endpoints, servicios en la nube y demás controles tecnológicos permitirá dar continuidad a las inversiones realizadas y fortalecer su utilidad operativa. El análisis de registros y eventos, la priorización de vulnerabilidades según su criticidad e impacto y la respuesta especializada favorecerán la transición de un enfoque reactivo hacia uno preventivo, con el propósito de reducir la superficie de ataque y el riesgo de afectación a la operación vial nacional. Así, la protección de los recursos tecnológicos que soportan VIITS contribuye a reducir el riesgo de interrupción de servicios críticos para la movilidad y la transitabilidad.

No adelantar la contratación no significa conservar una condición estable. Por el contrario, implica mantener las brechas actuales de monitoreo, correlación, automatización y respuesta, mientras evolucionan las técnicas utilizadas por los actores de amenaza y aumenta la dependencia institucional de los sistemas de información, los servicios en la nube y la infraestructura tecnológica.

La contratación proyectada contribuye, además, al fortalecimiento de la gestión de riesgos de seguridad digital y a la aplicación de los lineamientos establecidos en el CONPES 3854 de 2016, el CONPES 3995 de 2020, el Decreto 338 de 2022 y el Modelo de Seguridad y Privacidad de la Información — MSPI —, tomando como referentes técnicos complementarios los estándares y buenas prácticas reconocidos internacionalmente, entre ellos ISO/IEC 27001 y el marco de ciberseguridad del NIST. En consecuencia, la contratación se encuentra justificada por la necesidad de cerrar una brecha institucional demostrada, fortalecer las capacidades preventivas y reactivas del INVIAS, reducir la probabilidad y el impacto de nuevos incidentes, y proteger la continuidad de los servicios tecnológicos que soportan su gestión misional.



Figura. Comparación del impacto institucional de contratar o no contratar el servicio SOC.

La comparación evidencia que la contratación no se orienta únicamente a incorporar nuevas herramientas, sino a integrar, operar y aprovechar de manera coordinada las capacidades ya existentes en la entidad, cerrando las brechas de visibilidad, correlación, automatización y respuesta identificadas a lo largo del presente estudio. Por lo anterior, el escenario de contratación ofrece una reducción sustancial de la exposición institucional y fortalece la capacidad del INVIAS para gestionar los riesgos de seguridad digital de manera preventiva, coordinada, trazable y acorde con la criticidad de los servicios que presta.

La adquisición de un Centro de Operaciones de Seguridad operado bajo modalidad de servicio gestionado, con las características descritas en el presente estudio previo frente a la integración e interoperabilidad verificables que reduzcan la heterogeneidad tecnológica innecesaria, trayectoria y experiencia operativa comprobada, articulación con la comunidad internacional FIRST y con el COLCERT nacional, y alineación verificable con los estándares ISO/IEC 27001, el NIST Cybersecurity Framework y el marco normativo colombiano de seguridad digital, no constituye entonces una opción entre otras igualmente válidas para el fortalecimiento tecnológico de la entidad,

sino la respuesta institucional idónea, proporcional, técnicamente fundamentada y urgente frente a una necesidad que la propia experiencia reciente del INVIAS ha puesto de manifiesto de la manera más contundente posible: la de contar, finalmente, con la capacidad de monitorear, correlacionar, detectar y responder de manera continua y especializada ante las amenazas cibernéticas que, como ha quedado demostrado, no son una posibilidad remota sino una realidad ya materializada contra la infraestructura tecnológica de la entidad, con el potencial de comprometer nuevamente, en cualquier momento, la continuidad de la gestión pública que el Instituto Nacional de Vías tiene a su cargo en beneficio de la conectividad, la transitabilidad y la movilidad de todos los colombianos.

La presente contratación se encuentra plenamente alineada con el Plan Estratégico de Tecnologías de la Información y las Comunicaciones — PETI 2025-2026 del INVIAS, en su tercera versión, aprobada por el Comité Institucional de Gestión y Desempeño el 28 de agosto de 2025. El PETI incorpora la Seguridad Digital como uno de los servicios permanentes del catálogo de servicios de TI de la entidad, definido como la capacidad de "gestionar y atender de manera eficaz y oportuna, los incidentes y/o eventos de seguridad digital que se presenten en los activos de información del INVÍAS", respecto de los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad — los mismos tres pilares sobre los que se estructuró el análisis de necesidad desarrollado en el presente estudio.

Dentro de las oportunidades de mejora identificadas por la OTIC para la implementación de la Política de Gobierno Digital en el período 2025-2026, el PETI define de manera expresa el lineamiento "Modelo de Seguridad y Privacidad de la Información y Seguridad Digital", que contempla, entre sus acciones prioritarias: la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI); la implementación del plan de tratamiento de riesgos de seguridad de la información; la realización de auditorías internas, externas y de certificación o recertificación respecto al estándar ISO/IEC 27001; la elaboración del análisis de impacto del negocio, el plan de continuidad de negocio y el plan de recuperación de desastres; la contextualización y aprobación de la Política de Ciberseguridad institucional; la elaboración de un informe de cumplimiento de las políticas de ciberseguridad por parte de proveedores y contratistas; el monitoreo de la disponibilidad de la sede electrónica conforme a los lineamientos del CSIRT Gobierno; y la implementación de indicadores para medir la caracterización de los incidentes de seguridad digital. La totalidad de estas acciones encuentra en el presente proceso de contratación el instrumento idóneo para su materialización, en la medida en que el Centro de Operaciones de Seguridad objeto de este estudio provee precisamente la capacidad operativa de monitoreo continuo, gestión de incidentes, tratamiento de vulnerabilidades y reporte de disponibilidad que dichas acciones del PETI presuponen.

Adicionalmente, el PETI identifica de manera explícita, dentro de su portafolio de proyectos institucionales asociados a tecnologías de la Cuarta Revolución Industrial, el proyecto "Actualización de la Seguridad Informática", categorizado bajo el componente de Ciberseguridad, en el marco del proyecto de inversión registrado ante el Departamento Nacional de Planeación con código BPIN C-2499-0600-21-51102D-2499062-02, denominado "Renovación, Actualización y Mantenimiento de

las Tecnologías de la Información y las Comunicaciones en el INVÍAS. Nacional", cuyo objetivo general consiste en "disponer de información confiable y segura para la toma de decisiones" y cuyo objetivo específico busca "reducir la brecha entre los objetivos estratégicos de la entidad y los lineamientos de sistemas de información y tecnología, mediante la automatización de los procesos, para garantizar la seguridad y confiabilidad de la información". El presente proceso de contratación constituye la ejecución directa de dicho proyecto de inversión en su componente de ciberseguridad, con cargo a los recursos apropiados dentro del producto "Servicios Tecnológicos" del referido proyecto BPIN.

En consecuencia, la contratación del Centro de Operaciones de Seguridad y sus servicios asociados no solo responde a la necesidad institucional evidenciada por el incidente de diciembre de 2025 y al marco normativo nacional de seguridad digital desarrollado en el presente estudio, sino que constituye además el mecanismo de ejecución formal de las metas ya trazadas por la propia entidad en su instrumento de planeación estratégica de TI vigente, garantizando la coherencia entre la planeación institucional y la contratación que aquí se sustenta.

A la relación entre la necesidad operativa y la planeación institucional se suma la continuidad temporal requerida para la prestación del servicio. Conforme a la justificación de vigencia futura, la contratación del servicio gestionado de Centro de Operaciones de Seguridad —SOC— no puede ejecutarse dentro de una sola vigencia fiscal: la implementación de las plataformas tiene un plazo de doce (12) semanas y la suscripción del servicio rige por un (1) año contado desde la activación de la totalidad de los productos contratados. En consecuencia, aunque el contrato se suscriba en la vigencia 2026, la operación efectiva del SOC se prestará de manera sustancial en la vigencia 2027. Esta secuencia responde a la naturaleza del servicio y a la necesidad de completar su implementación antes de desarrollar la operación durante el período previsto.

Por ello, la continuidad del monitoreo entre una vigencia y la siguiente constituye una condición necesaria para atender la necesidad descrita, especialmente frente a la operación permanente de VIITS y de la infraestructura del INVIAS utilizada para su funcionamiento. Las suscripciones de las plataformas son anuales e indivisibles, mientras que la implementación corresponde a una inversión única que se amortiza durante la prestación del servicio. Fraccionar la atención de esta necesidad por años calendario podría generar períodos sin cobertura y afectar la continuidad del monitoreo, la correlación de eventos y la respuesta especializada.

Adicionalmente, contratar por vigencias sucesivas obligaría a repetir la estructuración y sujetaría la continuidad del servicio a los tiempos de apropiación y contratación de los primeros meses de cada año. Esta situación podría dejar la infraestructura sin monitoreo, correlación ni respuesta durante la estabilización del servicio y obligar a reimplementar configuraciones, reglas de correlación y playbooks ya ajustados al entorno del Instituto. La previsión de un solo compromiso plurianual busca asegurar la continuidad, dar certeza de precio y evitar la duplicación de los esfuerzos y costos asociados a la curva de implementación.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

En este contexto, la gestión y autorización del trámite de vigencia futura se relaciona con la necesidad de disponer de los recursos para sostener la operación del SOC durante el período previsto y evitar interrupciones que comprometan la protección de VIITS y de la infraestructura tecnológica que lo soporta. No contar con dicha continuidad mantendría la exposición a incidentes con posibles consecuencias sobre la seguridad vial nacional, la articulación del Instituto con las demás entidades del Estado y la seguridad de la información institucional. Por tanto, la justificación temporal complementa la necesidad técnica y misional desarrollada en este documento.

La presente contratación se encuentra incluida en el Plan Anual de Adquisiciones del INVIAS para la vigencia 2026, y Se verificó la información publicada en el portal oficial de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente y en el catálogo público de la Tienda Virtual del Estado Colombiano, sin identificar, un Acuerdo Marco de Precios de ciberseguridad vigente y disponible para la adquisición de los bienes y servicios objeto del proceso.

Como antecedente, el proceso CCENEG-094-1-2026, orientado a seleccionar proveedores de bienes y servicios de ciberseguridad, fue suspendido mediante la Resolución 463 del 24 de julio de 2026. Posteriormente, según información oficial de la Procuraduría General de la Nación, Colombia Compra Eficiente revocó su apertura mediante la Resolución 566 del 22 de septiembre de 2026, dejando sin efectos el procedimiento.

Por lo anterior, a la fecha, NO EXISTE un Acuerdo Marco de precios que satisfaga la necesidad de la entidad, razón por la cual se adelanta el presente proceso de contratación de conformidad con la Ley 80 de 1993, la Ley 1150 de 2007 y el Decreto 1082 de 2015.

2. ANÁLISIS TÉCNICO Y ECONÓMICO DEL SECTOR

El sector de las tecnologías de información y comunicaciones en Colombia cuenta con gran potencial humano, logístico y técnico el cual se ha venido desarrollando desde hace más de una década con el propósito de convertir a Colombia en una sociedad digital, buscando acercar a la ciudadanía a la tecnología, logrando que se destaque en Latinoamérica y en el mundo, en la que todos los ciudadanos del territorio, bien sea de zonas urbanas o rurales, están conectados con calidad, seguridad y sostenibilidad.

El plan estratégico 2023-2026 "Conectividad y Tecnología para cambiar la vida" del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, tomado de: https://mintic.gov.co/portal/715/articles-334069_plan_estrategico_01.pdf (MinTIC, 2024), y consultado nuevamente en mayo del 2026 presenta tres líneas estratégicas para dar cumplimiento al Plan Nacional de Desarrollo. Dichas líneas son:

- Conectividad reducción de la brecha digital y la pobreza
- Tecnologías que transforman

- Educación digital

Ahora bien; con el fin de reducir la brecha digital en el país, estas líneas estratégicas buscan realizar transformaciones en seguridad humana, justicia social, transformación productiva, convergencia regional a través de indicadores PND. El cumplimiento de estos indicadores permite mejorar aspectos como la conexión en las zonas más apartadas del país, puntos de internet en los municipios, fortalecer la industria del software, creación de centros de investigación y el uso de la tecnología para acompañar los procesos de educación.

En general, se puede afirmar que en Colombia el sector de las TIC hace parte fundamental de su desarrollo y por ello el Gobierno nacional a través del MinTIC se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las TIC.

El sector de las TIC hace referencia a la digitalización del estado y la adopción de procesos productivos que cumplan con los estándares más avanzados en términos tecnológicos. El sector de las tecnologías de información y comunicaciones, de acuerdo con el Ministerio TIC es promotor de programas y proyectos que fortalecen las competencias ciudadanas digitales de acuerdo con el contexto de cada región y establece alianzas público-privadas bajo un modelo que le genera desarrollo al país.

En la actualidad, el MinTIC trabaja en diferentes metas, en los cuales se deben identificar iniciativas para prestar asistencia técnica y financiación, algunas de ellas son:

1. Gestión integral de espectro para el incremento del bienestar social
2. Apoyo financiero a Computadores para Educar
3. Internet Seguro y Responsable
4. Cultura de seguridad digital para prevención y preparación del estado colombiano
5. Fortalecimiento del sector TIC y Postal
6. Fortalecer la Industria Digital Nacional

En este contexto, el Instituto Nacional de Vías – INVÍAS, formuló el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) 2024-2026 (INVIAS, potencia tecnológica de la vida), por medio del cual se busca modernizar la entidad mediante la implementación de estrategias de transformación digital. En línea con políticas gubernamentales y objetivos nacionales, el plan tiene como meta cerrar la brecha digital y generar oportunidades para los colombianos. Se enfoca en mejorar la conectividad, fortalecer la seguridad cibernética y promover el desarrollo de ciudades inteligentes. El PETI es un proceso dinámico que requiere revisión y actualización anual para adaptarse a los cambios del sector y las necesidades institucionales. Su éxito depende del apoyo de la alta gerencia y la implementación eficaz de proyectos de inversión en TIC.

2.1 OPERACIÓN Y CADENA DE DISTRIBUCIÓN

Para impulsar el desarrollo, producción y comercialización de las TIC de las empresas asociadas al sector, se han conformado diversos gremios empresariales cuyo objetivo es potencializar los servicios de los agremiados en el mercado, local y globalmente, mediante estrategias académicas, económicas y de cooperación.

Además de lo anterior, dichas agremiaciones se encargan de velar y representar los intereses del sector ante los diversos entes gubernamentales, opinión pública, entidades extranjeras y ciudadanía en general.

La Entidad, identifica dos formas de operación en la comercialización de servicios de TI:

1) Directa (60% de las ventas):

   El oferente contacta y vende soluciones al usuario final.

   - Algunos, exclusivamente en esta modalidad.
   - Algunos en forma mixta con Asociados o Aliados para integrar una Solución.

2) A través de Asociados o Aliados (Subcontratistas) (40% de las ventas): las soluciones se ofrecen a través de VARs (canales que agregan valor en su proceso de venta), integradores, o canales especializados por nicho o geográficamente y para algunas funciones a través de centros autorizados de servicio certificados.

De esta manera, el esquema general es:

Fabricante: Mediante mecanismos de venta

- Directa
- A través de Intermediario

Integrador: A través de la siguiente cadena de distribución

- Fabricantes
- Directo
- Intermediario
- Subcontratistas

En Servicios: la estructura se da por mercados verticales

- Gobierno
- Salud
- Educación

- Finanzas
- Comercio
- Telecomunicaciones
- Minería y Petróleo

PERSPECTIVA ECONÓMICA

De conformidad con lo establecido en el artículo 2.2.1.1.1.6.1. del Decreto 1082 de 2015, y en concordancia con el Manual de Colombia Compra Eficiente - *"Guía para la elaboración de estudios del sector*" se procede a elaborar el análisis necesario para conocer el sector relativo al objeto del presente proceso contractual, así:

2.2 IDENTIFICACIÓN DEL SECTOR

El presente proceso se enmarca en el **MACRO SECTOR** económico **DEL SERVICIO**, clasificándose respectivamente en el **SECTOR TERCIARIO**.

El objeto contractual no corresponde únicamente al suministro de bienes tecnológicos, sino principalmente a la prestación de servicios especializados de ciberseguridad, soportados en plataformas tecnológicas, licenciamiento, infraestructura en la nube y personal altamente calificado, cuya finalidad es fortalecer la capacidad institucional para prevenir, detectar, analizar y responder oportunamente a incidentes de seguridad informática.

Desde el punto de vista del mercado, en Colombia existe una oferta amplia de empresas especializadas en servicios de ciberseguridad, conformada por fabricantes, distribuidores autorizados, integradores tecnológicos, proveedores de servicios administrados (MSSP) y empresas consultoras en seguridad de la información, que cuentan con la capacidad técnica, financiera y operativa para ejecutar este tipo de proyectos, garantizando condiciones de competencia, pluralidad de oferentes y disponibilidad de soluciones acordes con las necesidades de las entidades públicas.

En consecuencia, el presente proceso contractual se desarrolla dentro de un mercado altamente especializado, dinámico y en permanente evolución tecnológica, caracterizado por una creciente demanda de soluciones de ciberseguridad como resultado de la transformación digital, la adopción de servicios en la nube, el incremento de las amenazas cibernéticas y el fortalecimiento de las políticas de seguridad digital y continuidad de los servicios institucionales.

2.3 INDICADORES ECONÓMICOS

Los indicadores económicos constituyen herramientas que permiten analizar el comportamiento de la economía y del mercado en el cual se desarrolla el objeto contractual. Su análisis facilita la identificación de variables que pueden incidir en la estructuración del proceso de contratación, tales

como la oferta y demanda del sector, la inflación, la tasa representativa del mercado (TRM), los costos de prestación de servicios especializados y las condiciones generales del mercado de Tecnologías de la Información y las Comunicaciones (TIC).

El presente proceso se encuentra enmarcado en el sector terciario o de servicios, por cuanto comprende la prestación de servicios especializados de ciberseguridad, orientados a la protección de la infraestructura tecnológica institucional mediante la operación de un Centro de Operaciones de Seguridad (SOC), el monitoreo continuo de eventos e incidentes de seguridad, la gestión de vulnerabilidades, la inteligencia de amenazas, la protección de aplicaciones y demás servicios administrados de seguridad informática.

La contratación de estos servicios contribuye a fortalecer la seguridad digital del Instituto Nacional de Vías – INVÍAS, garantizando la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de la operación de los servicios tecnológicos institucionales y el cumplimiento de las políticas de Gobierno Digital y seguridad de la información.

Para efectos del presente estudio, el proceso se clasifica de la siguiente manera:

- **Sector económico:** Tecnologías de la Información y las Comunicaciones (TIC).
- **Subsector:** Ciberseguridad y Seguridad Digital.
- **Tipo de mercado:** Servicios especializados de Tecnologías de la Información y la Ciberseguridad.

2.3.1 TASA REPRESENTATIVA DEL MERCADO (TRM)[1]

Los indicadores económicos son datos estadísticos sobre la economía que nos permiten realizar un análisis de la situación económica tanto para el pasado como para el presente y además nos permite realizar previsiones de cómo evolucionará la economía en el futuro con los datos que tenemos hoy en día, entre los principales indicadores encontramos:

2.3.1 TASA REPRESENTATIVA DEL MERCADO (TRM)

La Tasa de Cambio Representativa del Mercado–TRM corresponde al promedio ponderado de las operaciones de compra y venta de contado de dólares de los Estados Unidos de América a cambio de moneda legal colombiana.

La Tasa de Cambio Representativa del Mercado–TRM corresponde al promedio ponderado de las operaciones de compra y venta de contado de dólares de los Estados Unidos de América a cambio de moneda legal colombiana.

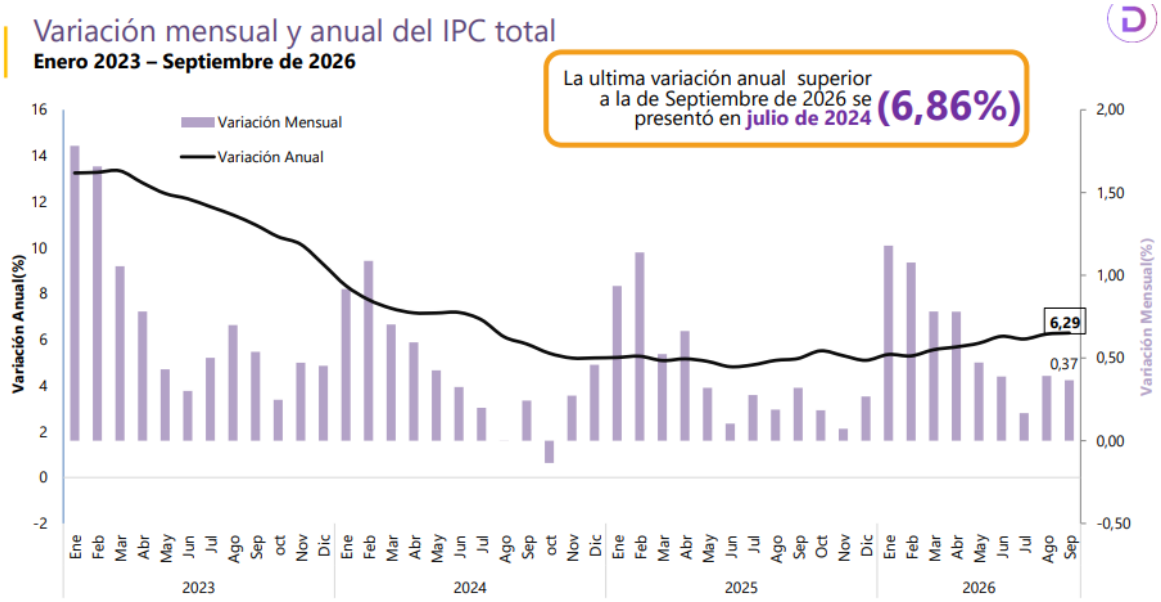


Fuente: Superfinanciera disponible en https://www.superfinanciera.gov.co/powerbi/reportes/514/482/

2.3.2 INDICE DE PRECIO AL CONSUMIDOR (IPC) 2026

El IPC es una investigación estadística que permite medir la variación porcentual promedio de los precios al por menor entre dos periodos de tiempo, de un conjunto de bienes y servicios de consumo final que es representativa del gasto de los hogares del país. El indicador es utilizado para la toma de decisiones, tanto del gobierno como de los entes privados, al tiempo que permite analizar situaciones de carácter económico.

la evolución del IPC en los últimos años, se puede observar el siguiente gráfico que muestra la variación mensual y anual que ha tenido la inflación en Colombia en cada uno de los meses desde 2023 hasta 2026:



Fuente: Presentación Principales Resultados IPC Septiembre 2026

Como se puede observar, desde 2023 hasta 2026 la variación del IPC revela importantes tendencias inflacionarias en el país. En el 2023 se observa un contexto de elevada inflación, seguido por un proceso sostenido de desaceleración manteniéndose relativamente estable a partir del 2024 y 2025.

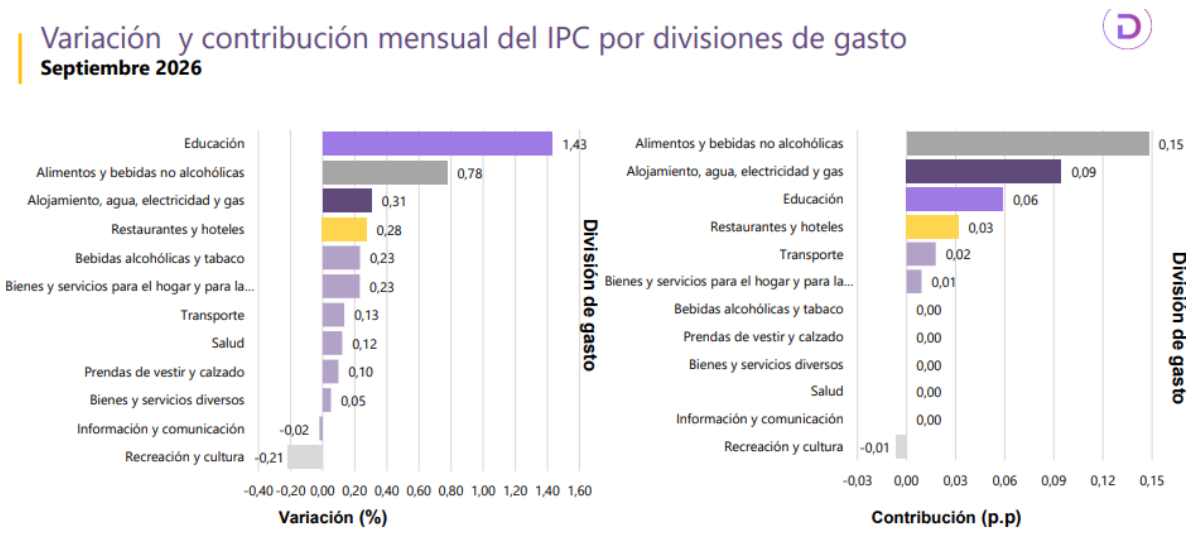
En la siguiente tabla se puede encontrar el histórico de la variación del IPC en los últimos 5 años:

Año	Inflación anual
2025	5,10 %
2024	5,20 %
2023	9,28 %
2022	13,12 %
2021	5,62 %

RESULTADOS DEL MES DE SEPTIEMBRE 2026

En el mes de septiembre de 2026, el IPC registró una variación de 0,37% en comparación con agosto de 2026, dos divisiones se ubicaron por encima del promedio nacional: Educación (1,43%) y, por último, Alimentos y bebidas no alcohólicas (0,78%). Por debajo se ubicaron: Alojamiento, agua, electricidad, gas y otros combustibles (0,31%), Restaurantes y hoteles (0,28%), Bebidas alcohólicas

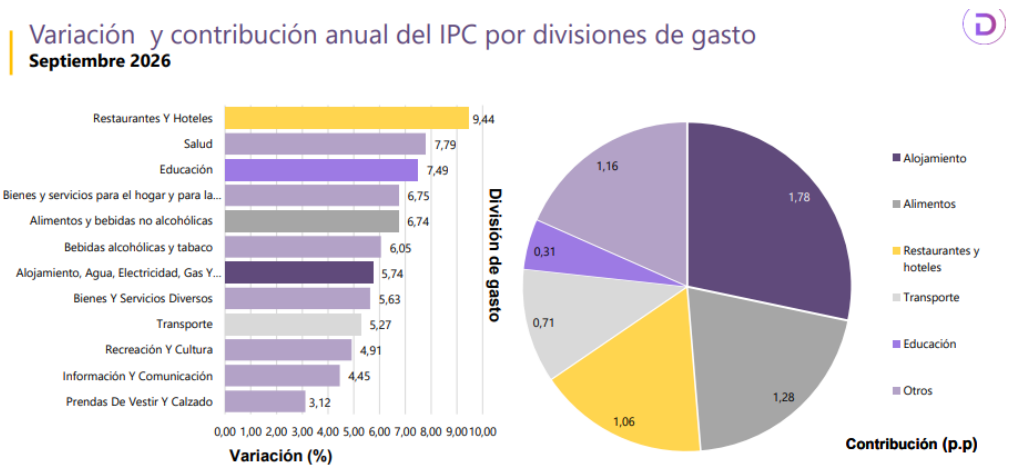
y tabaco (0,23%), Muebles, artículos para el hogar y para la conservación ordinaria del hogar (0,23%), Transporte (0,13%), Salud (0,12%), Prendas de vestir y calzado (0,10%), Bienes y servicios diversos (0,05%), Información y comunicación (-0,02%) y, por último, Recreación y cultura (-0,21%).



Fuente: Presentación Principales Resultados IPC Septiembre 2026

VARIACIÓN ANUAL (SEPTIEMBRE DE 2025 A SEPTIEMBRE DE 2026)

En septiembre de 2026 la variación anual del IPC fue 6,29%. Esta variación se explicó principalmente por la variación anual de las divisiones Restaurantes y hoteles (9,44%), Salud (7,79%), Educación (7,49%),.



Fuente: Presentación Principales Resultados IPC Septiembre 2026

En el mes de septiembre de 2026, el IPC registró una variación de 6,29% en comparación con septiembre de 2025. En el último año, las divisiones Restaurantes y hoteles (9,44%), Salud (7,79%), Educación (7,49%), Muebles, artículos para el hogar y para la conservación ordinaria del hogar (6,75%) y, por último, Alimentos y bebidas no alcohólicas (6,74%) se ubicaron por encima del promedio nacional. Entre tanto, las divisiones Bebidas alcohólicas y tabaco (6,05%), Alojamiento, agua, electricidad, gas y otros combustibles (5,74%), Bienes y servicios diversos (5,63%), Transporte (5,27%), Recreación y cultura (4,91%), Información y comunicación (4,45%) y, por último, Prendas de vestir y calzado (3,12%) se ubicaron por debajo del promedio nacional

IPC SEGÚN NIVELES DE INGRESO POR CRITERIO ABSOLUTO

Cuadro 7. IPC según niveles de ingreso por criterio absoluto
Total IPC
Septiembre 2025 - 2026

	Variación (%)					
	Mensual		Año Corrido		Anual	
	2025	2026	2025	2026	2025	2026
Pobres	0,26	0,41	4,57	5,74	5,21	6,14
Vulnerables	0,26	0,39	4,58	5,83	5,15	6,22
Clase media	0,31	0,38	4,55	5,73	5,17	6,30
Ingresos altos	0,38	0,32	4,54	5,69	5,20	6,32
Total nivel de ingresos	0,32	0,37	4,55	5,74	5,18	6,29

Fuente: DANE, IPC.

En septiembre de 2026, la variación mensual del IPC por nivel de ingresos fue: Pobres (0,41%),

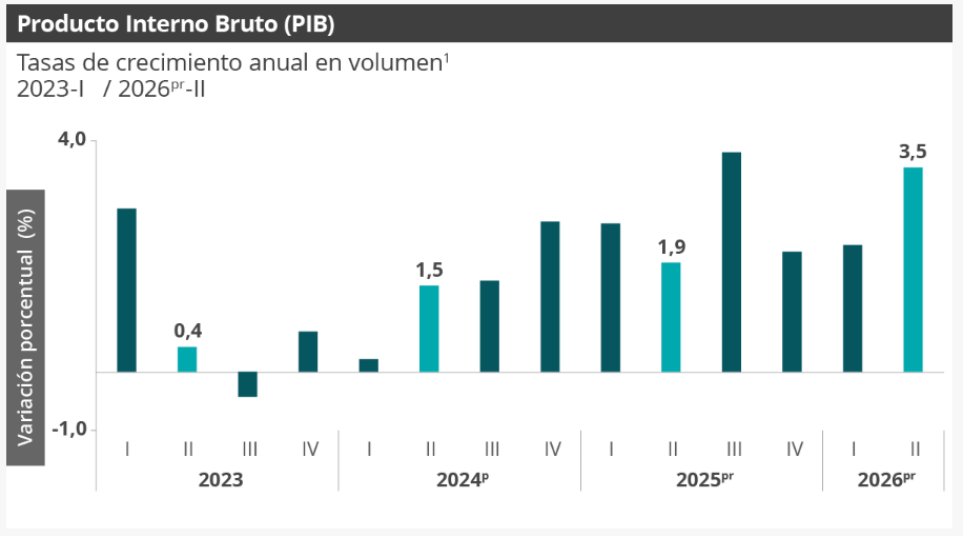
Vulnerables (0,39%), Clase media (0,38%), Ingresos altos (0,32%) y, por último, Total nivel de ingresos(0,37%).

En lo corrido del año, la variación del IPC por nivel de ingresos fue: Pobres (5,74%), Vulnerables (5,83%), Clase media (5,73%), Ingresos altos (5,69%) y, por último, Total nivel de ingresos (5,74%).

La variación anual del IPC por nivel de ingresos fue: Pobres (6,14%), Vulnerables (6,22%), Clase media (6,30%), Ingresos altos (6,32%) y, por último, Total nivel de ingresos (6,29%).

2.3.3 PRODUCTO INTERNO BRUTO (PIB)[1]

Es la representación del resultado final de la actividad productiva del total de las unidades de producción residentes. Es un agregado que caracteriza la economía en su conjunto. Se deriva básicamente del concepto de valor agregado. El valor agregado bruto es la diferencia entre la producción y el consumo intermedio. El PIB es la suma del valor agregado bruto de todas las unidades de producción residentes más la parte (posiblemente el total) de los impuestos, menos las subvenciones, sobre los productos, no incluida en la valoración de la producción. En el segundo trimestre de 2026, el Producto Interno Bruto en su serie original, crece 3,5% respecto al mismo periodo de 2025.



Fuente: DANE

Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

[1] https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

• Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 10,0% (contribuye 1,7 puntos porcentuales a la variación anual).

• Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 2,2% (contribuye 0,5 puntos porcentuales a la variación anual).

Tabla 1. Producto Interno Bruto (PIB)
Enfoque de la producción
Tasas de crecimiento (%) anual y trimestral en volumen[1] por actividad económica
Segundo trimestre 2026[pr]

Actividad económica	Serie original		Serie ajustada por efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2026[pr] - II / 2025[pr] - II	2026[pr] / 2025[pr]	2026[pr] – II / 2026[pr]- I
Agricultura, ganadería, caza, silvicultura y pesca	-2,1	-1,7	0,4
Explotación de minas y canteras	4,2	1,6	0,4
Industrias manufactureras	2,0	2,3	-0,4
Suministro de electricidad, gas, vapor y aire acondicionado[2]	4,8	3,7	2,8
Construcción	2,2	-1,5	6,4
Comercio al por mayor y al por menor[3]	2,2	2,6	0,3
Información y comunicaciones	-0,1	0,7	0,3
Actividades financieras y de seguros	4,3	3,6	1,9
Actividades inmobiliarias	2,1	2,1	0,5
Actividades profesionales, científicas y técnicas[4]	2,6	2,5	0,8
Administración pública, defensa, educación y salud[5]	10,0	7,9	2,3
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios[6]	9,5	6,3	4,0
Valor agregado bruto	**3,6**	**2,9**	**1,4**
Impuestos menos subvenciones sobre los productos	2,4	2,7	0,2
Producto Interno Bruto	**3,5**	**2,9**	**1,3**

Fuente: Comunicado de Prensa PIB trimestral segundo trimestre 2026

Información y comunicaciones

En el segundo trimestre de 2026 el valor agregado de información y comunicaciones decrece 0,1% en su serie original, respecto al mismo periodo de 2025. Para la serie ajustada por efecto estacional y calendario, el valor agregado crece en 0,3%, respecto al trimestre inmediatamente anterior.

2.3.4 SALARIO MÍNIMO MENSUAL LEGAL VIGENTE

Teniendo en cuenta que en Colombia el Salario Mínimo Mensual Legal Vigente (SMMLV) es la base para el pago de salarios y honorarios así como los pagos al sistema de seguridad social, es necesario revisar su evolución, pues este incremento además sirve para el reajuste financiero de las finanzas personales de los colombianos, tiene mucho que ver en el incremento de los precios de los productos y servicios tales como salarios, arriendos, avalúos, servicios públicos, entre otros, por tal razón la Entidad da una mirada al incremento que este indicador ha tenido en el tiempo, que sirve para mirar la situación de un aspecto económico particular que influye en el costo para el objeto a contratar.

En la tabla, se observa la evolución del salario mínimo en los últimos 10 años y se contrasta el incremento anual.

AÑO	SALARIO MÍNIMO LEGAL DIARIO	SALARIO MÍNIMO LEGAL MENSUAL	VARIACIÓN % ANUAL
2015	$ 21.478,33	$ 644.350,00	4,6
2016	$ 22.981,83	$ 689.455,00	7
2017	$ 24.590,57	$ 737.717,00	7
2018	$ 26.041,40	$ 781.242,00	5,9
2019	$ 27.603,87	$ 828.116,00	6
2020	$ 29.260,10	$ 877.803,00	6
2021	$ 30.284,20	$ 908.526,00	3,5
2022	$ 33.333,33	$ 1.000.000,00	10,07
2023	$ 38.666,66	$ 1.160.000,00	16
2024	$ 43.333,33	$ 1.300.000,00	12,07
2025	$ 47.450,00	$ 1.423.500,00	9,5
2026	$ 58.363,5	$ 1.750.905,00	23

2.4 VISIÓN ESTRATÉGICA DE LAS TIC

Las Tecnologías de la Información y las Comunicaciones (TIC) constituyen un eje estratégico para el cumplimiento de la misión institucional del Instituto Nacional de Vías – INVÍAS, al facilitar la modernización de los procesos, la transformación digital y la prestación eficiente de los servicios a la ciudadanía. En este contexto, la gestión de las TIC se orienta a fortalecer la infraestructura tecnológica, garantizar la disponibilidad de los servicios institucionales y promover la innovación como elemento fundamental para mejorar la gestión pública.

La estrategia institucional reconoce que la transformación digital requiere una infraestructura tecnológica segura, confiable y resiliente, capaz de soportar el crecimiento de los servicios digitales, la interoperabilidad entre los sistemas de información y la protección de los activos tecnológicos de la Entidad. En este sentido, la seguridad de la información y la ciberseguridad constituyen componentes esenciales para garantizar la confidencialidad, integridad y disponibilidad de la información institucional, así como la continuidad de la operación tecnológica.

La visión institucional a corto y mediano plazo busca posicionar al INVÍAS como una entidad referente en la implementación de buenas prácticas de transformación digital, fortaleciendo la gestión de la información mediante el uso eficiente de las Tecnologías de la Información y las Comunicaciones, la automatización de procesos, la adopción de plataformas tecnológicas seguras y la implementación de soluciones innovadoras que generen valor público.

En concordancia con esta visión estratégica, el presente proceso de contratación para la implementación de una solución integral de ciberseguridad constituye una inversión fundamental para fortalecer las capacidades institucionales de prevención, detección, análisis y respuesta frente a amenazas cibernéticas. La solución contempla la operación de un Centro de Operaciones de Seguridad (SOC), el monitoreo continuo de eventos de seguridad, la gestión de vulnerabilidades, la inteligencia de amenazas, la protección de aplicaciones, la automatización de la respuesta a incidentes y demás servicios especializados que contribuyen a garantizar la continuidad de los servicios tecnológicos institucionales.

Así mismo, la implementación de esta solución permitirá fortalecer la protección de la infraestructura tecnológica del INVÍAS, mejorar la capacidad de respuesta ante incidentes de seguridad informática, reducir los riesgos asociados a ciberataques y contribuir al cumplimiento de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las demás políticas institucionales en materia de seguridad digital y continuidad del negocio.

2.5 ASPECTOS MACROECONÓMICOS

- Comportamiento de la Tasa Representativa del Mercado (TRM)

Uno de los principales factores que incide en el comportamiento económico del sector corresponde a la Tasa Representativa del Mercado (TRM)**,** debido a que una parte importante del licenciamiento, las suscripciones, el soporte especializado y los servicios asociados a plataformas de ciberseguridad son comercializados por fabricantes internacionales en dólares estadounidenses.

En consecuencia, las variaciones de la TRM pueden generar incrementos o disminuciones en los costos de adquisición de licencias, suscripciones, servicios administrados y soporte técnico especializado, razón por la cual esta variable constituye un elemento relevante para la estructuración del presupuesto oficial del presente proceso.

- Inflación y Costos de Prestación del Servicio

La inflación constituye otro factor macroeconómico que incide en el mercado de tecnologías de la información, debido a su impacto sobre los costos de prestación de servicios profesionales especializados, infraestructura tecnológica, logística, contratación de talento humano altamente calificado y servicios asociados a la operación de plataformas tecnológicas.

De igual forma, el crecimiento de la demanda de profesionales especializados en ciberseguridad ha incrementado los costos asociados a la operación de Centros de Operaciones de Seguridad (SOC), servicios de monitoreo continuo y respuesta a incidentes, situación que debe ser considerada dentro del análisis económico del presente proceso.

- Servicios en la Nube y Economía Digital

La creciente adopción de modelos de computación en la nube (Cloud Computing) ha transformado la forma en que las organizaciones implementan soluciones de seguridad informática, permitiendo acceder a plataformas especializadas mediante esquemas de suscripción y servicios administrados.

Este modelo facilita la actualización permanente de las soluciones tecnológicas, el acceso a inteligencia de amenazas, la escalabilidad de los servicios y la reducción de costos asociados a infraestructura física, favoreciendo la implementación de soluciones integrales de ciberseguridad alineadas con las mejores prácticas internacionales.

El comportamiento del sector de Tecnologías de la Información y las Comunicaciones (TIC), y en particular del subsector de ciberseguridad, evidencia un mercado dinámico, competitivo y en constante crecimiento, impulsado por la transformación digital, la adopción de servicios en la nube y el incremento de las amenazas cibernéticas.

Si bien variables macroeconómicas como la inflación y la Tasa Representativa del Mercado (TRM) pueden influir en los costos del licenciamiento, las suscripciones y los servicios especializados, el mercado nacional cuenta con una oferta suficiente de fabricantes, integradores tecnológicos y proveedores de servicios administrados que garantizan condiciones adecuadas de competencia y pluralidad de oferentes para la ejecución del presente proceso contractual.[2]

2.6 ANÁLISIS DEL SECTOR TIC – CIBERSEGURIDAD



El presente proceso contractual se desarrolla dentro del sector de Tecnologías de la Información y las Comunicaciones (TIC)**,** específicamente en el subsector de ciberseguridad, el cual ha presentado un crecimiento constante durante los últimos años como consecuencia del incremento de las

- Ministerio De Tecnologías De La Información Y Las Comunicaciones (Mintic)
- Política De Gobierno Digital - Mintic
- Modelo De Seguridad Y Privacidad De La Información (Mspi)
- Departamento Administrativo Nacional De Estadística (Dane)
- Banco De La República De Colombia
- Comisión De Regulación De Comunicaciones (Crc)
- Procolombia
- Fedesoft - Federación Colombiana De La Industria De Software Y Ti

amenazas informáticas, la acelerada transformación digital y la creciente adopción de servicios tecnológicos en ambientes híbridos y de computación en la nube.

Actualmente, tanto las entidades públicas como las organizaciones privadas demandan soluciones que permitan fortalecer la protección de su infraestructura tecnológica frente a riesgos asociados a ataques cibernéticos, pérdida de información, accesos no autorizados y vulnerabilidades de seguridad. Esta situación ha impulsado el desarrollo de un mercado especializado conformado por empresas que ofrecen servicios administrados de seguridad, monitoreo continuo, respuesta a incidentes, análisis de vulnerabilidades, inteligencia de amenazas y protección de aplicaciones e infraestructura tecnológica.

En Colombia existe una oferta amplia de empresas con capacidad para prestar este tipo de servicios, conformada por fabricantes internacionales, distribuidores autorizados, integradores tecnológicos y proveedores de servicios administrados de seguridad (MSSP). Estas empresas cuentan con personal especializado, certificaciones técnicas y experiencia en la implementación y operación de soluciones de ciberseguridad para entidades públicas y privadas.

La comercialización de estas soluciones se realiza principalmente mediante esquemas de licenciamiento, suscripciones anuales, servicios administrados y plataformas en la nube, lo que ha permitido ampliar la oferta del mercado y facilitar el acceso a tecnologías de seguridad avanzadas sin requerir grandes inversiones en infraestructura propia.

Desde el punto de vista económico, este mercado presenta una alta dependencia de variables como la Tasa Representativa del Mercado (TRM), debido a que gran parte de las soluciones tecnológicas, licencias, suscripciones y servicios especializados son comercializados por fabricantes internacionales en dólares estadounidenses. De igual manera, la inflación y el incremento en la demanda de profesionales especializados en ciberseguridad inciden en los costos de implementación, soporte y operación de este tipo de servicios.

Como resultado del estudio de mercado realizado por la Entidad, se evidenció la participación de diferentes proveedores especializados con capacidad técnica, financiera y operativa para atender el objeto contractual, situación que demuestra la existencia de condiciones de competencia y pluralidad de oferentes para adelantar el presente proceso de contratación.

En consecuencia, se concluye que el mercado nacional de ciberseguridad cuenta con una oferta suficiente de proveedores especializados, condiciones adecuadas de competencia y disponibilidad de soluciones tecnológicas que permiten satisfacer las necesidades del Instituto Nacional de Vías –

INVÍAS, garantizando la ejecución del contrato bajo criterios de eficiencia, calidad y libre concurrencia.

2.7 CONTEXTO EN EL SECTOR DE LA ECONOMÍA

El presente proceso pertenece al sector terciario de la economía, específicamente al sector de Tecnologías de la Información y las Comunicaciones (TIC), subsector de ciberseguridad, por cuanto comprende la prestación de servicios especializados orientados a la protección de la infraestructura del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS mediante soluciones administradas de seguridad, plataformas tecnológicas, licenciamiento y servicios especializados.

2.8 CLASIFICACIÓN DE LAS PYMES EN COLOMBIA

El Gobierno Nacional expidió el Decreto 957 de 2019, mediante el cual se establece una nueva clasificación del tamaño empresarial basada en el criterio único de ingresos por actividades ordinarias.

A la fecha, las empresas en Colombia se han clasificado por medio de las variables "Número de empleados" y "Volumen de activos"; sin embargo, dada la necesidad de contar con una clasificación que responda a las nuevas realidades de las empresas colombianas, el Gobierno Nacional decidió adoptar los ingresos como único criterio, ya que aporta mejor información sobre el tamaño real de las empresas y permite tener presentes las particularidades de cada sector de la economía, como ocurre con las empresas del sector de tecnologías de la información y ciberseguridad.

En concordancia con lo establecido por la normatividad, aquellas firmas que no clasifiquen en alguno de los tres sectores enunciados anteriormente deberán usar los umbrales determinados para el macro sector de manufactura.

De otra parte, en el caso de las empresas que tengan más de una actividad económica, el tamaño será definido por aquella que reporte el mayor volumen de ingresos.

El Decreto 957 de 2019, con el que se adopta la variable de ingresos por actividades ordinarias anuales, fijó rangos para los macrosectores de manufactura, servicios y comercio. Los umbrales establecidos en Unidad de Valor Tributario (UVT) para cada uno de estos macrosectores se presentan en la siguiente tabla:

Clasificación de las micro, pequeñas y medianas empresas

Tamaño	Manufactura	Servicios	Comercio
Micro empresa	Inferiores o iguales a 23.563 UVT	Inferiores o iguales 32.988 UVT	Inferiores o iguales a 44.769 UVT
Pequeña empresa	Superiores a 23.563 UVT, e inferiores o iguales a 204.995 UVT	Superiores a 32.988 UVT inferiores o iguales a 131.951 UVT	Superiores a 44.769 UVT e inferiores o iguales a 431.196 UVT
Mediana empresa	Superiores a 204.995 UVT e inferiores o iguales a 1.736.565 UVT	Superiores a 131.951 UVT) e inferiores o iguales a 483.034 UVT	Superiores a 431.196 UVT e inferiores o iguales a 2'160.692 UVT

Fecha de consulta: Decreto 957 de 2019, Ministerio de Comercio, Industria y Turismo (MinCIT). Clasificación empresarial vigente. Consulta realizada en julio de 2026

LIMITACIÓN DE LA CONVOCATORIA A MIPYMES

De conformidad con lo establecido en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, modificado por el Decreto 1860 de 2021, las Entidades Estatales podrán limitar la convocatoria a Mipymes colombianas en los procesos de licitación pública, selección abreviada y concurso de méritos, cuando el valor estimado del proceso sea inferior al umbral definido anualmente por el Ministerio de Comercio, Industria y Turismo y se cumplan los demás requisitos previstos en la normativa vigente.

Para la vigencia 2026, el umbral establecido para la limitación de convocatorias a Mipymes equivalente a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000), corresponde en moneda legal colombiana a QUINIENTOS ONCE MILLONES SETECIENTOS OCHO MIL CUATROCIENTOS NOVENTA Y SIETE PESOS M/CTE. ($511.708.497) de acuerdo con la información publicada por Colombia Compra Eficiente en el siguiente enlace:

https://www.colombiacompra.gov.co/archivos/manual/valores-a-partir-de-los-cuales-son-aplicables-los-acuerdos-comerciales-umbrales

UMBRAL DE MIPYMES 2026	
US$	125.000
COL$	**511.708.497**

Fuente: Colombia Compra Eficiente

Ahora bien, el presupuesto oficial del presente proceso asciende a la suma de **SEIS MIL TREINTA MILLONES CIENTO SESENTA Y CUATRO MIL NOVECIENTOS VEINTISIETE PESOS M/CTE**. (**$ 6.030.164.927,00)** incluido IVA (en los ítems que apliquen o correspondan) y todos los costos directos e indirectos necesarios. Este valor supera ampliamente el umbral establecido para la vigencia 2026 para la limitación de convocatorias a Mipymes.

En consecuencia, **NO** procede la limitación de la convocatoria a Mipymes, por cuanto el presupuesto oficial del presente proceso supera el umbral establecido en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, modificado por el Decreto 1860 de 2021. En consecuencia, el proceso de selección se adelantará garantizando la libre concurrencia de los interesados que acrediten el cumplimiento de los requisitos habilitantes establecidos en los documentos del proceso, en observancia de los principios de transparencia, selección objetiva, igualdad y libre competencia.

2.8 ANÁLISIS NORMATIVO

En el marco del presente proceso contractual, es pertinente considerar el cumplimiento de la normativa aplicable en materia ambiental, tecnológica y de propiedad intelectual, conforme a las siguientes disposiciones:

Decreto 0287 de 2026 – Personas en condición de discapacidad Contratación pública inclusiva para personas con discapacidad

Sistema de preferencias para las personas con discapacidad en la contratación estatal

Históricamente, las Personas con Discapacidad (en adelante, PcD) han enfrentado mayores tasas de desempleo y barreras de acceso al mercado. Aunque leyes previas (como la Ley 1618 de 2013) ordenaban un sistema de preferencias para las PcD en la contratación estatal, la regulación anterior (Decreto 392 de 2018) se limitaba a medidas aisladas de puntaje que no garantizaban una participación equitativa desde el inicio de los procesos contractuales. Esto fue ratificado por la sentencia del Consejo de Estado, Sección Quinta, del 12 de diciembre de 2024 *(Rad. 05001-23-33-*

000-2024-00847-01, M.P. Omar Joaquín Barreto Suárez), que mediante acción de cumplimiento declaró el incumplimiento del deber de reglamentar integralmente el artículo 13 de la Ley 1618 de 2013 y ordenó al Gobierno Nacional expedir la regulación necesaria para hacer efectivo el sistema de preferencias en favor de las personas con discapacidad**.**

El legislador así lo estableció en el numeral 8 del artículo 13 de la Ley 1618 de 2013, y al Gobierno Nacional le correspondía definir qué es un sistema de preferencias y sus componentes, en todo caso, un sistema no puede ser compuesto de una única medida como el puntaje que señalaba el Decreto 392 de 2018, que fue modificado con este nuevo Decreto 287 de 2026. En ese sentido, este último define que es un conjunto de beneficios obligatorios en todas las fases de la contratación estatal (planeación, selección, adjudicación y ejecución) a favor de personas con discapacidad, sus emprendimientos y empresas que las contratan.

La entrada en vigencia del Decreto 0287 fue el 19 de marzo de 2026.

Antes (Decreto 392 de 2018)	Ahora (Decreto 287 de 2026)
1% de puntaje solo para empleadores de PcD	2% de puntaje para empleadores y empresas de PcD
Exigencia básica de número mínimo de trabajadores	Se duplica el mínimo y se ajusta a la reforma laboral
En consorcios y UT contaba quien aportara el 40% de la experiencia	En consorcios y UT cuenta quien tenga mayor participación
Preferencias solo en caso de empate	Preferencias con varias medidas en todo el proceso

Beneficios solo para empleadores de PcD	Beneficios directos también para empresas de PcD
No era obligatorio contratar con accesibilidad	La accesibilidad ahora es obligatoria
Sin medidas en planeación ni ejecución	Se incluyen medidas desde planeación hasta ejecución
Sin medidas en contratación directa	Se incluyen PcD en contratos de prestación de servicios de forma potestativa
No había seguimiento	Se establecen mecanismos de seguimiento
No se usaban herramientas de Colombia Compra Eficiente	Se prevé su implementación en SECOP, pliegos tipo y acuerdos marco, previa adecuación por parte de Colombia Compra Eficiente

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS



Así las cosas el artículo 2.2.1.2.4.2.7.5. denominado INCORPORACIÓN DE CONDICIONES ESPECIALES DE EJECUCIÓN EN FAVOR DE LAS PERSONAS CON DISCAPACIDAD.es típula que:

"(…) ARTÍCULO 2.2.1.2.4.2.7.5. INCORPORACIÓN DE CONDICIONES ESPECIALES DE EJECUCIÓN EN FAVOR DE LAS PERSONAS CON DISCAPACIDAD. En desarrollo del Sistema de

Preferencias definido en el artículo 2.2.1.2.4.2.7. del presente Decreto y en virtud del inciso cuarto del artículo 12 de la Ley 1150 de 2007, las Entidades Estatales deberán incluir como obligación contractual, en los Documentos del Proceso, previo análisis de conveniencia y oportunidad, al menos una (1) de las siguientes condiciones especiales de ejecución:

1) Subcontratación inclusiva: Cuando para la ejecución del contrato se requiera subcontratar bienes, obras, o servicios dentro de la cadena de provisión, se deberá punzonar la contratación de personas naturales con discapacidad y los emprendimientos y empresas de personas con discapacidad, conforme a los criterios definidos en el artículo 2.2.1.2.4.2.6. del presente Decreto.

2) integración del equipo de trabajo. Cuando para la ejecución del contrato se requiera la conformación de un equipo de trabajo, se deberá priorizar la contratación de personas naturales con discapacidad.

En caso de que no se incluya alguna de estas condiciones especiales de ejecución, la Entidad Estatal deberá justificar dicha omisión en las estudios previos o documentos equivalentes" (…)

En cumplimiento de lo dispuesto en el artículo 2.2.1.2.4.2.7.5 del Decreto 1082 de 2015, adicionado por el artículo 1 del Decreto 0287 de 2026, el INVIAS analizó la conveniencia y oportunidad de incorporar una condición especial de ejecución en favor de las personas con discapacidad, de acuerdo con el objeto y la forma de ejecución del contrato.
El alcance contractual comprende la implementación y operación de un Centro de Operaciones de Seguridad (SOC), así como la prestación continua de servicios de monitoreo, detección, correlación y respuesta a incidentes. Para su ejecución se requiere la participación de analistas del SOC, ingenieros de implementación y perfiles especializados asociados a la bolsa de horas, por lo cual se conformará un equipo de trabajo.
En consecuencia, el INVIAS considera procedente incorporar la condición especial de integración del equipo de trabajo, mediante la priorización de la contratación de personas naturales con discapacidad que acrediten los requisitos técnicos, de experiencia y demás condiciones establecidas para los roles requeridos. El hecho de que el servicio se preste principalmente de forma remota no impide aplicar esta medida, pues la norma no exige que el equipo desarrolle sus labores en las instalaciones de la Entidad.

La priorización se aplicará entre las personas que cumplan los requisitos del respectivo perfil y no implica una cuota ni exime al contratista de garantizar la idoneidad del equipo y la correcta prestación del servicio. De esta manera, la medida promueve la inclusión laboral y resulta compatible con las necesidades técnicas y operativas del contrato.

Adicional a lo anterior, en cumplimiento del artículo 2.2.1.2.4.2.7.3. del Decreto 287 de 2026 el cual establece que:

" (…)
Artículo 2.2.1.2.4.2.7.3. Incorporación de criterios habilitantes diferenciales en favor de los emprendimientos y empresas de personas con discapacidad. *En los procesos de licitación pública, selección abreviada y concurso de méritos, así como en los procesos competitivos adelantados por entidades no sometidas al Estatuto General de Contratación de la Administración Pública, deberán establecer requisitos* ***habilitantes diferenciales o ajustados en materia de experiencia, capacidad financiera u organizacional, o el valor de la garantía de seriedad de la oferta,*** *con el fin de promover la participación de emprendimientos y empresas de personas con discapacidad con domicilio en el territorio nacional.*

Estos requisitos deberán estructurarse garantizando el cumplimiento adecuado del objeto contractual, teniendo en cuenta el alcance de las obligaciones y el principio de proporcionalidad. En desarrollo de lo anterior, se deberán establecer condiciones habilitantes diferenciadas o ajustadas que, sin comprometer los fines del contrato, faciliten el acceso de los emprendimientos y empresas de personas con discapacidad.

Parágrafo 1°. *Tratándose de proponentes plurales, estas condiciones solo se aplicarán cuando al menos uno de los integrantes cumpla con los criterios previstos en el artículo 2.2.1.2.4.2.6. de este Decreto y acredite una participación no inferior al diez por ciento (10%) en el consorcio o la unión temporal, aportando la experiencia requerida, como mínimo, en una proporción equivalente a su participación en la conformación del proponente plural.*

Parágrafo 2°. *Las medidas de fomento previstas en el presente artículo serán compatibles con otros criterios diferenciales o de preferencia establecidos en el ordenamiento jurídico, tales como las aplicables a MiPymes o a las empresas y emprendimientos de mujeres." (…)* ***Negrilla y subrayado fuera del texto***

Dicho esto, y de acuerdo con el análisis de la muestra para determinar los indicadores de capacidad financiera y organizacional anteriormente expuesta, este Comité se permite establecer los indicadores de **CAPACIDAD FINANCIERA PARA DISCAPACIDAD EN EL SISTEMAS DE COMPRAS PUBLICAS.**

ASPECTOS REGULATORIOS

El presente proceso contractual se desarrollará de conformidad con el régimen de contratación estatal vigente y con la normatividad que regula el sector de las Tecnologías de la Información y las Comunicaciones (TIC), atendiendo la naturaleza del objeto contractual, el cual comprende la implementación de una solución integral de ciberseguridad para fortalecer la protección de la infraestructura del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS, la gestión de eventos e incidentes de seguridad y la continuidad de los servicios tecnológicos.

- Constitución Política de Colombia.
- Ley 80 de 1993, Estatuto General de Contratación de la Administración Pública.
- Ley 1150 de 2007.
- Ley 1474 de 2011 (Estatuto Anticorrupción).
- Ley 1882 de 2018.
- Decreto 1082 de 2015.
- Decreto 1860 de 2021 y demás normas que lo modifiquen, adicionen o sustituyan.

Normatividad aplicable al sector TIC

Por tratarse de un proceso relacionado con la prestación de servicios especializados de ciberseguridad, serán aplicables las siguientes disposiciones:

- Ley 1341 de 2009, modificada por la Ley 1978 de 2019.
- Decreto 1078 de 2015.
- Decreto 620 de 2020.
- Política de Gobierno Digital.
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Ley 1581 de 2012 (Protección de Datos Personales).
- Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública).
- Ley 527 de 1999 (Mensajes de datos y comercio electrónico).
- Ley 1273 de 2009 (Delitos Informáticos).

Propiedad intelectual

En materia de licenciamiento de software y plataformas tecnológicas serán aplicables las siguientes disposiciones:

- Ley 23 de 1982.

- Ley 44 de 1993.
- Decisión Andina 351 de 1993.
- Ley 1915 de 2018.

TENDENCIAS TECNOLÓGICAS

El mercado de la ciberseguridad evoluciona permanentemente como respuesta al incremento de las amenazas informáticas y al crecimiento de los servicios digitales. Actualmente, las organizaciones orientan sus inversiones hacia soluciones que permitan fortalecer la capacidad de prevención, detección, análisis y respuesta frente a incidentes de seguridad mediante tecnologías como:

- Computación en la nube (Cloud Computing).
- Centros de Operaciones de Seguridad (SOC).
- Gestión de Eventos e Información de Seguridad (SIEM).
- Automatización y Orquestación de Respuesta (SOAR).
- Detección y Respuesta en Endpoints (EDR/XDR).
- Inteligencia de Amenazas (Threat Intelligence).
- Gestión de Vulnerabilidades.
- Protección de aplicaciones web (WAF).
- Mitigación de ataques DDoS.
- Arquitecturas Zero Trust.
- Inteligencia Artificial aplicada a la ciberseguridad.

Estas tendencias han impulsado el crecimiento del mercado de servicios administrados de seguridad, permitiendo a las entidades públicas fortalecer la protección de su infraestructura tecnológica mediante plataformas especializadas, monitoreo continuo y personal altamente calificado.

3.0 ANÁLISIS DE LA DEMANDA.

HISTÓRICO DE LA ENTIDAD:

El histórico de contratación del Instituto Nacional de Vías – INVÍAS evidencia que la Entidad ha adelantado procesos orientados al fortalecimiento de su infraestructura tecnológica y de sus capacidades de ciberseguridad, mediante la adquisición, renovación e implementación de soluciones especializadas para la protección de la información, la seguridad de los servicios tecnológicos y la continuidad de la operación institucional.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

En este contexto, se identifica el siguiente proceso contractual relacionado con el objeto del presente estudio:

NOMBRE ENTIDAD	REFERENCIA DEL CONTRATO	DESCRIPCIÓN DEL PROCESO	MODALIDAD DE CONTRATACIÓN	PROVEEDOR ADJUDICADO	VALOR DEL CONTRATO
INVIAS	1353-2025	RENOVACIÓN E IMPLEMENTACIÓN DE NUEVAS FUNCIONALIDADES EN CIBERSEGURIDAD Y ADQUISICIÓN DE COMPONENTES TECNOLÓGICOS PARA LA IMPLEMENTACIÓN DE SERVICIOS DE CONECTIVIDAD SD-WAN PARA EL INSTITUTO NACIONAL DE VÍAS	Selección abreviada subasta inversa	Grupo Microsistemas Colombia SAS	$1.776.622.043,

Fuente: elaboración propia. OTIC – INVIAS

El análisis del histórico de contratación evidencia que el Instituto Nacional de Vías – INVÍAS ha adelantado procesos orientados al fortalecimiento de su infraestructura tecnológica y de ciberseguridad. En este sentido, el contrato No. 1353-2025 constituye un antecedente del presente proceso, al estar relacionado con la implementación de soluciones de ciberseguridad y conectividad. El presente proceso da continuidad a dicha estrategia institucional, fortaleciendo las capacidades de prevención, detección y respuesta frente a amenazas cibernéticas.

- **HISTÓRICO DE OTRAS ENTIDADES SECOP II:**

Para establecer los contratos celebrados por otras entidades, se realizó la búsqueda de procesos similares en el SECOP II, encontrando los contratos descritos a continuación:

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

NOMBRE ENTIDAD	REFERENCIA DEL CONTRATO	DESCRIPCIÓN DEL PROCESO	MODALIDAD DE CONTRATACIÓN	FECHA DE FIRMA	PROVEEDOR ADJUDICADO	VALOR DEL CONTRATO
Superintendencia Nacional De Salud	387 De 2025	Adquirir Y Renovar El Licenciamiento; Soporte Y Servicios De La Plataforma De Ciberseguridad Trend Micro Vision One Para Fortalecer La Protección Y Respuesta Ante Amenazas Que Afecten Los Activos De Información De La Superintendencia Nacional De Salud	Selección Abreviada Subasta Inversa	12/17/2025	Union Temporal High Technology 2025	$4.206.645.154,
Dirección De Investigación Criminal E Interpol	03-2-10063-24	Adquisición ; Instalación E Integración De Sistemas De Cctv Para La Dirección	Selección Abreviada Subasta Inversa	08/27/2024	Security Video Equipment S.A.S.	$3.179.917.678,

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

NOMBRE ENTIDAD	REFERENCIA DEL CONTRATO	DESCRIPCIÓN DEL PROCESO	MODALIDAD DE CONTRATACIÓN	FECHA DE FIRMA	PROVEEDOR ADJUDICADO	VALOR DEL CONTRATO
		De Investigación Criminal E Interpol; Centro De Capacidades Para La Ciberseguridad De Colombia (C4) Y Para Las Instalaciones De La Sala De Capturados				
Unidad De Búsqueda De Personas Desaparecidas	667-2025-Ubpd	Contratar Por Suscripción Los Servicios Especializados De Análisis Y Monitoreo Para La Gestión De Eventos De Ciberseguridad Con El Fin De Fortalecer La Infraestructura Tecnológica De La Unidad.	Selección Abreviada Subasta Inversa	10/16/2025	Heimcore Sas	$2.755.905.000,

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

NOMBRE ENTIDAD	REFERENCIA DEL CONTRATO	DESCRIPCIÓN DEL PROCESO	MODALIDAD DE CONTRATACIÓN	FECHA DE FIRMA	PROVEEDOR ADJUDICADO	VALOR DEL CONTRATO
Dilof	06-2-10326-25	Adquisición De Una Solución Integral De Ciberseguridad Para Campañas Antiphishing Y Monitoreo Continuo De La Infraestructura Tecnológica De La Policía Nacional	Selección Abreviada Subasta Inversa	11/11/2025	Global Open Technologies Sas	$2.298.151.125,
Inm	106 De 2024	Contratar El Monitoreo; Fortalecimiento Y Mejoramiento De La Ciberseguridad De La Red De Datos Del Inm Asi Como La Extensión De Garantía De Los Dispositivos De Seguridad Con Los Que	Selección Abreviada Subasta Inversa	04/30/2024	Gamma Ingenieros Sas	$1.060.184.149,

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

NOMBRE ENTIDAD	REFERENCIA DEL CONTRATO	DESCRIPCIÓN DEL PROCESO	MODALIDAD DE CONTRATACIÓN	FECHA DE FIRMA	PROVEEDOR ADJUDICADO	VALOR DEL CONTRATO
		Actualmente Cuenta La Entidad				
Congreso De La República - Honorable Senado De La República	1460-2024	Adquisicion De Licencias Para El Sistema De Ciberseguridad De La Entidad; Que Garantice La Proteccion De Las Estaciones De Trabajo; Servidores On-Premise Y Cloud; Al Igual Que Sus Diferentes Aplicativos Misionales.	Selección Abreviada Subasta Inversa	12/24/2024	Wexler S.A.S	$13.170.511.100,

Fuente: elaboración propia. OTIC – INVIAS

El análisis de los procesos contractuales adelantados por otras entidades públicas evidencia una creciente demanda de soluciones integrales de ciberseguridad orientadas a fortalecer la protección de la infraestructura tecnológica y de los activos de información. De igual forma, se observa la participación de diversos proveedores especializados en la implementación, operación y soporte de este tipo de soluciones, lo que demuestra la existencia de un mercado consolidado, una oferta suficiente y condiciones de competencia que garantizan la pluralidad de oferentes para el presente proceso de contratación.

3.1 COMPORTAMIENTO DEL GASTO HISTÓRICO ESTUDIO DE LA DEMANDA Y OFERTA

¿Cómo adquieren las Entidades Estatales y las empresas privadas este bien, obra o servicio?

Con el fin de conocer el gasto público a nivel nacional de los servicios requeridos, la Entidad procedió a consultar mediante el Modelo de Abastecimiento Estratégico desarrollado por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, busca mejorar las buenas prácticas en la planeación y gestión de los procesos contractuales para que los participantes del Sistema de Compra Pública lo adopten y se destaquen por sus niveles de transparencia, eficiencia y generación de mayor valor por dinero.



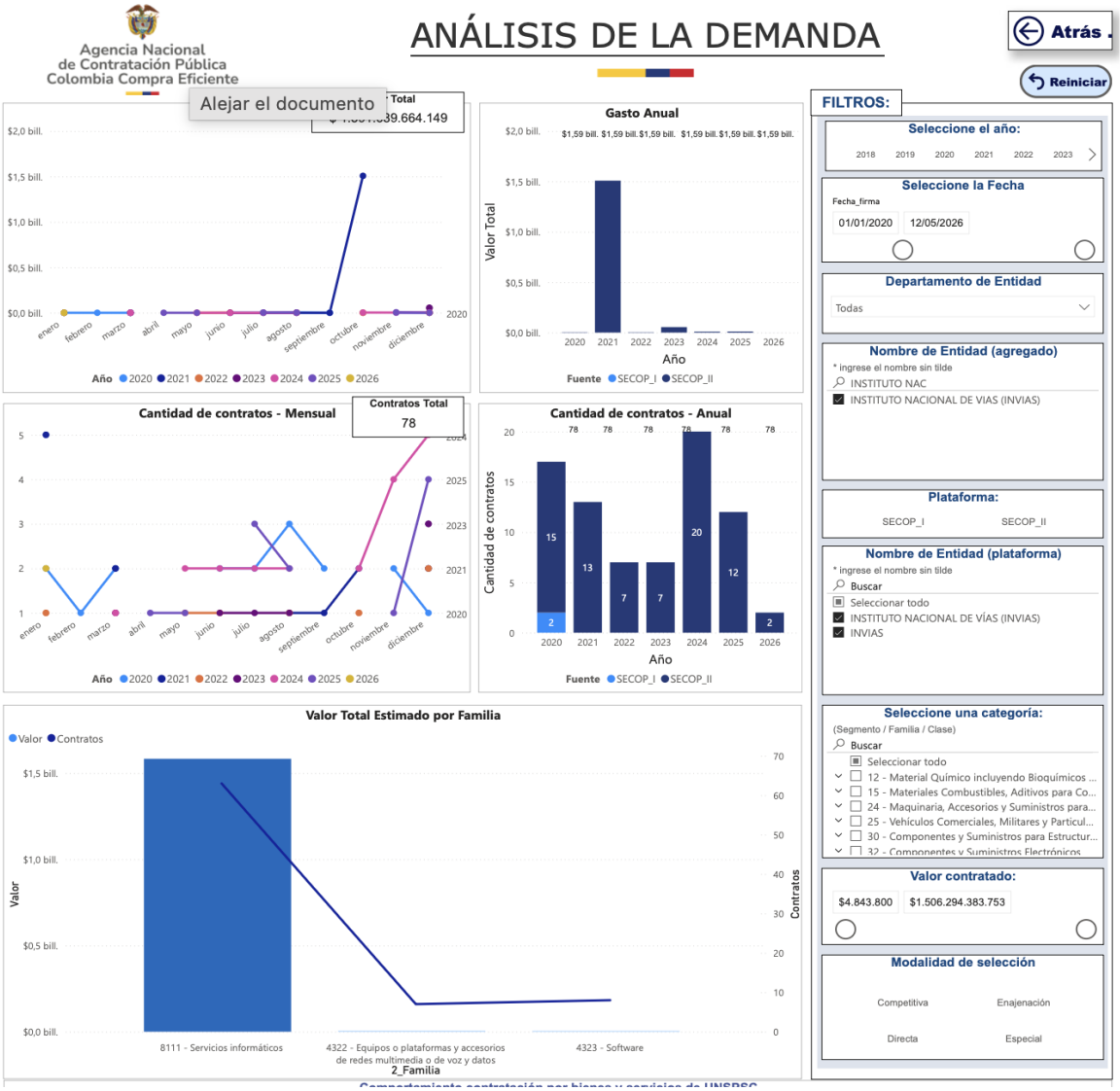
Análisis de la Demanda – Abastecimiento Estratégico CCE

Para el Instituto Nacional de Vías – INVÍAS es fundamental identificar la disponibilidad de los bienes y servicios requeridos en el mercado, así como conocer las condiciones técnicas, económicas y comerciales bajo las cuales estos son ofertados, con el fin de estructurar un proceso contractual acorde con las necesidades institucionales y con las condiciones reales del mercado.

Para ello, la Entidad consultó la herramienta de Abastecimiento Estratégico – Análisis de la Demanda de Colombia Compra Eficiente, la cual permite analizar el comportamiento histórico de la contratación pública, identificar la disponibilidad de proveedores, establecer precios de referencia, conocer las modalidades de contratación utilizadas y verificar las condiciones de adquisición de los bienes y servicios requeridos para el presente proceso contractual.

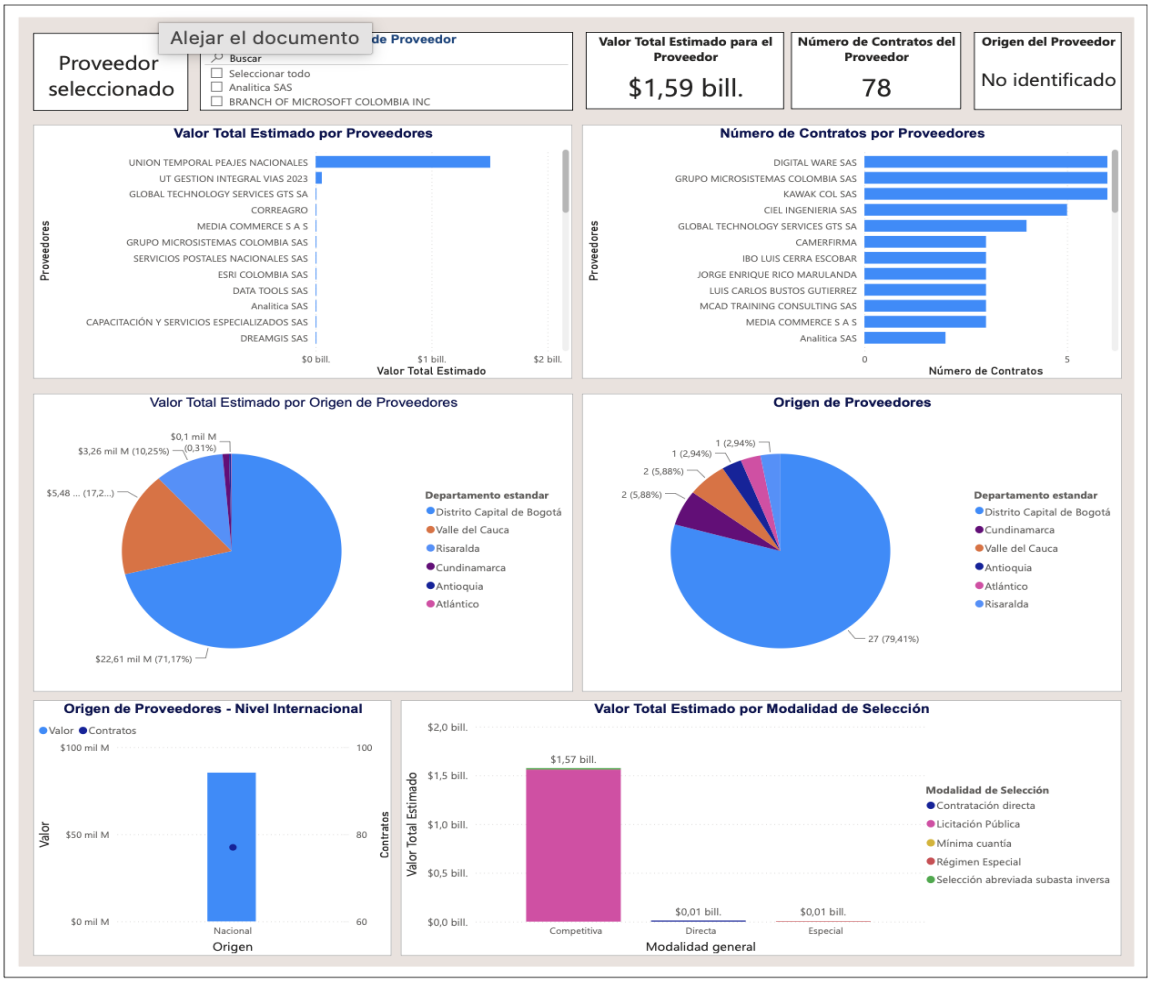
De acuerdo con la información consultada, el análisis se realizó sobre los segmentos y familias del Clasificador UNSPSC relacionados con el objeto del proceso, principalmente la familia 8111 – Servicios informáticos, seguida de las familias 4322 – Equipos o plataformas y accesorios de redes multimedia o de voz y datos y 4323 – Software, las cuales concentran la mayor contratación asociada a soluciones tecnológicas y servicios especializados de tecnologías de la información.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS



Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS



Con el fin de analizar el comportamiento de la demanda del sector, la Entidad consultó la herramienta Análisis de la Demanda de Colombia Compra Eficiente, con información proveniente de las plataformas SECOP I y SECOP II para el período comprendido entre los años 2020 y 2026.

Del análisis realizado se evidencia que el Instituto Nacional de Vías – INVÍAS ha celebrado setenta y ocho (78) contratos, con un valor total estimado de $1.591.689.664.149, lo que refleja una demanda constante de bienes y servicios asociados a las Tecnologías de la Información y las Comunicaciones (TIC).

Así mismo, se observa que la mayor participación de la contratación se concentra en la familia UNSPSC 8111 – Servicios informáticos**,** seguida por las familias 4322 – Equipos o plataformas y accesorios de redes multimedia o de voz y datos y 4323 – Software, evidenciando que la Entidad orienta sus inversiones principalmente hacia la adquisición de servicios tecnológicos, licenciamiento de software e infraestructura tecnológica especializada.

En cuanto a las modalidades de selección, la información muestra que la contratación se ha adelantado principalmente mediante procesos competitivos**,** destacándose la Selección Abreviada por Subasta Inversa**,** la Licitación Pública y la Contratación Directa**,** de acuerdo con las características y necesidades de cada proceso contractual.

Respecto de la oferta del mercado, se evidencia la participación de un número importante de proveedores especializados, entre los cuales se encuentran empresas con amplia trayectoria en el sector TIC, tales como Grupo Microsistemas Colombia S.A.S., Global Technology Services GTS S.A., Media Commerce S.A.S., ESRI Colombia S.A.S., Analítica S.A.S., entre otras. De igual forma, la mayor concentración de proveedores corresponde al Distrito Capital de Bogotá, seguido por empresas ubicadas en los departamentos de Cundinamarca, Valle del Cauca, Antioquia, Atlántico y Risaralda, lo que demuestra la existencia de un mercado nacional con capacidad técnica y operativa para atender este tipo de procesos.

En consecuencia, el análisis de la demanda evidencia que existe un mercado consolidado para la contratación de bienes y servicios de Tecnologías de la Información y las Comunicaciones, con una participación significativa de proveedores especializados y una demanda permanente por parte de la Entidad. Lo anterior permite concluir que el presente proceso de contratación se desarrolla en un mercado competitivo, con pluralidad de oferentes y condiciones adecuadas para garantizar la libre concurrencia y la selección objetiva.

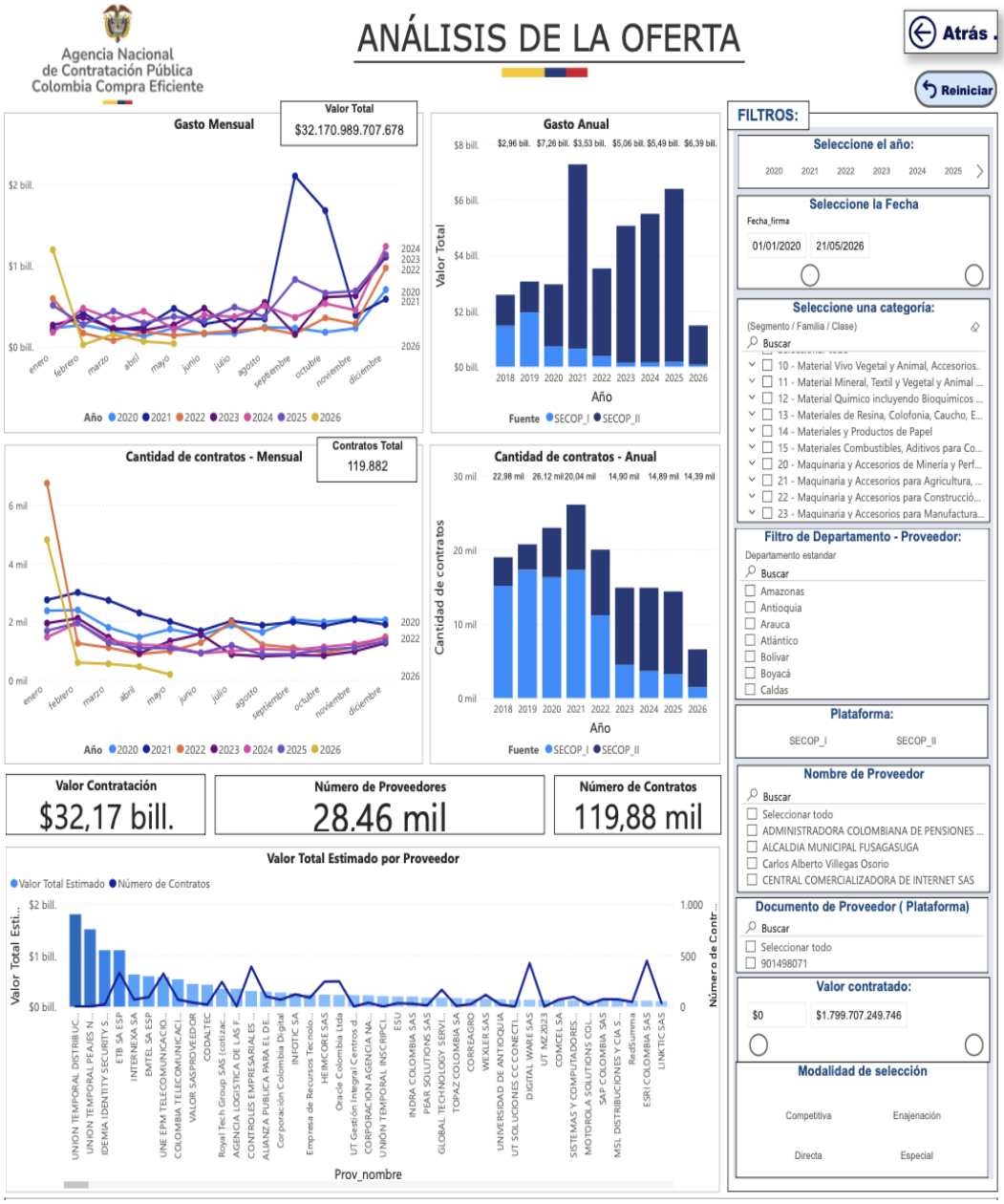
Análisis De La Oferta – Abastecimiento Estratégico CCE

En aplicación de lo establecido en la Guía para la Elaboración de Estudios del Sector – Versión 2 del 15 de agosto de 2025, expedida por Colombia Compra Eficiente, la Entidad realizó la consulta de la herramienta Modelo de Abastecimiento Estratégico – Análisis de la Oferta**,** disponible en la página oficial de Colombia Compra Eficiente, con el fin de identificar el comportamiento del mercado, la disponibilidad de proveedores y las condiciones de oferta para los bienes y servicios relacionados con el objeto del presente proceso contractual.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

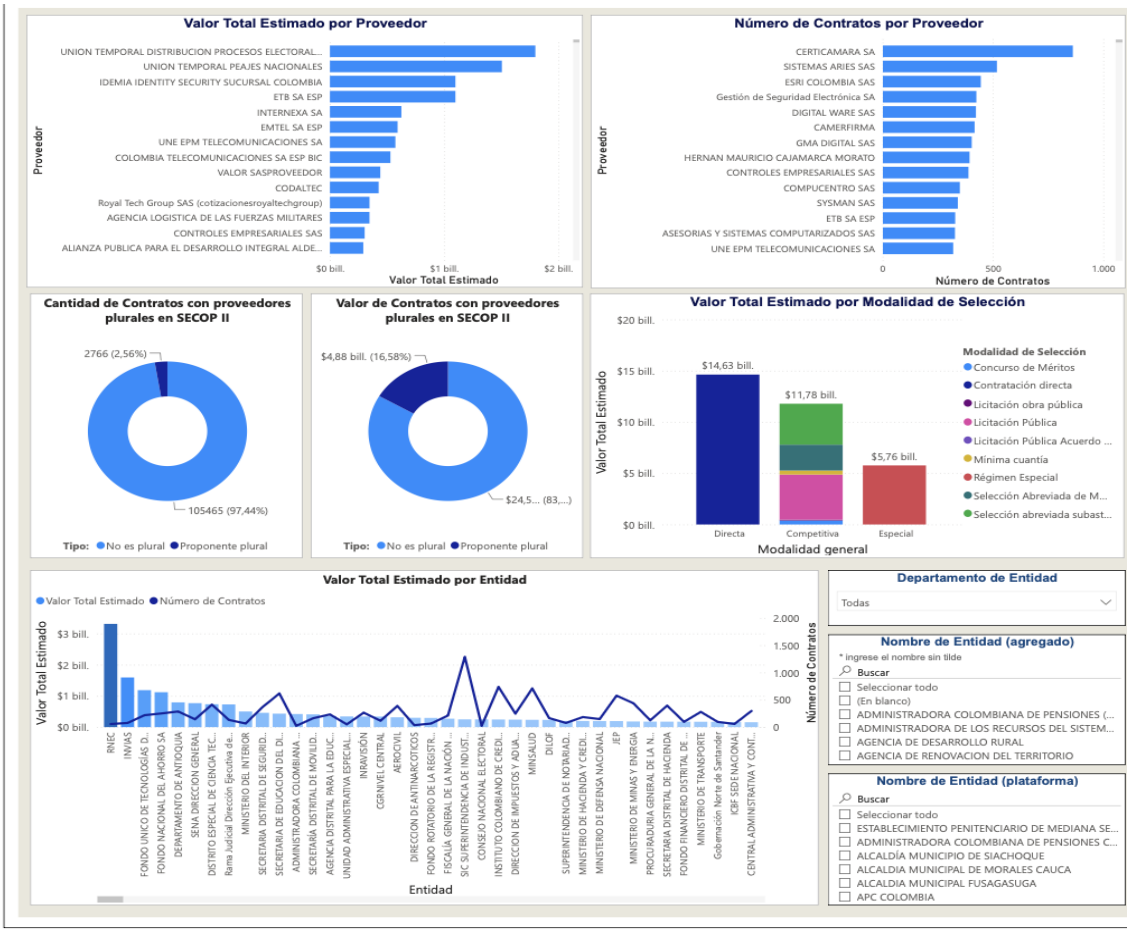
La consulta se efectuó sobre las familias del Clasificador UNSPSC relacionadas con el sector de Tecnologías de la Información y las Comunicaciones (TIC), principalmente la 8111 – Servicios informáticos, seguida de las familias 4322 – Equipos o plataformas y accesorios de redes multimedia o de voz y datos y 4323 – Software, por corresponder a las categorías que agrupan los bienes y servicios requeridos para la implementación de la solución integral de ciberseguridad.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS



Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS



De acuerdo con la información consultada, el mercado presenta un comportamiento dinámico y competitivo, registrando 119.882 contratos**,** un valor total contratado de $32,17 billones y la participación de 28.460 proveedores, lo que evidencia una amplia oferta de empresas con capacidad para suministrar bienes y prestar servicios relacionados con tecnologías de la información, software y ciberseguridad.

Así mismo, el análisis evidencia que la mayor parte de la contratación se realiza mediante modalidades competitivas, las cuales representan aproximadamente $14,63 billones del valor contratado, seguidas por la contratación directa y los regímenes especiales. Este comportamiento

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

demuestra que el mercado cuenta con condiciones adecuadas de competencia y participación de múltiples oferentes.

Entre los proveedores con mayor participación en este mercado se identifican empresas ampliamente reconocidas en el sector TIC, tales como ETB S.A. E.S.P., INTERNEXA S.A., UNE EPM Telecomunicaciones S.A., Colombia Telecomunicaciones S.A. E.S.P. BIC, ESRI Colombia S.A.S., Digital Ware S.A.S., LinkTIC S.A.S., Oracle Colombia Ltda., Heimcore S.A.S., Wexler S.A.S. y Global Technology Services, entre otras, lo que evidencia la existencia de un ecosistema consolidado de proveedores especializados para atender este tipo de procesos.

Adicionalmente, la herramienta evidencia que el 97,44 % de los contratos han sido adjudicados a proponentes individuales, mientras que el 2,56 % corresponde a proponentes plurales, lo que demuestra que el mercado cuenta con un número importante de empresas con capacidad técnica, financiera y operativa para participar de manera independiente en procesos de contratación relacionados con tecnologías de la información y ciberseguridad.

En consecuencia, el análisis de la oferta permite concluir que el mercado nacional presenta una oferta amplia, especializada y suficiente, con pluralidad de proveedores, condiciones adecuadas de competencia y experiencia en la ejecución de contratos similares, garantizando la existencia de oferentes con capacidad para atender las necesidades del Instituto Nacional de Vías – INVÍAS en el marco del presente proceso contractual.

3.2 EL CONTRATO POR INVIAS

Una vez identificados los contratos celebrados en la Entidad y en otras Entidades y con objetos similares al del Instituto, se procedió al análisis que se describe a continuación:

ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS	
CRITERIO	**ANÁLISIS**
Modalidad	El proceso de selección a adelantar según el contrato a celebrar, a las prestaciones y a la cuantía estimada del contrato o contratos surgidos del proceso, según el Estatuto General de la Contratación de la Administración Pública, es el de SELECCIÓN ABREVIADA POR SUBASTA INVERSA por ser de características técnicas uniformes.

ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS	
CRITERIO	**ANÁLISIS**
Aplicabilidad de Acuerdo Marco de Precios, Colombia Compra Eficiente, Tienda Virtual	Se verificó la información publicada en el portal oficial de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente y en el catálogo público de la Tienda Virtual del Estado Colombiano, sin identificar, un Acuerdo Marco de Precios de ciberseguridad vigente y disponible para la adquisición de los bienes y servicios objeto del proceso. Como antecedente, el proceso CCENEG-094-1-2026, orientado a seleccionar proveedores de bienes y servicios de ciberseguridad, fue suspendido mediante la Resolución 463 del 24 de julio de 2026. Posteriormente, según información oficial de la Procuraduría General de la Nación, Colombia Compra Eficiente revocó su apertura mediante la Resolución 566 del 22 de septiembre de 2026, dejando sin efectos el procedimiento. Por lo anterior, a la fecha, NO EXISTE un Acuerdo Marco de precios que satisfaga la necesidad de la entidad.

ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS	
CRITERIO	**ANÁLISIS**
Objeto	De conformidad con la necesidad de la entidad, el objeto del presente contrato será la de CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE

<table>
<tr><th colspan="2">ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS</th></tr>
<tr><th>CRITERIO</th><th>ANÁLISIS</th></tr>
<tr><td></td><td>UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS</td></tr>
<tr><td>Valor del contrato y forma de pago</td><td>Se estima un valor de SEIS MIL TREINTA MILLONES CIENTO SESENTA Y CUATRO MIL NOVECIENTOS VEINTISIETE PESOS M/CTE. ($ 6.030.164.927,00) incluido IVA (en los ítems que apliquen o correspondan) y todos los impuestos, tasas, contribuciones, gravámenes, costos directos e indirectos y demás erogaciones a que haya lugar, como resultado del promedio de las cotizaciones recibidas.

El INVIAS realizará 3 pagos del presente contrato de la siguiente manera:

Pago 1 — Suscripciones de soluciones de seguridad: Corresponde al valor de las suscripciones anuales de los ítems 2 (SIEM), 3 (EDR/XDR), 4 (SOAR/IRP), 5 (Threat Intelligence), 6 (Gestión de Vulnerabilidades) y 8 (WAF Imperva), que se pagará en un desembolso, dentro de los sesenta (60) días siguientes a la radicación de la factura electrónica:

Condiciones de verificación del primer desembolso por cada suscripción:

<table>
<tr><th>Suscripción</th><th>Condición de verificación</th></tr>
<tr><td>SIEM</td><td>Activación de la suscripción con evidencia de registro ante el fabricante.</td></tr>
<tr><td>EDR/XDR</td><td>Activación de la suscripción con evidencia de registro ante el fabricante.</td></tr>
<tr><td>SOAR/IRP</td><td>Activación de la suscripción con evidencia de registro ante el fabricante.</td></tr>
<tr><td>Threat Intelligence</td><td>Activación de la suscripción con evidencia de registro ante el fabricante.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th colspan="2">ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS</th></tr>
<tr><th>CRITERIO</th><th>ANÁLISIS</th></tr>
<tr><td></td><td>
<table>
<tr><td>Gestión de Vulnerabilidades</td><td>Activación de la suscripción con evidencia de registro ante el fabricante.</td></tr>
<tr><td>WAF Imperva</td><td>Activación de la renovación y ampliación de la suscripción con certificado oficial de Imperva.</td></tr>
</table>

En todos los casos, el desembolso estará condicionado a la suscripción del acta de recibo a satisfacción por parte del supervisor del contrato, que certifique la verificación de cada suscripción activa.

Pago 2 — Appliances físicos y sus licencias: Corresponde al valor de los appliances físicos y las licencias de software asociadas con los ítems 7 (AntiDDoS) y 9 (NAC). Se realizará dentro de los sesenta (60) días siguientes a la radicación de la factura electrónica, previa verificación y acreditación simultánea de las siguientes condiciones:

1. Entrega física de los appliances en las instalaciones del INVIAS en Bogotá D.C., en condiciones nuevas y en caja sellada de fábrica.
2. Instalación y puesta en operación de los appliances a entera satisfacción del supervisor del contrato.
3. Activación de las licencias de software asociadas con evidencia de registro ante el fabricante.
4. Incorporación de los bienes al inventario institucional del INVIAS con soporte de entrada al almacén suscrito por el almacenista de la entidad.
5. Suscripción del acta de recibo a satisfacción de los bienes y sus licencias por parte del supervisor del contrato.

Pago 3 — Implementación, Monitoreo SOC y Bolsa de horas especializadas: Corresponde al valor de los ítems 10 (Implementación y despliegue), 1 (Monitoreo SOC) y 11 (Bolsa de horas especializadas prepagadas). Se realizará dentro de los sesenta (60) días siguientes a la radicación de la factura electrónica, previa verificación y acreditación simultánea de las siguientes condiciones:
</td></tr>
</table>

ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS	
CRITERIO	**ANÁLISIS**
	1. Puesta en operación completa del SOC con la totalidad de las plataformas contratadas funcionando de forma integrada y verificada. 2. Suscripción del acta de inicio operativo del SOC por ambas partes, que certifique el cumplimiento simultáneo de los diez (10) criterios de arranque operativo definidos en la ficha técnica. Confirmación escrita de la disponibilidad inmediata de los perfiles especializados de la bolsa de horas, con datos de contacto 24×7 aceptada por el supervisor del contrato.
Presupuesto (inversión o funcionamiento) y vigencias futuras	Los recursos que la Entidad ha dispuesto para la presente contratación provienen de recursos de inversión asociados al proyecto Desarrollo e Implementación de un Sistema Inteligente de Transporte para la Red Vial. Nacional con código BPIN 2021011000249 Rubro: C-2409-0600-9-20301C-2409010-02 Fuente: Propios - 20 Ingresos Corrientes '2. SEGURIDAD HUMANA Y JUSTICIA SOCIAL / C. FORTALECIMIENTO DE LA SEGURIDAD VIAL PARA LA PROTECCIÓN DE LA VIDA. VALOR: **($ 6.030.164.927,00)** La necesidad que se pretende satisfacer con el objeto contractual se encuentra enmarcada dentro de la actividad *Implementar las herramientas tecnológicas para la completa explotación y reporte de la información* la cual hace parte del producto 2409010 - SERVICIO DE INFORMACIÓN DE SEGURIDAD VIAL de la ficha del proyecto de inversión.

ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS	
CRITERIO	**ANÁLISIS**
Garantías	Históricamente en los últimos años se han identificado las siguientes garantías: – SERIEDAD DE LA OFERTA. Por una cuantía equivalente al diez por ciento (10%) del presupuesto del proceso. – CUMPLIMIENTO GENERAL DEL CONTRATO: Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato, con vigencia hasta la liquidación del contrato. – CALIDAD DEL SERVICIO: Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato, con vigencia posterior a la ejecución del contrato y hasta seis (6) meses después, garantizando la correcta prestación y funcionamiento del servicio entregado. – CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES: Por una cuantía equivalente al veinte por ciento (20%) del valor del contrato, con vigencia igual al tiempo de ejecución del contrato y tres (3) años más. – EL PAGO DE SALARIOS, PRESTACIONES SOCIALES E INDEMNIZACIONES LABORALES: Por el equivalente al cinco por ciento (5%) del valor total del contrato y una vigencia igual al plazo del contrato y tres (3) años más. – GARANTÍA DE RESPONSABILIDAD EXTRACONTRACTUAL: Por una cuantía equivalente a 200 SMMLV con una vigencia igual a la del plazo del contrato
Índices Financieros	– INDICE DE LIQUIDEZ: Mayor o Igual a 1,58 vez – INDICE DE ENDEUDAMIENTO: Menor o igual a 60% – RAZON DE CORBERTURA DE INTERESES: Mayor o Igual a 2,48 – CAPITAL DE TRABAJO: Mayor o Igual al 70% del presupuesto oficial

ANÁLISIS DE LAS CONDICIONES PARA CELEBRAR EL CONTRATO POR INVIAS	
CRITERIO	**ANÁLISIS**
	– RENTABILIDAD DEL PATRIMONIO (ROE): Mayor o Igual a 13% – RENTABILIDAD DEL ACTIVO (ROA): Mayor o Igual a 9% Ver numeral 4.0. “ANÁLISIS DE ÍNDICES FINANCIEROS”

Fuente: elaboración propia. Oficina de Tecnologías de la Información y Comunicaciones OTIC - INVIAS (2026)

4.0 INDICADORES FINANCIEROS

Para el análisis financiero del presente proceso se tomó como fuente la información contenida en la Base Completa de Estados Financieros 2025, publicada por la Superintendencia de Sociedades en el portal de Informes Económicos y Financieros. Inicialmente se identificó una muestra de cincuenta y dos (52) empresas clasificadas en los códigos CIIU : 6202 – Actividades de consultoría informática y administración de instalaciones informáticas, 6209 – Otras actividades de tecnologías de información y actividades de servicios informáticos, y 6311 – Procesamiento de datos, alojamiento (hosting) y actividades relacionadas, por corresponder a actividades económicas directamente relacionadas con el objeto contractual.

Posteriormente, la base de datos fue objeto de un proceso de depuración, mediante el cual se conservaron únicamente aquellas empresas que presentaban información financiera completa y consistente, patrimonio positivo, activos positivos e ingresos operacionales acordes con la actividad económica desarrollada. Así mismo, se excluyeron los registros con información incompleta o inconsistente, empresas sin actividad operativa representativa y aquellas cuyos indicadores financieros presentaban comportamientos atípicos que pudieran distorsionar los resultados del análisis y afectar la representatividad de la muestra.

Como resultado de este procedimiento, se obtuvo una muestra representativa del sector, la cual constituye una base objetiva y suficiente para determinar los indicadores de capacidad financiera y capacidad organizacional que serán exigidos en el presente proceso de contratación, garantizando que dichos requisitos reflejen las condiciones reales del mercado y favorezcan la pluralidad de oferentes.

MUESTRA

No. de Muestra	NIT	Razon Social de la Sociedad	Clasificación Industrial Internacional Uniforme Versión 4 A.C (CIIU)*	Fecha Corte	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ENDEUDAMIENTO (PAS TOT / ACT TOTAL)	COBERTURA DE INTERESES (UTIL OPER / GASTOS FINANC)	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	RENTABILIDAD ACTIVO (UTIL OPER / ACT)	CAPITAL DE TRABAJO (ACT CTE - PAS CTE)
1	800042471	ARUS S.A.S.	J6202	31/12/2025	1,54	55,64 %	2,31	14,05 %	6,23%	22.693.522
2	800057965	VISION SOFTWARE SAS	J6202	31/12/2025	1,18	82,32 %	3,68	63,55 %	11,24%	6.442.415
3	800114672	STEFANINI COLOMBIA SAS	J6202	31/12/2025	1,56	57,98 %	3,46	18,71 %	7,86%	16.968.042
4	800159527	AMADEUS IT GROUP COLOMBIA SAS	J6202	31/12/2025	1,07	75,83 %	2,44	64,21 %	15,52%	4.683.790
5	800241958	HEWLETT PACKARD COLOMBIA LTDA	J6202	31/12/2025	2,13	51,78 %	2,44	16,94 %	8,17%	141.708.330
6	830039329	IMAGE QUALITY OUTSOURCING SAS	J6311	31/12/2025	1,63	52,00 %	1,02	5,59%	2,68%	15.972.995
7	830047444	SERVICIOS ESPECIALIZADOS DE TECNOLOGIA E INFORMATICA SETI SAS	J6202	31/12/2025	1,08	78,13 %	4,74	112,53%	24,61%	2.115.136
8	830055791	AXITY COLOMBIA SAS	J6202	31/12/2025	1,2	68,61 %	2,66	47,50 %	14,91%	13.343.270
9	830084433	SOCIEDAD CAMERAL DE	J6209	31/12/2025	1,99	29,36 %	53,01	12,69 %	8,96%	10.524.612

No. de Muestra	NIT	Razon Social de la Sociedad	Clasificación Industrial Internacional Uniforme Versión 4 A.C (CIIU)*	Fecha Corte	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ENDEUDAMIENTO (PAS TOT / ACT TOTAL)	COBERTURA DE INTERESES (UTIL OPER / GASTOS FINANC)	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	RENTABILIDAD ACTIVO (UTIL OPER / ACT)	CAPITAL DE TRABAJO (ACT CTE - PAS CTE)
		CERTIFICACION DIGITAL CERTICAMARA S A								
10	830096374	INDRA SISTEMAS S,A SUC COLOMBIA	J6202	31/12/2025	1,93	45,64 %	10,11	38,89 %	21,14%	34.238.707
11	830114969	TOPAZ COLOMBIA SA	J6202	31/12/2025	2	41,12 %	1,94	22,71 %	13,37%	51.469.312
12	900089104	ENLACE OPERTATIVO S.A.	J6311	31/12/2025	2	36,43 %	24,73	65,73 %	41,78%	12.464.109
13	900103457	TCS URUGUAY S.A. SUCURSAL COLOMBIA	J6202	31/12/2025	2,79	32,04 %	35,42	33,16 %	22,53%	95.334.403
14	900195141	EQUINIX COLOMBIA INC PTE LTD SUCURSAL COLOMBIA	J6311	31/12/2025	3,43	7,10%	72,95	7,57%	7,04%	81.744.573
15	900210032	NTT DATA SPAIN S.L	J6202	31/12/2025	2,7	36,82 %	2,63	4,85%	3,07%	52.209.623
16	900478383	SOFTWAREONE COLOMBIA SAS	J6202	31/12/2025	1,23	94,24 %	5,37	186,67%	10,75%	46.088.219
17	901445912	WIZELINE S.A.S.	J6202	31/12/2025	1,1	69,12 %	1,1	166,72%	51,47%	529.179

No. de Muestra	NIT	Razon Social de la Sociedad	Clasificación Industrial Internacional Uniforme Versión 4 A.C (CIIU)*	Fecha Corte	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ENDEUDAMIENTO (PAS TOT / ACT TOTAL)	COBERTURA DE INTERESES (UTIL OPER / GASTOS FINANC)	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	RENTABILIDAD ACTIVO (UTIL OPER / ACT)	CAPITAL DE TRABAJO (ACT CTE - PAS CTE)
18	800046226	HEINSOHN BUSINESS TECHNOLOGY S.A BIC	J6202	31/12/2025	4,1	19,47 %	2,51	26,79 %	21,57%	72.803.415
19	830001637	SONDA DE COLOMBIA S.A.	J6202	31/12/2025	1,91	41,41 %	1,99	5,55%	3,25%	76.177.938
20	830042244	DIGITAL WARE SAS	J6202	31/12/2025	1,41	37,23 %	3,22	21,87 %	13,73%	7.726.143
21	830078515	LIBERTY NETWORKS DE COLOMBIA S.A.S	J6311	31/12/2025	1,48	32,64 %	2,08	7,14%	4,81%	110.571.887
22	860002120	IBM DE COLOMBIA SAS	J6202	31/12/2025	1,33	73,75 %	1,88	33,45 %	8,78%	96.155.292
23	890206351	SISTEMAS Y COMPYTADORES S.A.	J6311	31/12/2025	3,32	21,95 %	203,49	36,54 %	28,52%	61.062.917
24	890321151	CARVAJAL TECNOLOGIA Y SERVICIOS S.A.S.	J6311	31/12/2025	1,59	32,18 %	6,38	16,40 %	11,12%	21.917.910
25	900074316	GFT TECHONOLOGIES COLOMBIA SAS	J6202	31/12/2025	1,48	57,26 %	7,89	27,75 %	11,86%	30.928.726
26	900128566	NTT DATA COLOMBIA S. A. S.	J6202	31/12/2025	1,72	58,44 %	5,42	41,56 %	17,27%	50.393.464
27	900422614	EXPERIAN COLOMBIA SA	J6311	31/12/2025	2,01	42,66 %	2,19	10,97 %	6,29%	117.965.882

No. de Muestra	NIT	Razon Social de la Sociedad	Clasificación Industrial Internacional Uniforme Versión 4 A.C (CIIU)*	Fecha Corte	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ENDEUDAMIENTO (PAS TOT / ACT TOTAL)	COBERTURA DE INTERESES (UTIL OPER / GASTOS FINANC)	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	RENTABILIDAD ACTIVO (UTIL OPER / ACT)	CAPITAL DE TRABAJO (ACT CTE - PAS CTE)
28	901183029	PEXTO COLOMBIA SAS	J6311	31/12/2025	1,22	69,80 %	0,35	34,33 %	10,37%	51.385.508
29	830021894	SINCOSOFT SAS	J6311	31/12/2025	3,03	25,47 %	4	38,68 %	28,82%	27.182.894
30	830056149	COMPAÑIA INTERNACIONAL DE INTEGRACION SA	J6311	31/12/2025	3,45	22,28 %	7,8	19,28 %	14,99%	50.664.166
31	830058677	IFX NETWORKS COLOMBIA SAS	J6209	31/12/2025	1,55	47,21 %	1,22	7,65%	4,04%	17.778.896
32	830120215	S3 SIMPLE SMART SPEEDY SAS	J6311	31/12/2025	2,41	65,86 %	2,31	33,60 %	11,47%	23.407.903
33	900097333	SISTEMA INTEGRADO MULTIPLE DE PAGOS ELECTRONICOS SA	J6311	31/12/2025	2,6	56,11 %	2110,92	75,41 %	33,10%	12.778.475
34	900148177	PEAR SOLUTIONS SAS	J6202	31/12/2025	2,73	55,37 %	1,28	18,25 %	8,15%	35.322.693
35	900169608	NEORIS COLOMBIA SAS	J6202	31/12/2025	2,48	37,57 %	6,88	40,70 %	25,41%	27.323.850
36	900200356	CLOUXTER SAS	J6202	31/12/2025	1,43	68,98 %	2,01	37,80 %	11,73%	5.890.423

No. de Muestra	NIT	Razon Social de la Sociedad	Clasificación Industrial Internacional Uniforme Versión 4 A.C (CIIU)*	Fecha Corte	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ENDEUDAMIENTO (PAS TOT / ACT TOTAL)	COBERTURA DE INTERESES (UTIL OPER / GASTOS FINANC)	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	RENTABILIDAD ACTIVO (UTIL OPER / ACT)	CAPITAL DE TRABAJO (ACT CTE - PAS CTE)
37	900204272	GESTION DE SEGURIDAD ELECTRONICA SA	J6202	31/12/2025	4,05	19,57 %	26,39	36,05 %	28,99%	67.318.683
38	900237844	THE BEST EXPERIENCE IN TECHNOLOGY SAS	J6202	31/12/2025	1,6	59,18 %	1,84	56,48 %	23,05%	11.705.237
39	900238438	GROW DATA SAS	J6202	31/12/2025	1,62	58,80 %	48,18	38,85 %	16,01%	45.098.976
40	900294369	COMERCIAL CARD SAS	J6209	31/12/2025	1,47	66,94 %	3,58	131,86%	43,59%	30.464.581
41	900340993	ADMISNISTRACION DE REDES Y PROYECTOS SAS	J6202	31/12/2025	1,61	57,37 %	8,74	68,95 %	29,40%	4.938.798
42	900389156	NOVENTIQ INTERNATIONAL COLOMBIA SAS	J6202	31/12/2025	1,59	97,58 %	3,56	529,16%	12,80%	21.078.564
43	900396176	MNEMO COLOMBIA SAS	J6202	31/12/2025	1,92	58,39 %	20,75	38,84 %	16,16%	34.577.645
44	900557218	DAVINCI TECHNLOGIES SAS	J6202	31/12/2025	1,11	90,21 %	1,26	120,12%	11,76%	3.849.622
45	900572445	CIFIN SAS	J6311	31/12/2025	1,56	35,17 %	113,24	6,47%	4,19%	41.294.060
46	900631710	VERITRAN COLOMBIA S.A.S.	J6202	31/12/2025	2,42	39,37 %	6,31	86,23 %	52,28%	26.729.662

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

No. de Muestra	NIT	Razon Social de la Sociedad	Clasificación Industrial Internacional Uniforme Versión 4 A.C (CIIU)*	Fecha Corte	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ENDEUDAMIENTO (PAS TOT / ACT TOTAL)	COBERTURA DE INTERESES (UTIL OPER / GASTOS FINANC)	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	RENTABILIDAD ACTIVO (UTIL OPER / ACT)	CAPITAL DE TRABAJO (ACT CTE - PAS CTE)
47	900682258	DLOCAL COLOMBIA SAS	J6311	31/12/2025	1,03	97,36%	12,13	262,87%	6,93%	5.098.200
48	901148432	IGT SERVICES AND TECHNOLOGIES COLOMBIA SAS	J6202	31/12/2025	4,73	15,80%	2,14	18,37%	15,47%	38.961.281
49	830099847	SOFTTEK RENOVATION SAS	J6202	31/12/2025	1,24	70,79%	0,43	19,62%	5,73%	7.893.856
50	830131674	HR SOLUTIONS SAS	J6202	31/12/2025	6,53	47,30%	64,3	101,68%	53,58%	43.255.425
51	860502327	JAIME TORRES C Y CIA SA	J6311	31/12/2025	3,3	19,46%	2,54	9,14%	7,36%	10.995.356
52	860510031	GRUPO ASESORIA EN SISTEMATIZACION DE DATOS S.A.S.	J6311	31/12/2025	1,64	36,12%	3,5	16,66%	10,64%	45.321.460

*Convenciones

J6202 - Actividades de consultoría informática y actividades de administración de instalaciones informáticas
J6209 - Otras actividades de tecnologías de información y actividades de servicios informáticos
J6311 - Procesamiento de datos, alojamiento (hosting) y actividades relacionadas

A. INDICADORES DE CAPACIDAD FINANCIERA

- **INDICE DE LIQUIDEZ**

La siguiente tabla presenta el índice de LIQUIDEZ de la muestra en orden ascendente y la **MEDIA PODADA.**

Donde:
N: Numero de muestra = 52
a: porción de los datos que se quien excluir = 12%

52 x 12% = 6 (podamos los seis (3) datos más bajos y los seis (3) datos más altos)

ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)
1	1	11	1,3	21	1,59	31	1,93	41	2,7	51	4,73
2	1,1	12	1,4	22	1,59	32	1,99	42	2,73	52	6,53
3	1,1	13	1,4	23	1,6	33	2	43	2,79		
4	1,1	14	1,47	24	1,61	34	2	44	3,03		
5	1,1	15	1,48	25	1,62	35	2,01	45	3,3		
6	1,2	16	1,48	26	1,63	36	2,13	46	3,32		
7	1,2	17	1,54	27	1,64	37	2,41	47	3,43		
8	1,2	18	1,55	28	1,72	38	2,42	48	3,45		
9	1,2	19	1,56	29	1,91	39	2,48	49	4,05		
10	1,2	20	1,56	30	1,92	40	2,6	50	4,1		

A continuación, se presenta la muestra acotada resultante de eliminar los valores extremos identificados durante el análisis estadístico, con el fin de obtener indicadores financieros representativos del mercado:

ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)	ITEM	INDICE DE LIQUIDEZ (ACT CTE / PAS CTE)
1	1,1	10	1,4	19	1,59	28	1,93	37	2,6	46	4,05
2	1,1	11	1,47	20	1,6	29	1,99	38	2,7		
3	1,2	12	1,48	21	1,61	30	2	39	2,73		
4	1,2	13	1,48	22	1,62	31	2	40	2,79		
5	1,2	14	1,54	23	1,63	32	2,01	41	3,03		
6	1,2	15	1,55	24	1,64	33	2,13	42	3,3		
7	1,2	16	1,56	25	1,72	34	2,41	43	3,32		
8	1,3	17	1,56	26	1,91	35	2,42	44	3,43		
9	1,4	18	1,59	27	1,92	36	2,48	45	3,45		

A partir de la nueva muestra se calculan los siguientes datos estadísticos con el fin de determinar el indicador según la muestra así:

DATOS ESTADISTICOS	LIQUIDEZ
MINIMO	1,10
MAXIMO	4,05
PROMEDIO	1,97
MEDIANA	1,63
MEDIA GEOMETRICA	1,86
MEDIA ARMONICA	1,76
LIQUIDEZ SEGÚN MUESTRA	**1,76**

- **INDICE DE ENDEUDAMIENTO**

La siguiente tabla presenta el índice de ENDEUDAMIENTO de la muestra en orden ascendente y la **MEDIA PODADA.**

Donde:
N: Numero de muestra = 52
a: porción de los datos que se quien excluir = 12%

52 x 12% = 6 (podamos los seis (3) datos más bajos y los seis (3) datos más altos)

ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)
1	0,07	11	0,32	21	0,41	31	0,57	41	0,69	51	0,97
2	0,16	12	0,33	22	0,43	32	0,57	42	0,69	52	0,98
3	0,19	13	0,35	23	0,46	33	0,58	43	0,7		
4	0,19	14	0,36	24	0,47	34	0,58	44	0,71		
5	0,2	15	0,36	25	0,47	35	0,58	45	0,74		
6	0,22	16	0,37	26	0,52	36	0,59	46	0,76		
7	0,22	17	0,37	27	0,52	37	0,59	47	0,78		
8	0,25	18	0,38	28	0,55	38	0,66	48	0,82		
9	0,29	19	0,39	29	0,56	39	0,67	49	0,9		
10	0,32	20	0,41	30	0,56	40	0,69	50	0,94		

A continuación, se presenta la muestra acotada resultante de eliminar los valores extremos identificados durante el análisis estadístico, con el fin de obtener indicadores financieros representativos del mercado.:

ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)	ITEM	ÍNDICE DE ENDEUDAMIENTO (PAS TOTAL / ACT TOTAL)
1	0,19	11	0,36	21	0,47	31	0,58	41	0,71
2	0,2	12	0,36	22	0,47	32	0,58	42	0,74
3	0,22	13	0,37	23	0,52	33	0,59	43	0,76
4	0,22	14	0,37	24	0,52	34	0,59	44	0,78
5	0,25	15	0,38	25	0,55	35	0,66	45	0,82
6	0,29	16	0,39	26	0,56	36	0,67	46	0,9
7	0,32	17	0,41	27	0,56	37	0,69		
8	0,32	18	0,41	28	0,57	38	0,69		
9	0,33	19	0,43	29	0,57	39	0,69		
10	0,35	20	0,46	30	0,58	40	0,7		

A partir de la nueva muestra se calculan los siguientes datos estadísticos con el fin de determinar el indicador según la muestra así:

DATOS ESTADISTICOS	ENDEUDAMIENTO
MINIMO	0,19
MAXIMO	0,90
PROMEDIO	0,50
MEDIANA	0,52
MEDIA GEOMETRICA	0,47
MEDIA ARMONICA	0,43
ENDEUDAMIENTO SEGÚN MUESTRA	**0,52**

- **INDICE DE RAZON COBERTURA INTERESES**

La siguiente tabla presenta el índice de **COBERTURA DE INTERESES** de la muestra en orden ascendente y la **MEDIA PODADA.**

Donde:
N: Numero de muestra = 52
a: porción de los datos que se quien excluir = 12%

52 x 12% = 6 (podamos los seis (3) datos más bajos y los seis (3) datos más altos)

ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)
1	0,35	11	1,99	21	2,54	31	4,74	41	12,1	51	203
2	0,43	12	2,01	22	2,63	32	5,37	42	20,8	52	2111
3	1,02	13	2,08	23	2,66	33	5,42	43	24,7		
4	1,1	14	2,14	24	3,22	34	6,31	44	26,4		
5	1,22	15	2,19	25	3,46	35	6,38	45	35,4		
6	1,26	16	2,31	26	3,5	36	6,88	46	48,2		
7	1,28	17	2,31	27	3,56	37	7,8	47	53		
8	1,84	18	2,44	28	3,58	38	7,89	48	64,3		
9	1,88	19	2,44	29	3,68	39	8,74	49	73		
10	1,94	20	2,51	30	4	40	10,1	50	113		

A continuación, se presenta la muestra acotada resultante de eliminar los valores extremos identificados durante el análisis estadístico, con el fin de obtener indicadores financieros representativos del mercado

ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)	ITEM	ÍNDICE DE COBERTURA DE INTERESES (UTIL OPER / GASTOS FIN)
1	1,1	11	2,14	21	3,22	31	6,31	41	26,4
2	1,22	12	2,19	22	3,46	32	6,38	42	35,4
3	1,26	13	2,31	23	3,5	33	6,88	43	48,2
4	1,28	14	2,31	24	3,56	34	7,8	44	53
5	1,84	15	2,44	25	3,58	35	7,89	45	64,3
6	1,88	16	2,44	26	3,68	36	8,74	46	73
7	1,94	17	2,51	27	4	37	10,1		
8	1,99	18	2,54	28	4,74	38	12,1		
9	2,01	19	2,63	29	5,37	39	20,8		
10	2,08	20	2,66	30	5,42	40	24,7		

A partir de la nueva muestra se calculan los siguientes datos estadísticos con el fin de determinar el indicador según la muestra así:

DATOS ESTADISTICOS	COBERTURA INTERES
MINIMO	1,10
MAXIMO	72,95
PROMEDIO	10,72
MEDIANA	3,53
MEDIA GEOMETRICA	4,94
MEDIA ARMONICA	3,21
RAZON DE COBERTURA SEGÚN MUESTRA	**3,21**

CAPITAL DE TRABAJO

El capital de trabajo representa la capacidad financiera del proponente para atender las obligaciones de corto plazo y garantizar la disponibilidad de recursos para la adecuada ejecución del contrato. Este indicador corresponde a la diferencia entre el activo corriente y el pasivo corriente, reflejando los recursos líquidos con los que cuenta el proponente una vez cubiertas sus obligaciones exigibles en el corto plazo.

Un capital de trabajo positivo constituye un indicador de solvencia y estabilidad financiera, permitiendo evidenciar que el proponente dispone de la capacidad económica necesaria para financiar el inicio y desarrollo de las actividades contractuales sin comprometer su liquidez operativa.

Teniendo en cuenta la naturaleza del objeto contractual, el presupuesto oficial del proceso y la necesidad de garantizar que el futuro contratista cuente con recursos suficientes para asumir las obligaciones derivadas de la ejecución del contrato, la Entidad considera procedente exigir un capital de trabajo que permita evidenciar una adecuada capacidad financiera, sin generar restricciones injustificadas a la participación de oferentes.

En consecuencia, el Instituto Nacional de Vías – INVÍAS establece como requisito habilitante un Capital de Trabajo mayor o igual al setenta por ciento (70 %) del presupuesto oficial, considerando que el objeto contractual comprende la adquisición e implementación de una solución integral de ciberseguridad, la cual involucra licenciamiento, servicios especializados, implementación, integración, soporte técnico y operación. Este porcentaje garantiza que el futuro contratista cuente con recursos líquidos suficientes para atender las obligaciones derivadas del contrato durante su ejecución, manteniendo un equilibrio entre la adecuada capacidad financiera requerida y la promoción de la pluralidad de oferentes, de conformidad con las condiciones evidenciadas en el estudio del sector y el análisis financiero realizado.

El indicador será MAYOR O IGUAL AL 70% DEL PRESUPUESTO OFICIAL

B. INDICADORES DE CAPACIDAD ORGANIZACIONAL

- **ÍNDICE DE RENTABILIDAD DEL PATRIMONIO**

La siguiente tabla presenta el índice de R**ENTABILIDAD DEL PATRIMONIO** de la muestra en orden ascendente y la **MEDIA PODADA**

Donde:
N: Numero de muestra = 52
a: porción de los datos que se quien excluir = 12%

52 x 12% = 6 (podamos los seis (3) datos más bajos y los seis (3) datos más altos)

ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)
1	0,05	11	0,14	21	0,23	31	0,39	41	0,66	51	2,63
2	0,06	12	0,16	22	0,27	32	0,39	42	0,69	52	5,29
3	0,06	13	0,17	23	0,28	33	0,39	43	0,75		
4	0,06	14	0,17	24	0,33	34	0,39	44	0,86		
5	0,07	15	0,18	25	0,33	35	0,41	45	1,02		
6	0,08	16	0 ,18	26	0,34	36	0,42	46	1,13		
7	0,08	17	0,19	27	0,34	37	0,47	47	1,2		
8	0,09	18	0,19	28	0,36	38	0,56	48	1,32		
9	0,11	19	0,2	29	0,37	39	0,64	49	1,67		
10	0,13	20	0,22	30	0,38	40	0,64	50	1,87		

A continuación, se presenta la muestra acotada resultante de eliminar los valores extremos identificados durante el análisis estadístico, con el fin de obtener indicadores financieros representativos del mercado:

ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)	ITEM	RENTABILIDAD PATRIMONIO (UTIL OPER / PAT)

1	0,06	11	0,17	21	0,33	31	0,39	41	0,86
2	0,07	12	0,18	22	0,33	32	0,41	42	1,02
3	0,08	13	0 ,18	23	0,34	33	0,42	43	1,13
4	0,08	14	0,19	24	0,34	34	0,47	44	1,2
5	0,09	15	0,19	25	0,36	35	0,56	45	1,32
6	0,11	16	0,2	26	0,37	36	0,64	46	1,67
7	0,13	17	0,22	27	0,38	37	0,64		
8	0,14	18	0,23	28	0,39	38	0,66		
9	0,16	19	0,27	29	0,39	39	0,69		
10	0,17	20	0,28	30	0,39	40	0,75		

A partir de la nueva muestra se calculan los siguientes datos estadísticos con el fin de determinar el indicador según la muestra así:

DATOS ESTADISTICOS	RENTABILIDAD DEL PATRIMONIO
MINIMO	0,06
MAXIMO	1,67
PROMEDIO	0,43
MEDIANA	0,34
MEDIA GEOMETRICA	0,32
MEDIA ARMONICA	0,23
RENTAB. PATRIMONIO SEGÚN MUESTRA	**0,23**

- **ÍNDICE DE RENTABILIDAD DEL ACTIVO**

La siguiente tabla presenta el índice de **RENTABILIDAD DEL ACTIVO** de la muestra en orden ascendente y la **MEDIA PODADA.**

Donde:
N: Numero de muestra = 52
a: porción de los datos que se quien excluir = 12%

52 x 12% = 6 (podamos los seis (3) datos más bajos y los seis (3) datos más altos)

ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)
1	0,03	11	0,07	21	0,11	31	0,15	41	0,25	51	0,52
2	0,03	12	0,07	22	0,11	32	0,15	42	0,25	52	0,54
3	0,03	13	0,08	23	0,11	33	0,16	43	0,29		
4	0,04	14	0,08	24	0,12	34	0,16	44	0,29		
5	0,04	15	0,08	25	0,12	35	0,16	45	0,29		
6	0,05	16	0,09	26	0,12	36	0,17	46	0,29		
7	0,06	17	0,09	27	0,13	37	0,21	47	0,33		
8	0,06	18	0,1	28	0,13	38	0,22	48	0,42		
9	0,06	19	0,11	29	0,14	39	0,23	49	0,44		
10	0,07	20	0,11	30	0,15	40	0,23	50	0,51		

A continuación, se presenta la muestra acotada resultante de eliminar los valores extremos identificados durante el análisis estadístico, con el fin de obtener indicadores financieros representativos del mercado:

ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)	ITEM	RENTABILIDAD ACTIVO (UTIL OPER / ACTIVO)

1	0,04	11	0,08	21	0,12	31	0,16	41	0,29
2	0,04	12	0,08	22	0,12	32	0,16	42	0,29
3	0,05	13	0,09	23	0,12	33	0,17	43	0,29
4	0,06	14	0,09	24	0,13	34	0,21	44	0,33
5	0,06	15	0,1	25	0,13	35	0,22	45	0,42
6	0,06	16	0,11	26	0,14	36	0,23	46	0,44
7	0,07	17	0,11	27	0,15	37	0,23		
8	0,07	18	0,11	28	0,15	38	0,25		
9	0,07	19	0,11	29	0,15	39	0,25		
10	0,08	20	0,11	30	0,16	40	0,29		

A partir de la nueva muestra se calculan los siguientes datos estadísticos con el fin de determinar el indicador según la muestra así:

DATOS ESTADISTICOS	RENTABILIDAD DEL ACTIVO
MINIMO	0,04
MAXIMO	0,44
PROMEDIO	0,16
MEDIANA	0,13
MEDIA GEOMETRICA	0,13
MEDIA ARMONICA	0,11
RENTAB. DEL ACTIVO SEGÚN MUESTRA	**0,16**

RESULTADO DE LA MUESTRA ANTERIOR SUPERINTENDENCIA DE SOCIEDADES

El análisis de la información financiera reportada por las empresas que conforman la muestra depurada de la Superintendencia de Sociedades evidencia un comportamiento financiero estable del sector de Tecnologías de la Información y las Comunicaciones (TIC), específicamente de las actividades económicas clasificadas en los códigos CIIU 6202, 6209 y 6311**,** relacionadas con el objeto del presente proceso contractual.

METRICA	LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD SOBRE PATRIMONIO	RENTABILIDAD SOBRE ACTIVO
MINIMO	1,1	0,19	1,1	0,06	0,04

MAXIMO	4,05	0,9	72,95	1,67	0,44
PROMEDIO	1,97	0,5	10,72	0,43	0,16
MEDIANA	1,63	0,52	3,53	0,34	0,13
MEDIA GEOMETRICA	1,86	0,47	4,94	0,32	0,13
MEDIA ARMONICA	1,76	0,43	3,21	0,23	0,11
MUESTRA	**1,76**	**52%**	**3,21**	**23%**	**16%**

C. INDICADORES REQUERIDOS EN PROCESOS DE SELECCIÓN ADELANTADOS POR EL INVÍAS

Con el fin de establecer indicadores financieros acordes con las condiciones del mercado y la experiencia institucional, la Entidad tomó como referencia el proceso de contratación No. 1353-2025, adelantado por el Instituto Nacional de Vías – INVÍAS, por corresponder a un proceso de características similares al presente, relacionado con la implementación de soluciones de ciberseguridad.

El análisis de este antecedente permitió identificar los indicadores de capacidad financiera y capacidad organizacional previamente exigidos por la Entidad, los cuales constituyen un referente para la estructuración del presente proceso, en la medida en que fueron definidos para un contrato de naturaleza tecnológica y complejidad similar.

Los indicadores establecidos en dicho proceso fueron los siguientes:

PROCESO	INDICE DE LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO	CAPITAL DE TRABAJO
CONTRATO INVÍAS 1353-2025	1,5	63%	2,4	0,07	0,05	80%
HISTORICOS	**1,5**	**0,63**	**2,4**	**0,07**	**0,05**	**0,8**

En consecuencia, estos indicadores fueron considerados como una de las fuentes de información para el análisis comparativo realizado por la Entidad, junto con la información financiera de la

Superintendencia de Sociedades y los indicadores exigidos por otras entidades estatales, con el propósito de establecer requisitos habilitantes objetivos, proporcionales y acordes con las condiciones actuales del mercado.

D. INDICADORES REQUERIDOS EN PROCESOS DE SELECCIÓN ADELANTADOS POR OTRAS ENTIDADES

Con el propósito de establecer indicadores financieros acordes con las condiciones del mercado y garantizar su proporcionalidad frente al objeto contractual, la Entidad realizó la consulta de procesos de contratación publicados en la plataforma SECOP II, correspondientes a entidades estatales que adelantaron procesos para la adquisición e implementación de soluciones de ciberseguridad y servicios especializados de tecnologías de la información.

Como resultado de esta consulta, se analizaron procesos con características similares al presente, adelantados por diferentes entidades públicas, cuyos indicadores de capacidad financiera y capacidad organizacional se relacionan a continuación:

ENTIDAD	No. DE PROCESO	INDICE DE LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
Superintendencia Nacional De Salud	387 DE 2025	1,3	70,00%	1,3	0,05	0,04
Dirección De Investigación Criminal E Interpol	03-2-10063-24	1,53	65,00%	3,38	0,09	0,05
Unidad De Busqueda De Personas Desaparecidas	667-2025-UBPD	1,46	70,00%	1,26	0,09	0,03
DILOF	06-2-10326-25	0,77	74,00%	0,98	0,06	0,03

Congreso De La República - Honorable Senado De La República	1460-2024	2,3	48,00%	2,2	0,14	0,13
PROMEDIOS OTRAS ENTIDADES		**1,47**	**65,00%**	**1,82**	**0,09**	**0,06**

Del análisis efectuado se evidencia que los indicadores financieros exigidos por otras entidades estatales presentan un comportamiento homogéneo y guardan relación con la naturaleza de los procesos de contratación de soluciones de ciberseguridad y servicios especializados de tecnologías de la información.

Estos resultados constituyen un referente para la estructuración de los requisitos habilitantes del presente proceso, toda vez que reflejan las condiciones financieras exigidas por otras entidades públicas en procesos de características similares y fueron considerados, junto con la información financiera de la Superintendencia de Sociedades y los antecedentes contractuales del INVÍAS, para definir los indicadores de capacidad financiera y capacidad organizacional del presente proceso

E. ANÁLISIS COMPARATIVO DE LOS INDICADORES FINANCIEROS

Para la determinación de los indicadores de capacidad financiera y capacidad organizacional del presente proceso, la Entidad realizó un análisis comparativo tomando como referencia tres fuentes de información:

- La información financiera reportada por una muestra depurada de empresas de la Superintendencia de Sociedades, correspondiente a los códigos CIIU 6202, 6209 y 6311, por ser actividades económicas relacionadas con el objeto contractual.
- Los indicadores financieros exigidos por el Instituto Nacional de Vías – INVÍAS en procesos contractuales con características similares.
- Los indicadores financieros establecidos por otras entidades estatales en procesos de contratación adelantados a través de la plataforma SECOP II para la adquisición de soluciones y servicios de tecnologías de la información y ciberseguridad.

Con base en el análisis efectuado, se consolidaron los valores promedio obtenidos en cada una de las fuentes consultadas, con el propósito de establecer requisitos habilitantes acordes con las

condiciones financieras del mercado, garantizando el equilibrio entre la adecuada capacidad económica de los futuros contratistas y la promoción de la pluralidad de oferentes.

INDICADORES	INDICE DE LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
PROMEDIO INDICADORES OTRAS ENTIDADES PROCESOS SECOP II	1,47	65,0%	1,82	0,09	0,06
PROMEDIO INDICADORES INVIAS	1,50	63,0%	2,40	0,07	0,05
INDICADORES SEGÚN MUESTRA SUPERSOCIEDADES	1,76	52,0%	3,21	0,23	0,16
PROMEDIO	**1,58**	**60%**	**2,48**	**0,13**	**0,09**

Como resultado del análisis comparativo realizado entre la información financiera de la Superintendencia de Sociedades, los antecedentes contractuales del INVÍAS y los procesos adelantados por otras entidades estatales, se determinaron los siguientes indicadores de capacidad financiera y capacidad organizacional para el presente proceso.

F. INDICADORES DE CAPACIDAD FINANCIERA Y ORGANIZACIONAL A REQUERIR EN EL PRESENTE PROCESO

Con fundamento en el análisis financiero realizado, los indicadores de capacidad financiera y capacidad organizacional establecidos para el presente proceso se consideran proporcionales a la naturaleza, complejidad y valor del contrato. Así mismo, reflejan las condiciones financieras del mercado, al haber sido definidos con base en la información de la Superintendencia de Sociedades,

los antecedentes contractuales del INVÍAS y los procesos similares adelantados por otras entidades estatales.

En consecuencia, los requisitos establecidos garantizan que los futuros proponentes cuenten con la capacidad financiera y organizacional necesaria para asumir las obligaciones derivadas del contrato, contribuyendo a una adecuada ejecución contractual, a la mitigación de riesgos financieros y al cumplimiento de los principios de selección objetiva, libre concurrencia, proporcionalidad y pluralidad de oferentes previstos en la normativa de contratación estatal.

CAPACIDAD FINANCIERA	ÍNDICE REQUERIDO
Índice de Liquidez: Activo Corriente/Pasivo Corriente	Mayor o igual (≥) a 1,58
Nivel de Endeudamiento: Pasivo Total / Activo Total	Menor o Igual (≤) a 60%
Razón de cobertura de intereses: Utilidad Operacional / Gastos Financieros	Mayor o Igual (≥) a 2,48 o indeterminado
Capital de Trabajo: Activo Corriente - Pasivo Corriente	Mayor o igual (≥) al 70% del presupuesto del proceso
CAPACIDAD ORGANIZACIONAL	**ÍNDICE REQUERIDO**
Rentabilidad del patrimonio: Utilidad Operacional / Patrimonio	Mayor o Igual (≥) a 13%
Rentabilidad del activo: Utilidad Operacional / Activo Total	Mayor o Igual (≥) a 9%

Así mismo, es de resaltar que los indicadores establecidos permiten la pluralidad de oferentes y selección objetiva dentro del proceso de selección en curso y a su vez buscan que los proponentes interesados en el proceso cuenten con un musculo financiero adecuado que no ponga en riesgo la ejecución del contrato a suscribirse.

CRITERIOS DIFERENCIALES PARA LAS MIPYMES LOS EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD

El **Decreto 0287 de 2026** establece un sistema de preferencias para personas con discapacidad, y dispone criterios habilitantes diferenciales o ajustados en:

1. Experiencia
2. **Índices de capacidad financiera.**
3. Índices de capacidad organizacional.
4. Valor de la garantía de seriedad de la oferta.

Para MIPYMES, el artículo 2.2.1.2.4.2.18 del Decreto 1082 contempla expresamente los **índices de capacidad financiera y de capacidad organizacional** como posibles criterios diferenciales.

(…) De acuerdo con el numeral 1 del artículo 12 de la Ley 590 de 2000, según los resultados del análisis del sector, las Entidades Estatales indistintamente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos de las Mipyme domiciliadas en Colombia. Para el efecto, en función de los criterios de clasificación empresarial, los Documentos del Proceso deberán incorporar requisitos habilitantes diferenciales relacionados con alguno o algunos de los siguientes aspectos:

1. Tiempo de experiencia.
2. Número de contratos para la acreditación de la experiencia.
3. **Índices de capacidad financiera.**
4. Índices de capacidad organizacional.
5. Valor de la garantía de seriedad de la oferta.

De acuerdo con las condiciones habilitantes diferenciales previstas en la normativa aplicable para las MIPYMES y los emprendimientos y empresas de personas con discapacidad, se considera pertinente establecer criterios diferenciales en materia de capacidad financiera, teniendo en cuenta las características del presente proceso.

La selección de **indicadores de capacidad financiera** como criterio diferencial responde a la necesidad de mantener un equilibrio entre la verificación de la capacidad económica mínima requerida

para la adecuada ejecución del contrato y la promoción de condiciones de participación más accesibles para las MIPYMES y los emprendimientos y empresas de personas con discapacidad.

En este sentido, se seleccionan indicadores que permiten evaluar diferentes componentes de la situación financiera de los proponentes. El **Índice de Liquidez** permite determinar la capacidad para atender obligaciones de corto plazo; el **Nivel de Endeudamiento** permite identificar el grado de apalancamiento financiero; la **Razón de Cobertura de Intereses** permite evaluar la capacidad para atender los gastos financieros con los resultados de la operación; y el **Capital de Trabajo** permite valorar la disponibilidad de recursos de corto plazo para atender las obligaciones asociadas a la ejecución contractual.

La selección de estos indicadores permite establecer condiciones habilitantes diferenciales que faciliten la participación de las MIPYMES y de los emprendimientos y empresas de personas con discapacidad, manteniendo al mismo tiempo condiciones mínimas de capacidad financiera acordes con el objeto, alcance, valor y riesgos del proceso.

Con base en el análisis efectuado, se consolidaron los valores promedio obtenidos en cada una de las fuentes consultadas (información financiera reportada por una muestra depurada de empresas de la Superintendencia de Sociedades, indicadores financieros exigidos por el INVÍAS en procesos contractuales con características similares, e indicadores financieros establecidos por otras entidades estatales en procesos de contratación adelantados a través de la plataforma SECOP II), con el propósito de establecer requisitos habilitantes acordes con las condiciones financieras del mercado, garantizando el equilibrio entre la adecuada capacidad económica de los futuros contratistas y la promoción de la pluralidad de oferentes.

Resultados de las diferentes métricas para la muestra Supersociedades

METRICA	LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD SOBRE PATRIMONIO	RENTABILIDAD SOBRE ACTIVO
MINIMO	1,1	0,19	1,1	0,06	0,04
MAXIMO	4,05	0,9	72,95	1,67	0,44
PROMEDIO	1,97	0,5	10,72	0,43	0,16
MEDIANA	1,63	0,52	3,53	0,34	0,13
MEDIA GEOMETRICA	1,86	0,47	4,94	0,32	0,13

MEDIA ARMONICA	1,76	0,43	3,21	0,23	0,11
MUESTRA	**1,76**	**52%**	**3,21**	**23%**	**16%**

Indicadores financieros exigidos por otras entidades estatales y exigidos por el INVIAS en procesos históricos

INDICADORES	INDICE DE LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
PROMEDIO INDICADORES OTRAS ENTIDADES PROCESOS SECOP II	1,47	65,0%	1,82	0,09	0,06
PROMEDIO INDICADORES INVIAS	1,50	63,0%	2,40	0,07	0,05

Para la determinación de los valores diferenciales se tomaron como referencia los resultados estadísticos de las fuentes mencionadas anteriormente. En consecuencia, los valores adoptados buscan reducir el nivel de restricción de los requisitos financieros generales, sin eliminar la capacidad mínima necesaria para una adecuada ejecución contractual.

Dicho esto, y de acuerdo con el análisis de la muestra para determinar los indicadores de capacidad financiera y organizacional anteriormente expuesta, este Comité se permite establecer los indicadores de **CAPACIDAD FINANCIERA PARA CRITERIOS DIFERENCIALES PARA LAS MIPYMES LOS EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD**

CAPITAL DE TRABAJO

El Presupuesto Oficial asciende a **$ 6.030.164.927,00** En este contexto, y atendiendo las características del proceso y la necesidad de establecer condiciones habilitantes proporcionales, se determina un Capital de Trabajo equivalente al 60% del Presupuesto Oficial para las MIPYMES y los emprendimientos y empresas de personas con discapacidad, como condición diferencial orientada

a facilitar su participación, manteniendo a su vez un nivel de disponibilidad de recursos que permita atender las obligaciones de corto plazo asociadas a la ejecución contractual.

El porcentaje adoptado del 60% representa una flexibilización frente al requisito general establecido para los demás proponentes, procurando equilibrar la promoción de la participación y pluralidad de oferentes con la necesidad de conservar una capacidad financiera mínima acorde con las condiciones y riesgos del contrato.

Concepto	Valor
Empresas analizadas	52
Unidad de información	Miles de pesos
Mediana del Capital de Trabajo	28.894.216
Promedio del Capital de Trabajo	37.395.193
Presupuesto Oficial	$ 6.030.164.927
Capital de Trabajo diferencial 60%	$ 3.618.098.956

Los valores adoptados fueron determinados a partir de los resultados estadísticos de la información analizada. Estos valores permiten establecer condiciones diferenciales frente a los requisitos generales, conservando referentes derivados del comportamiento financiero observado en la muestra.

CAPACIDAD FINANCIERA	ÍNDICE REQUERIDO
Índice de Liquidez: Activo Corriente/Pasivo Corriente	Mayor o igual (≥) a 1,47
Nivel de Endeudamiento: Pasivo Total / Activo Total	Menor o Igual (≤) a 52%
Razón de cobertura de intereses: Utilidad Operacional / Gastos Financieros	Mayor o Igual (>) a 1,82 o indeterminado
Capital de Trabajo: Activo Corriente - Pasivo Corriente	Mayor o igual (≥) al 60% del presupuesto del proceso

5.0. ANÁLISIS DE LAS COTIZACIONES RECIBIDAS

Para el análisis del valor estimado de precios, Colombia Compra Eficiente en su Guía para la Elaboración de los Estudios del Sector, incorporó técnicas de análisis de información que permiten a la Entidad Estatal analizar sus adquisiciones de bienes y servicios. Esto en cuanto a valores, cantidad adecuada según la frecuencia de uso del bien y/o servicio y demás datos importantes para determinar de manera objetiva la satisfacción de la necesidad.

Cuando se tenga en cuenta los precios de la entidad de años anteriores a la vigencia del proceso, se deberá efectuar la indexación de valores con el IPP o IPC según corresponda. De no tenerse en cuenta los valores obtenidos del histórico de la Entidad (proyectado), solo se tendrá en cuenta el precio del mercado cotizado, lo cual debe ser sustentado.

Con el objetivo de obtener los valores del mercado, y finalizar de manera adecuada el desarrollo de este análisis estadístico, se debe tener en cuenta las medidas de tendencia central y dispersión recomendadas por Colombia Compra Eficiente, las cuales permiten entender el comportamiento del bien y/o servicio en el mercado.

Como fuente de información del estudio de mercado, la Entidad utilizo cuatro (4) criterios de consulta, con el fin de realizar comparativos de costos, así:

1. Solicitud de Información a Proveedores SECOP II
2. Cotizaciones
3. Análisis de las cotizaciones
4. Precio techo de referencias

1. Solicitud de Información a Proveedores SECOP II

Con el fin de elaborar el estudio de mercado que permita establecer las condiciones económicas que se presentan en el sector y definir los precios de referencia para el presente proceso, se publicó solicitud de cotizaciones mediante la plataforma SECOP II, bajo número SIP-SUBG-OTIC-033-2026 objeto "*CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA EL INSTITUTO NACIONAL DE VÍAS INVIAS, MEDIANTE LA OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS.*"

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

La publicación de la solicitud se realizó el 19 DE JUNIO 2026, estableciendo como fecha límite para la recepción de propuestas el 03 DE JULIO 2026, tal como se evidencia a continuación:



Proceso : SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD - SIP-SUBG-OTIC-033-2026

Solicitud de información a los Proveedores
SIP-SUBG-OTIC-033-2026 (En análisis) Pliegos

Unidad de contratación Oficina TICs
Ver Enlace

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA EL INSTITUTO NACIONAL DE VÍAS INVIAS, MEDIANTE LA OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS.

(Zona horaria (UTC-05:00) Bogotá, Lima, Quito)
Fecha de presentación de ofertas 3/07/2026 5:00 PM - **Fecha de publicación** 19/06/2026 2:58 PM

PROVEEDORES
Interesados 16
963
Competidores 5

LÍNEA DE TIEMPO

Fecha de publicación de concurso	Plazo para solicitar aclaraciones	Presentación de ofertas
19/06/2026	26/06/2026	03/07/2026

LISTA DE OFERTAS Opciones

Referencia de oferta	Entidad	Presentada	Oferta
Oferta PS EM Invias SOC	PEAR SOLUTIONS S.A.S	3/07/2026 3:46 PM	9.343.089.830
Cotización INVIAS - Servicios Ciberseguridad	Syncrotech SAS	3/07/2026 3:31 PM	5.917.240.584,16
GAMMA INVIAS	GAMMA INGENIEROS SAS	3/07/2026 3:13 PM	6.030.164.838
SIP-SUBG-OTIC-033-2026_E&C	eyc ingenieros SAS	3/07/2026 2:09 PM	6.143.089.289,34
Infraestructura Virtual S.A.S. SIP-SUBG-OTIC-033-2026	INFRAESTRUCTURA VIRTUAL	30/06/2026 3:03 PM	5.272.168.860

OBSERVACIONES AL PLIEGO DE CONDICIONES Contestar

RE: Observaciones al proceso, Observaciones al Proceso SIP-SUBG-OTIC-033-2026, Observaciones
DANIELA GOMEZ AYALA
2/07/2026 5:02 PM

Observaciones
SIMS TECHNOLOGIES SAS
26/06/2026 4:40 PM

Observaciones al Proceso SIP-SUBG-OTIC-033-2026
INFRAESTRUCTURA VIRTUAL
26/06/2026 4:20 PM

Con base en el procedimiento anterior, y tal como se muestra a continuación, se recibieron CINCO (5) cotizaciones, provenientes de las siguientes empresas:

EMPRESAS	NIT
PEAR SOLUTIONS S.A. S	900.148.177-6
SYNCROTECH SAS	901.795.827-3
GAMMA INGENIEROS SAS	891.501.783-1
EYC INGENIEROS SAS	900.024.202-1
INFRAESTRUCTURA VIRTUAL	900.486.933-7

Verificación Históricos.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

Revisados los antecedentes contractuales del Instituto Nacional de Vías – INVIAS, no se evidenció la celebración de contratos con un objeto similar al del presente proceso, correspondiente con la prestación de servicios especializados de ciberseguridad para fortalecer las capacidades de prevención, detección, monitoreo, correlación, respuesta y gestión de incidentes de seguridad de la información que soportan el programa de seguridad de carreteras nacionales (PSCN) y su componente vías inteligentes ITS (VIITS), mediante la implementación y operación de un Centro De Operaciones De Seguridad (SOC) y sus servicios asociados.

No obstante, la Entidad ha adelantado procesos relacionados con seguridad informática y fortalecimiento de la infraestructura tecnológica. Sin embargo, dichos procesos difieren en su alcance, especificaciones técnicas y niveles de servicio, por lo que constituyen únicamente una referencia institucional y no una base comparable para la determinación del presupuesto oficial del presente proceso.

2. Cotizaciones

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 1			
				Infraestructura Virtual S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
1	**Monitoreo SOC - Operación continua 24×7×365** Servicio de monitoreo continuo de seguridad operado por analistas especializados en tres niveles (L1, L2 y L3) durante las 24 horas del día, los 7 días de la semana y los 365 días del año, (por un (1) año).	**Unidad**	1	$ 1.399.678.000	$ 265.938.820	$ 1.665.616.820	$ 1.665.616.820
2	**SIEM - Correlación y visibilidad centralizada**	**Unidad**	1	$ 305.680.000	$ 58.079.200	$ 363.759.200	$ 363.759.200

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 1			
				Infraestructura Virtual S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	Plataforma de gestión de información y eventos de seguridad con recolección, normalización y correlación de eventos de todas las fuentes de INVIAS, , (por un (1) año).						
3	**EDR / XDR - Detección y respuesta en endpoints** Solución de detección y respuesta en endpoints con correlación extendida entre red, correo electrónico y nube (Office 365 / Copilot), , (por un (1) año).	**Unidad**	1	$ 955.250.000	$ 181.497.500	$ 1.136.747.500	$ 1.136.747.500
4	**SOAR + Gestión de incidentes - Automatización de respuesta e IRP** Plataforma de orquestación y automatización de respuesta con módulo integrado de	**Unidad**	1	$ 159.208.000	$ 30.249.520	$ 189.457.520	$ 189.457.520

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 1			
				Infraestructura Virtual S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	gestión del ciclo de vida de incidentes (IRP), , (por un (1) año).						
5	**Threat Intelligence - Inteligencia de amenazas** Servicio de inteligencia de amenazas con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y ejercicios de búsqueda proactiva (threat hunting), , (por un (1) año).	**Unidad**	1	$ 178.313.000	$ 33.879.470	$ 212.192.470	$ 212.192.470
6	**Gestión de vulnerabilidades - Escaneo continuo y remediación** Escaneo continuo de activos en sede principal y 26 Direcciones Territoriales, , (por un (1) año).	**Unidad**	1	$ 76.420.000	$ 14.519.800	$ 90.939.800	$ 90.939.800
7	**Protección AntiDDoS -**	**Unidad**	1	$ 541.308.000	$ 102.848.520	$ 644.156.520	$ 644.156.520

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 1			
				Infraestructura Virtual S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	Mitigación volumétrica L3/L4 Servicio de mitigación de ataques de denegación de servicio distribuido (DDoS) en capas 3 y 4 sobre la infraestructura de red de INVIAS, (por un (1) año).						
8	**Renovación y ampliación WAF - 100 Mbps · 30 sitios · L7** Servicio de un firewall de aplicaciones web (WAF) en modalidad nube con capacidades de 100 Mbps / 30 sitios, (por un (1) año).	**Unidad**	1	$ 140.103.000	$ 26.619.570	$ 166.722.570	$ 166.722.570
9	**Control de Acceso a la Red (NAC) - Appliance Fisico** Solución de control y respuesta automatizada sobre la totalidad de dispositivos, usuarios y aplicaciones que se conectan a la	**Unidad**	1	$ 547.677.000	$ 104.058.630	$ 651.735.630	$ 651.735.630

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 1			
				Infraestructura Virtual S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	infraestructura de red institucional						
10	**Implementación y despliegue - Puesta en producción del SOC** Instalación, integración y puesta en producción de la totalidad de plataformas contratadas, (por un (1) año).	**Unidad**	1	$ 89.157.000	$ 16.939.830	$ 106.096.830	$ 106.096.830
11	**Bolsa de horas especializadas - 200 horas prepagadas · alto nivel** Doscientas (200) horas prepagadas de servicios especializados de alto nivel, reservadas para situaciones críticas que superan la operación rutinaria del SOC, (por un (1) año).	**Unidad Hora**	200	$ 188.000	$ 35.720	$ 223.720	$ 44.744.000
TOTAL						**$ 5.227.648.580**	**$5.272.168.860**

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 2			
				E & C INGENIEROS S.A.S			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
1	**Monitoreo SOC - Operación continua 24×7×365** Servicio de monitoreo continuo de seguridad operado por analistas especializados en tres niveles (L1, L2 y L3) durante las 24 horas del día, los 7 días de la semana y los 365 días del año, (por un (1) año).	Unidad	1	$ 111.741.916,71	$ 21.230.964,00	$ 132.972.880,71	$ 132.972.880,71
2	**SIEM - Correlación y visibilidad centralizada** Plataforma de gestión de información y eventos de seguridad con recolección, normalización y correlación de eventos de todas	Unidad	1	$ 148.886.338,31	$ 28.288.404,00	$ 177.174.742,31	$ 177.174.742,31

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 2			
				E & C INGENIEROS S.A.S			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	las fuentes de INVIAS, , (por un (1) año).						
3	**EDR / XDR - Detección y respuesta en endpoints** Solución de detección y respuesta en endpoints con correlación extendida entre red, correo electrónico y nube (Office 365 / Copilot), , (por un (1) año).	Unidad	1	$ 465.978.919,80	N/A	$ 465.978.919,80	$ 465.978.919,80
4	**SOAR + Gestión de incidentes - Automatización de respuesta e IRP** Plataforma de orquestación y automatización de respuesta con módulo integrado de gestión del ciclo de vida de incidentes (IRP), , (por un (1) año).	Unidad	1	$ 438.226.447,80	$ 83.263.025,00	$ 521.489.472,80	$ 521.489.472,80
5	**Threat Intelligence -**	Unidad	1	$ 348.946.342,16	$ 66.299.805,00	$ 415.246.147,16	$ 415.246.147,16

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 2			
				E & C INGENIEROS S.A.S			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	Inteligencia de amenazas Servicio de inteligencia de amenazas con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y ejercicios de búsqueda proactiva (threat hunting), , (por un (1) año).						
6	**Gestión de vulnerabilidades - Escaneo continuo y remediación** Escaneo continuo de activos en sede principal y 26 Direcciones Territoriales, , (por un (1) año).	**Unidad**	1	1.068.602.451,48	N/A	1.068.602.451,48	1.068.602.451,48
7	**Protección AntiDDoS - Mitigación**	**Unidad**	1	1.119.583.659,43	212.720.895,00	1.332.304.554,43	1.332.304.554,43

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 2			
				E & C INGENIEROS S.A.S			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	volumétrica L3/L4 Servicio de mitigación de ataques de denegación de servicio distribuido (DDoS) en capas 3 y 4 sobre la infraestructura de red de INVIAS, (por un (1) año).						
8	**Renovación y ampliación WAF - 100 Mbps · 30 sitios · L7** Servicio de un firewall de aplicaciones web (WAF) en modalidad nube con capacidades de 100 Mbps / 30 sitios, (por un (1) año).	**Unidad**	1	$ 545.696.770,73	N/A	$ 545.696.770,73	$ 545.696.770,73
9	**Control de Acceso a la Red (NAC) - Appliance Fisico** Solución de control y respuesta automatizada	**Unidad**	1	$ 333.071.664,01	$ 63.283.616,00	$ 396.355.280,01	$ 396.355.280,01

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 2			
				E & C INGENIEROS S.A.S			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	sobre la totalidad de dispositivos, usuarios y aplicaciones que se conectan a la infraestructura de red institucional						
10	**Implementación y despliegue - Puesta en producción del SOC** Instalación, integración y puesta en producción de la totalidad de plataformas contratadas, (por un (1) año).	**Unidad**	1	$ 740.511.330,23	$ 140.697.153,00	$ 881.208.483,23	$ 881.208.483,23
11	**Bolsa de horas especializadas - 200 horas prepagadas · alto nivel** Doscientas (200) horas prepagadas de servicios especializados de alto nivel, reservadas para situaciones críticas que superan la	**Unidad Hora**	200	$ 865.796,93	$ 164.501,00	$ 1.030.297,93	$ 206.059.586,67

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 2			
				E & C INGENIEROS S.A.S			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	operación rutinaria del SOC, (por un (1) año).						
TOTAL						**5.938.060.000,61**	**6.143.089.289,34**

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 3			
				GAMMA INGENIEROS S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
1	**Monitoreo SOC - Operación continua 24×7×365** Servicio de monitoreo continuo de seguridad operado por analistas especializados en tres niveles (L1, L2 y L3) durante las 24 horas del día, los 7 días de la semana y los 365 días del año, (por un (1) año).	**Unidad**	1	$ 109.687.837,00	$ 20.840.689,00	$ 130.528.526,36	$ 130.528.526,36

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 3			
				GAMMA INGENIEROS S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
2	**SIEM - Correlación y visibilidad centralizada** Plataforma de gestión de información y eventos de seguridad con recolección, normalización y correlación de eventos de todas las fuentes de INVIAS, , (por un (1) año).	**Unidad**	1	$ 146.149.457,09	$ 27.768.397,00	$ 173.917.854,09	$ 173.917.854,09
3	**EDR / XDR - Detección y respuesta en endpoints** Solución de detección y respuesta en endpoints con correlación extendida entre red, correo electrónico y nube (Office 365 / Copilot), , (por un (1) año).	**Unidad**	1	$ 457.413.130,84	N/A	$ 457.413.130,84	$ 457.413.130,84
4	**SOAR + Gestión de incidentes - Automatización**	**Unidad**	1	$ 430.170.814,57	$ 81.732.455,00	$ 511.903.269,57	$ 511.903.269,57

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 3			
				GAMMA INGENIEROS S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	de respuesta e IRP Plataforma de orquestación y automatización de respuesta con módulo integrado de gestión del ciclo de vida de incidentes (IRP), , (por un (1) año).						
5	**Threat Intelligence - Inteligencia de amenazas** Servicio de inteligencia de amenazas con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y ejercicios de búsqueda proactiva (threat hunting), , (por un (1) año).	**Unidad**	1	$ 342.531.887,34	$ 65.081.059,00	$ 407.612.946,34	$ 407.612.946,34

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 3			
				GAMMA INGENIEROS S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
6	**Gestión de vulnerabilidades - Escaneo continuo y remediación** Escaneo continuo de activos en sede principal y 26 Direcciones Territoriales, , (por un (1) año).	**Unidad**	1	$1.048.959.024,07	N/A	$ 1.048.959.024,07	$ 1.048.959.024,07
7	**Protección AntiDDoS - Mitigación volumétrica L3/L4** Servicio de mitigación de ataques de denegación de servicio distribuido (DDoS) en capas 3 y 4 sobre la infraestructura de red de INVIAS, (por un (1) año).	**Unidad**	1	$1.099.003.077,46	$ 208.810.585,00	$ 1.307.813.662,46	$ 1.307.813.662,46
8	**Renovación y ampliación WAF - 100 Mbps · 30 sitios · L7**	**Unidad**	1	$ 535.665.580,09	N/A	$ 535.665.580,09	$ 535.665.580,09

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 3			
				GAMMA INGENIEROS S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	Servicio de un firewall de aplicaciones web (WAF) en modalidad nube con capacidades de 100 Mbps / 30 sitios, (por un (1) año).						
9	**Control de Acceso a la Red (NAC) - Appliance Fisico** Solución de control y respuesta automatizada sobre la totalidad de dispositivos, usuarios y aplicaciones que se conectan a la infraestructura de red institucional	**Unidad**	1	$ 326.949.023,13	$ 62.120.314,00	$ 389.069.337,13	$ 389.069.337,13
10	**Implementación y despliegue - Puesta en producción del SOC** Instalación, integración y puesta en producción de la	**Unidad**	1	$ 726.898.989,60	$ 138.110.808,00	$ 865.009.797,60	$ 865.009.797,60

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 3			
				GAMMA INGENIEROS S.A.S.			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	totalidad de plataformas contratadas, (por un (1) año).						
11	**Bolsa de horas especializadas - 200 horas prepagadas · alto nivel** Doscientas (200) horas prepagadas de servicios especializados de alto nivel, reservadas para situaciones críticas que superan la operación rutinaria del SOC, (por un (1) año).	**Unidad Hora**	200	$ 849.881,55	$ 161.477,00	$ 1.011.358,55	$ 202.271.709,71
TOTAL						**5.828.904.487,09**	**6.030.164.838,25**

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 4			
				Pear Solutions SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
1	**Monitoreo SOC - Operación continua 24×7×365** Servicio de monitoreo continuo de seguridad operado por analistas especializados en tres niveles (L1, L2 y L3) durante las 24 horas del día, los 7 días de la semana y los 365 días del año, (por un (1) año).	**Unidad**	1	$2.032.680.000	$ 386.209.200	$ 2.418.889.200	$ 2.418.889.200
2	**SIEM - Correlación y visibilidad centralizada** Plataforma de gestión de información y eventos de seguridad con recolección, normalización y correlación de eventos de todas las fuentes de INVIAS, , (por un (1) año).	**Unidad**	1	$ 712.350.000	$ 135.346.500	$ 847.696.500	$ 847.696.500

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 4			
				Pear Solutions SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
3	**EDR / XDR - Detección y respuesta en endpoints** Solución de detección y respuesta en endpoints con correlación extendida entre red, correo electrónico y nube (Office 365 / Copilot), , (por un (1) año).	**Unidad**	1	$ 651.024.000	$ 123.694.560	$ 774.718.560	$ 774.718.560
4	**SOAR + Gestión de incidentes - Automatización de respuesta e IRP** Plataforma de orquestación y automatización de respuesta con módulo integrado de gestión del ciclo de vida de incidentes (IRP), , (por un (1) año).	**Unidad**	1	$ 892.183.000	$ 169.514.770	$ 1.061.697.770	$ 1.061.697.770
5	**Threat Intelligence - Inteligencia de amenazas**	**Unidad**	1	$ 468.551.000	$ 89.024.690	$ 557.575.690	$ 557.575.690

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 4			
				Pear Solutions SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	Servicio de inteligencia de amenazas con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y ejercicios de búsqueda proactiva (threat hunting), , (por un (1) año).						
6	**Gestión de vulnerabilidades - Escaneo continuo y remediación** Escaneo continuo de activos en sede principal y 26 Direcciones Territoriales, , (por un (1) año).	**Unidad**	1	$ 769.377.000	$ 146.181.630	$ 915.558.630	$ 915.558.630
7	**Protección AntiDDoS - Mitigación volumétrica L3/L4**	**Unidad**	1	$ 687.996.000	$ 130.719.240	$ 818.715.240	$ 818.715.240

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 4			
				Pear Solutions SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	Servicio de mitigación de ataques de denegación de servicio distribuido (DDoS) en capas 3 y 4 sobre la infraestructura de red de INVIAS, (por un (1) año).						
8	**Renovación y ampliación WAF - 100 Mbps · 30 sitios · L7** Servicio de un firewall de aplicaciones web (WAF) en modalidad nube con capacidades de 100 Mbps / 30 sitios, (por un (1) año).	**Unidad**	1	$ 482.240.000	$ 91.625.600	$ 573.865.600	$ 573.865.600
9	**Control de Acceso a la Red (NAC) - Appliance Fisico** Solución de control y respuesta automatizada sobre la totalidad de dispositivos,	**Unidad**	1	$ 739.274.000	$ 140.462.060	$ 879.736.060	$ 879.736.060

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 4			
				Pear Solutions SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	usuarios y aplicaciones que se conectan a la infraestructura de red institucional						
10	**Implementación y despliegue - Puesta en producción del SOC** Instalación, integración y puesta en producción de la totalidad de plataformas contratadas, (por un (1) año).	**Unidad**	1	$ 268.602.000	$ 51.034.380	$ 319.636.380	$ 319.636.380
11	**Bolsa de horas especializadas - 200 horas prepagadas · alto nivel** Doscientas (200) horas prepagadas de servicios especializados de alto nivel, reservadas para situaciones críticas que superan la operación	**Unidad Hora**	200	$ 735.295	$ 139.706	$ 875.001	$ 175.000.200

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 4			
				Pear Solutions SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	rutinaria del SOC, (por un (1) año).						
TOTAL						**9.168.964.631,00**	**9.343.089.830,00**

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 5			
				SYNCROTECH SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
1	**Monitoreo SOC - Operación continua 24×7×365** Servicio de monitoreo continuo de seguridad operado por analistas especializados en tres niveles (L1, L2 y L3) durante las 24 horas del día, los 7 días de la semana y los 365 días del año, (por un (1) año).	**Unidad**	1	107.633.758,00	$20.450.414,00	$ 128.084.172,01	$ 128.084.172,01
2	**SIEM - Correlación y**	**Unidad**	1	$ 143.412.576,00	$27.248.389,00	$ 170.660.964,87	$ 170.660.964,87

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 5			
				SYNCROTECH SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	visibilidad centralizada Plataforma de gestión de información y eventos de seguridad con recolección, normalización y correlación de eventos de todas las fuentes de INVIAS, , (por un (1) año).						
3	**EDR / XDR - Detección y respuesta en endpoints** Solución de detección y respuesta en endpoints con correlación extendida entre red, correo electrónico y nube (Office 365 / Copilot), , (por un (1) año).	**Unidad**	1	$ 448.847.342,00	N/A	$ 448.847.341,87	$ 448.847.341,87
4	**SOAR + Gestión de incidentes - Automatización de respuesta e IRP**	**Unidad**	1	$ 422.115.181,00	$80.201.884,00	$ 502.317.065,34	$ 502.317.065,34

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 5			
				SYNCROTECH SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	Plataforma de orquestación y automatización de respuesta con módulo integrado de gestión del ciclo de vida de incidentes (IRP), , (por un (1) año).						
5	**Threat Intelligence - Inteligencia de amenazas** Servicio de inteligencia de amenazas con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y ejercicios de búsqueda proactiva (threat hunting), , (por un (1) año).	**Unidad**	1	$ 336.117.433,00	$ 63.862.312,00	$ 399.979.744,52	$ 399.979.744,52
6	**Gestión de vulnerabilidades - Escaneo**	**Unidad**	1	$ 1.029.315.597,00	N/A	$ 1.029.315.596,65	$ 1.029.315.596,65

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 5			
				SYNCROTECH SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	continuo y remediación Escaneo continuo de activos en sede principal y 26 Direcciones Territoriales, , (por un (1) año).						
7	**Protección AntiDDoS - Mitigación volumétrica L3/L4** Servicio de mitigación de ataques de denegación de servicio distribuido (DDoS) en capas 3 y 4 sobre la infraestructura de red de INVIAS, (por un (1) año).	**Unidad**	1	$ 1.078.422.495,00	$ 204.900.274,00	$ 1.283.322.769,48	$ 1.283.322.769,48
8	**Renovación y ampliación WAF - 100 Mbps · 30 sitios · L7** Servicio de un firewall de aplicaciones web (WAF) en modalidad nube con capacidades	**Unidad**	1	$ 525.634.389,00	N/A	$ 525.634.389,45	$ 525.634.389,45

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 5			
				SYNCROTECH SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	de 100 Mbps / 30 sitios, (por un (1) año).						
9	**Control de Acceso a la Red (NAC) - Appliance Fisico** Solución de control y respuesta automatizada sobre la totalidad de dispositivos, usuarios y aplicaciones que se conectan a la infraestructura de red institucional	**Unidad**	1	$ 320.826.382,00	$ 60.957.013,00	$ 381.783.395,25	$ 381.783.395,25
10	**Implementación y despliegue - Puesta en producción del SOC** Instalación, integración y puesta en producción de la totalidad de plataformas contratadas, (por un (1) año).	**Unidad**	1	$ 713.286.649,00	$ 135.524.463,00	$ 848.811.111,98	$ 848.811.111,98
11	**Bolsa de horas especializadas - 200 horas**	**Unidad Hora**	200	$ 833.966,00	$ 158.454,00	$ 992.420,16	$ 198.484.032,75

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	COTIZACIÓN 5			
				SYNCROTECH SAS			
				VALOR UNITARIO SIN IVA	IVA	VALOR UNITARIO TOTAL INCLUIDO IVA	VALOR TOTAL INCLUIDO IVA
	prepagadas · alto nivel Doscientas (200) horas prepagadas de servicios especializados de alto nivel, reservadas para situaciones críticas que superan la operación rutinaria del SOC, (por un (1) año).						
TOTAL						**5.719.748.971, 58**	**5.917.240.584,16**

Nota: Los ítems 6. Gestión de vulnerabilidades – Escaneo continuo y remediación y 8. Renovación y ampliación WAF – 100 Mbps · 30 sitios, corresponden a servicios prestados en modalidad Software as a Service (SaaS) / Cloud, razón por la cual fueron cotizados por los proveedores sin incluir IVA. En consecuencia, para la determinación del precio de referencia la Entidad adoptó los valores efectivamente cotizados para dichos componentes, sin perjuicio del tratamiento tributario que resulte aplicable conforme a la normatividad vigente al momento de la ejecución del contrato.

Nota: Como resultado de la Solicitud de Información a Proveedores la Entidad recibió cinco (5) cotizaciones. Para la determinación del presupuesto oficial y la aplicación de las métricas estadísticas, se realizó un análisis comparativo de los valores ofertados para cada uno de los componentes del servicio.

Producto de dicho análisis, no se tuvieron en cuenta las cotizaciones presentadas por las empresas Infraestructura Virtual S.A.S. y Pear Solutions S.A.S., toda vez que sus propuestas económicas

presentaron diferencias significativas frente a las demás cotizaciones recibidas. En particular, se identificaron valores considerablemente inferiores y superiores al comportamiento observado en el mercado, generando una alta dispersión que afectaba la representatividad de los resultados estadísticos y podía distorsionar la determinación del precio de referencia.

En consecuencia, el análisis económico se efectuó con las cotizaciones presentadas por E & C Ingenieros S.A.S., Gamma Ingenieros S.A.S. y Syncrotech S.A.S., las cuales presentaron un comportamiento homogéneo y consistente entre sí, permitiendo establecer un presupuesto oficial acorde con las condiciones actuales del mercado y con los principios de economía, planeación y selección objetiva.

3. Análisis de las cotizaciones

Con fundamento en las orientaciones contenidas en la Guía para la Elaboración de Estudios del Sector (Versión 3 – 2025) de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, el comité económico estructurador definió una metodología estadística para la determinación del precio de referencia de cada uno de los ítems que conforman el presupuesto oficial, considerando el comportamiento de las cotizaciones obtenidas durante el estudio de mercado.

Una vez consolidadas y verificadas las cotizaciones recibidas, se efectuó el análisis estadístico mediante la aplicación del coeficiente de variación (CV) o coeficiente de dispersión relativa**,** entendido como una medida que permite establecer el grado de variabilidad de los precios ofertados respecto de su media y evaluar el nivel de homogeneidad del mercado.

Coeficiente de dispersión relativa (Coeficiente de Variación – CV): Es una medida estadística que expresa la variabilidad relativa de un conjunto de datos y permite determinar la consistencia de las cotizaciones recibidas.

Fórmula:

$$CV = \left(\frac{\text{Desviación estándar}}{\text{Media}} \right) \times 100$$

Un coeficiente de variación bajo indica que las cotizaciones presentan un comportamiento homogéneo y que los precios se encuentran concentrados alrededor de la media, mientras que un

coeficiente elevado evidencia una mayor dispersión entre las ofertas, la cual puede obedecer a diferencias en las condiciones técnicas, comerciales o económicas de los proveedores.

La aplicación del coeficiente de variación permite:

- Evaluar el grado de homogeneidad de las cotizaciones recibidas.
- Comparar la variabilidad entre los diferentes ítems objeto del estudio.
- Identificar valores atípicos que puedan afectar la representatividad de las medidas estadísticas.
- Seleccionar la medida de tendencia central más adecuada para determinar el precio de referencia de cada ítem.

En concordancia con la Guía para la Elaboración de Estudios del Sector de Colombia Compra Eficiente, el análisis económico no debe limitarse a seleccionar la cotización de menor valor, sino que debe sustentarse en criterios técnicos y estadísticos que permitan establecer un presupuesto oficial acorde con las condiciones reales del mercado.

Como resultado del análisis, se evidenció que, una vez depuradas las cotizaciones que presentaban comportamientos atípicos, los coeficientes de variación obtenidos para los diferentes ítems fueron inferiores al veinte por ciento (20 %), reflejando un comportamiento homogéneo de los precios ofertados y un adecuado nivel de consistencia entre las cotizaciones representativas del mercado.

En consecuencia, el comité económico estructurador adoptó EL PROMEDIO ARITMÉTICO como medida de tendencia central para la determinación del precio de referencia de cada uno de los ítems, por considerarse la metodología estadística que mejor representa el comportamiento del mercado y que permite establecer un presupuesto oficial objetivo, razonable y acorde con los principios de planeación, economía, selección objetiva y eficiencia en el gasto público.

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANT	MEDIDAS ESTADISTICAS					
				MENOR VALOR	MAYOR VALOR	PROMEDIO	MEDIA GEOMETRICA	DEVIACIÓN ESTANDAR	%DE DISPERSIÓN
				VALOR UNITARIO INCLUIDO IVA	VALOR UNITARIO INCLUIDO IVA	VALOR UNITARIO INCLUIDO IVA	VALOR UNITARIO INCLUIDO IVA	VALOR UNITARIO INCLUIDO IVA	
1	**Monitoreo SOC - Operación continua 24×7×365** Servicio de monitoreo continuo de seguridad operado por analistas especializados en tres niveles (L1, L2 y L3) durante las 24 horas del día, los 7 días de la semana y los 365 días del año, (por un (1) año).	Unidad	1	$ 128.084.172	$ 132.972.881	$ 130.528.526	$ 130.513.266	$ 1.995.807	2%
2	**SIEM - Correlación y visibilidad centralizada** Plataforma de gestión de información y eventos de seguridad co	Unidad	1	$ 170.660.965	$ 177.174.742	$ 173.917.854	$ 173.897.521	$ 2.659.239	2%
3	**EDR / XDR - Detección y respuesta en endpoints** Solución de detección y respuesta en endpoints con correlación extendida	Unidad	1	$ 448.847.342	$ 465.978.920	$ 457.413.131	$ 457.359.655	$ 6.993.937	2%
4	**SOAR + Gestión de incidentes - Automatización de respuesta e IRP** Plataforma de orquestación y automatización de respuesta con módulo integrado de gestión del ciclo de vida de incidentes (IRP), , (por un (1) año).	Unidad	1	$ 502.317.065	$ 521.489.473	$ 511.903.269	$ 511.843.423	$ 7.827.103	2%
5	**Threat Intelligence - Inteligencia de amenazas** Servicio de inteligencia de amenazas con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y ejercicios de búsqueda proactiva (threat hunting), , (por un (1) año).	Unidad	1	$ 399.979.745	$ 415.246.147	$ 407.612.946	$ 407.565.292	$ 6.232.483	2%
6	**Gestión de vulnerabilidades - Escaneo continuo y remediación** Escaneo continuo de activos en sede principal y 26 Direcciones Territoriales, , (por un (1) año).	Unidad	1	$ 1.029.315.597	$ 1.068.602.451	$ 1.048.959.024	$ 1.048.836.392	$ 16.038.791	2%
7	**Protección AntiDDoS - Mitigación volumétrica L3/L4** Servicio de mitigación de ataques de denegación de servicio distribuido (DDoS) en capas 3 y 4 sobre la infraestructura de red de INVIAS, (por un (1) año).	Unidad	1	$ 1.283.322.769	$ 1.332.304.554	$ 1.307.813.662	$ 1.307.660.767	$ 19.996.730	2%
8	**Renovación y ampliación WAF - 100 Mbps · 30 sitios · L7** Servicio de un firewall de aplicaciones web (WAF) en modalidad nube con capacidades de 100 Mbps / 30 sitios, (por un (1) año).	Unidad	1	$ 525.634.389	$ 545.696.771	$ 535.665.580	$ 535.602.956	$ 8.190.433	2%
9	**Control de Acceso a la Red (NAC) - Appliance Fisico** Solución de control y respuesta automatizada sobre la totalidad de dispositivos, usuarios y aplicaciones que se conectan a la infraestructura de red institucional	Unidad	1	$ 381.783.395	$ 396.355.280	$ 389.069.337	$ 389.023.852	$ 5.948.947	2%
10	**Implementación y despliegue - Puesta en producción del SOC** Instalación, integración y puesta en producción de la totalidad de plataformas contratadas, (por un (1) año).	Unidad	1	$ 848.811.112	$ 881.208.483	$ 865.009.798	$ 864.908.670	$ 13.226.171	2%
11	**Bolsa de horas especializadas - 200 horas prepagadas · alto nivel** Doscientas (200) horas prepagadas de servicios especializados de alto nivel, reservadas para situaciones críticas que superan la operación rutinaria del SOC, (por un (1) año).	Unidad Hora	200	$ 992.420	$ 1.030.298	$ 1.011.359	$ 1.011.241	$ 15.464	2%

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

4. Precio techo de referencias

De conformidad con la necesidad identificada y justificada en el Estudio Previo, el Instituto Nacional de Vías – INVIAS requiere contratar la prestación de servicios especializados de ciberseguridad para fortalecer las capacidades de prevención, detección, monitoreo, correlación, respuesta y gestión de incidentes de seguridad de la información que soportan el programa de seguridad de carreteras nacionales (PSCN) y su componente vías inteligentes ITS (VIITS), mediante la implementación y operación de un Centro De Operaciones De Seguridad (SOC) y sus servicios asociados.

Como resultado del estudio de mercado, la Entidad determinó el precio de referencia para cada uno de los componentes que conforman el presupuesto oficial, tomando como base las especificaciones técnicas definidas, las condiciones actuales del mercado y la metodología estadística adoptada para el análisis de las cotizaciones.

En consecuencia, los valores establecidos constituyen el PRECIO DE REFERENCIA del presente proceso de contratación y sirven de fundamento para la determinación del presupuesto oficial, conforme se presenta a continuación:

ITEM	DESCRIPCIÓN	UNIDAD DE MEDIDA	CANT	PRECIO DE REFERENCIA		
				MÉTRICA	VALOR UNITARIO INCLUIDO IVA (si aplca)	VALOR TOTAL INCLUIDO IVA (si aplca)
1	**Monitoreo SOC - Operación continua 24×7×365** Servicio de monitoreo continuo de seguridad operado por analistas especializados en tres niveles (L1, L2 y L3) durante las 24 horas del día, los 7 días de la semana y los 365 días del año, (por un (1) año).	Unidad	1	PROMEDIO	$ 130.528.526,00	$ 130.528.526,00
2	**SIEM - Correlación y visibilidad centralizada** Plataforma de gestión de información y eventos de seguridad con recolección, normalización y correlación de eventos de todas las fuentes de INVIAS, , (por un (1) año).	Unidad	1	PROMEDIO	$ 173.917.854,00	$ 173.917.854,00

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

ITEM	DESCRIPCIÓN	UNIDAD DE MEDIDA	CANT	PRECIO DE REFERENCIA		
				MÉTRICA	VALOR UNITARIO INCLUIDO IVA (si aplca)	VALOR TOTAL INCLUIDO IVA (si aplca)
3	**EDR / XDR - Detección y respuesta en endpoints** Solución de detección y respuesta en endpoints con correlación extendida entre red, correo electrónico y nube (Office 365 / Copilot), , (por un (1) año).	Unidad	1	PROMEDIO	$ 457.413.131,00	$ 457.413.131,00
4	**SOAR + Gestión de incidentes - Automatización de respuesta e IRP** Plataforma de orquestación y automatización de respuesta con módulo integrado de gestión del ciclo de vida de incidentes (IRP), , (por un (1) año).	Unidad	1	PROMEDIO	$ 511.903.269,00	$ 511.903.269,00
5	**Threat Intelligence - Inteligencia de amenazas** Servicio de inteligencia de amenazas con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y ejercicios de búsqueda proactiva (threat hunting), , (por un (1) año).	Unidad	1	PROMEDIO	$ 407.612.946,00	$ 407.612.946,00
6	**Gestión de vulnerabilidades - Escaneo continuo y remediación** Escaneo continuo de activos en sede principal y 26 Direcciones Territoriales, , (por un (1) año).	Unidad	1	PROMEDIO	$ 1.048.959.024,00	$ 1.048.959.024,00
7	**Protección AntiDDoS - Mitigación volumétrica L3/L4** Servicio de mitigación de ataques de denegación de servicio distribuido (DDoS) en capas 3 y 4 sobre la infraestructura de red de INVIAS, (por un (1) año).	Unidad	1	PROMEDIO	$ 1.307.813.662,00	$ 1.307.813.662,00

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

ITEM	DESCRIPCIÓN	UNIDAD DE MEDIDA	CANT	PRECIO DE REFERENCIA		
				MÉTRICA	VALOR UNITARIO INCLUIDO IVA (si aplca)	VALOR TOTAL INCLUIDO IVA (si aplca)
8	**Renovación y ampliación WAF - 100 Mbps · 30 sitios · L7** Servicio de un firewall de aplicaciones web (WAF) en modalidad nube con capacidades de 100 Mbps / 30 sitios, (por un (1) año).	Unidad	1	PROMEDIO	$ 535.665.580,00	$ 535.665.580,00
9	**Control de Acceso a la Red (NAC) - Appliance Fisico** Solución de control y respuesta automatizada sobre la totalidad de dispositivos, usuarios y aplicaciones que se conectan a la infraestructura de red institucional	Unidad	1	PROMEDIO	$ 389.069.337,00	$ 389.069.337,00
10	**Implementación y despliegue - Puesta en producción del SOC** Instalación, integración y puesta en producción de la totalidad de plataformas contratadas, (por un (1) año).	Unidad	1	PROMEDIO	$ 865.009.798,00	$ 865.009.798,00
11	**Bolsa de horas especializadas - 200 horas prepagadas · alto nivel** Doscientas (200) horas prepagadas de servicios especializados de alto nivel, reservadas para situaciones críticas que superan la operación rutinaria del SOC, (por un (1) año).	Unidad Hora	200	PROMEDIO	$ 1.011.359,00	$ 202.271.800,00
TOTAL					**$ 5.828.904.486,00**	**$ 6.030.164.927,00**

El valor total del presupuesto oficial asciende a la suma de **SEIS MIL TREINTA MILLONES CIENTO SESENTA Y CUATRO MIL NOVECIENTOS VEINTISIETE PESOS M/CTE**. (**$ 6.030.164.927,00)** incluido IVA (en los ítems que apliquen o correspondan) y todos los costos directos e indirectos necesarios para la ejecución del contrato, así como los impuestos, tasas, contribuciones y demás gravámenes a que haya lugar.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

NOTA 1: El proponente no deberá superar el PRECIO DE REFERENCIA (PRECIO TECHO) unitario asignado, so pena de ser rechazado en su oferta.

NOTA 2: El proponente deberá OFERTAR las cantidades exigidas de los bienes y/o servicios establecidos en la Plataforma del SECOP II en la pregunta lista de precios, so pena de causal de rechazo de la propuesta.

NOTA 3: El proponente no deberá presentar su oferta con moneda diferente a la establecida para el presente proceso, so pena de ser rechazada su oferta.

NOTA 4: Los precios ofertados deberán incluir todos los costos directos e indirectos como impuestos, tasas, sobretasas y demás erogaciones relacionadas como administración, variaciones monetarias de orden cambiario y todo lo correspondiente al área comercial del proponente, por lo tanto, EL INSTITUTO NACIONAL DE INVIAS no se hará responsable por reclamaciones que tengan como causa los elementos antes descritos.

NOTA 5:

5. ANÁLISIS NORMATIVIDAD VIGENTE APLICABLE AL PROCESO

LEY DE EMPRENDIMIENTO - Finalidad

La Ley 2069 de 2020, reglamentada mediante el Decreto No. 1860 de 2021, tiene por objeto establecer un marco regulatorio que propicie el emprendimiento y el crecimiento, consolidación y sostenibilidad de las empresas, con el fin de aumentar el bienestar social y generar equidad, de igual forma la citada Ley tiene entre otros los siguientes objetivos: Reducir las cargas para emprendedores y generar gradualidad para empresas de menor escala. Ampliar las oportunidades de acceso a mercados, a través de **compras** públicas, diversificar y ampliar esquemas de financiamiento para todo tipo de emprendimiento.

Por otra parte, la importancia del emprendimiento en Colombia radica en la capacidad que tienen las PYMES para generar empleo y ser un motor para la economía nacional, prueba de ello es que el 80% del empleo nuevo en Colombia es generado por el 10% de los nuevos proyectos de emprendimiento, en muchos de los casos PYMES.

De conformidad con las previsiones contenidas en los artículos 30, 31, 32, 33, 34, 35 y 36 de la Ley 2069 de 2020, se generaron incentivos para las MIPYMES con el propósito de incrementar la participación de dichas empresas en las compras públicas permitiendo la inclusión de criterios diferenciales y de ponderación en las distintas modalidades de contratación.

En este sentido mediante el Decreto No. 1860 de 2021 “Por el cual se modifica y adiciona el Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, con el fin reglamentar los artículos 30, 31, 32, 34 y 35 de la Ley 2069 de 2020, en lo relativo al sistema de compras públicas y se dictan otras disposiciones", se incluyeron disposiciones particulares en el procedimiento de selección de mínima cuantía referidas a la contratación con Mipymes y grandes almacenes; se definieron y fijaron los criterios diferenciales para Mipymes y emprendimientos y empresas de mujeres; se profirió la reglamentación para las convocatorias limitadas a Mipymes, la ejecución de contratos estatales por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y, sujetos de especial protección constitucional; así como la acreditación de los factores de desempate previstos en la Ley de Emprendimiento.

Criterios diferenciales para Mipymes en el sistema de compra pública

El artículo 31 de la Ley 2069 de 2020 introdujo criterios diferenciales para el acceso de las Mipymes al sistema de compras y contratación pública. Para estos efectos, el inciso primero señala que «Las Entidades Estatales de acuerdo con el análisis de Sector podrán incluir, en los Documentos del Proceso, requisitos diferenciales y puntajes adicionales, en función del tamaño empresarial para la promoción del acceso de las MIPYMES al mercado de Compras Públicas», estos criterios diferenciales aplican para todos los procesos de selección.

En este sentido, en el Decreto 1860 del 24 de diciembre de 2021 se dispone que las entidades estatales deben fijar los requisitos habilitantes con alguno o algunos de los siguientes criterios diferenciales “que promuevan y faciliten la participación en los procedimientos de selección” a las MIPYMES (artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015), de manera que en alguno o algunos de los criterios que se indican, se establezcan condiciones más exigentes para aquellos participantes en el procedimiento de selección que no tengan la calidad de MIPYME:

1. Tiempo de Experiencia: para quienes no son MIPYME se podrá establecer un tiempo de experiencia mayor respecto del requerido para quienes son MIPYME.
2. Número de contratos para la acreditación de la experiencia: exigir una mayor cantidad de contratos para acreditar la experiencia a quienes no son MIPYME, de manera que las MIPYMES puedan demostrar la experiencia habilitante con menor número de contratos.
3. Índices de capacidad financiera: formular estos índices de manera más exigente para quienes no tienen la calidad de MIPYME.
4. Índices de capacidad organizacional: exigir un mayor índice de capacidad organizacional para los participantes que no son MIPYME.
5. Valor de la garantía de seriedad de la oferta: exigir un mayor valor asegurado para quienes no son MIPYME.

DINÁMICA DE CREACIÓN DE EMPRESAS EN COLOMBIA – 2026

De acuerdo con el DANE, durante el primer trimestre de 2026 la economía colombiana mostró un crecimiento moderado, con un aumento del PIB del 2,2% frente al mismo periodo de 2025.
Este dinamismo se combina con una inflación controlada: en junio de 2025 la variación anual del IPC fue del 4,8%, dos puntos y medio menos que el 7,2% registrado un año antes. El Banco de la República, atendiendo a este entorno, en mayo redujo la tasa de interés de política, del 9,5% en que había sido establecida en diciembre de 2024, a 9,25%; de esta forma, se confirma la expectativa de la estabilización en el comportamiento de los precios de la economía, con la convergencia de la inflación a su rango meta.

En el mercado laboral, en mayo de 2025 la tasa de desempleo nacional cayó a 9,0%, 1,3 puntos porcentuales menos que en mayo de 2024 (10,3%), y la tasa de ocupación subió a 58,2% (frente al 57,5% del año anterior). Aun así, aun se presentan oportunidades en el comportamiento de la economía, las ventas externas del país presentaron, en mayo, una caída de 2,1% en relación con el mismo mes del año pasado, lo cual, a pesar de también presentarse una caída en el nivel de importaciones, concluye en un mayor déficit en la balanza comercial colombiana.

En este contexto, la Confederación Colombiana de Cámaras de Comercio -Confecámaras- presenta el informe de dinámica de creación de empresas para el primer semestre de 2025, analizando el comportamiento de la constitución de sociedades y matrícula de personas naturales. Según los registros del RUES de las cámaras de comercio del país, en la primera mitad de 2025 se crearon 173.907 nuevas empresas, un 1,9% más que en 2024 cuando se establecieron 170.741 compañías en el mismo periodo. Del total de nuevas empresas, el 74% fueron creadas por personas naturales y el 26%, por sociedades. En comparación con 2024, las matrículas de nuevas de personas naturales aumentaron un 2,5%, mientras que el de las sociedades disminuyeron en 0,1%.



Fuente: RUES – Registro Único Empresarial y Social.

En 2025, la creación de empresas alcanzó su mayor nivel en marzo y el más bajo en abril. Se resalta que, al cierre del semestre, se evidenció un repunte en la creación de empresas en comparación con el mismo periodo de 2024.



Fuente: RUES – Registro Único Empresarial y Social.

Creación de empresas por tamaño

Al comparar la evolución de la creación de empresas entre el primer semestre de 2024 y 2025, según el tamaño definido por el valor de sus activos, se evidencia un aumento del 1,9% en la creación de microempresas, que además explican en su totalidad el crecimiento neto en el periodo. En contraste, se observa una disminución del 12,6% en la creación de pequeñas empresas, del 15% en las medianas y del 62% en las empresas grandes. Estos resultados reflejan que el dinamismo empresarial en el primer semestre de 2025 se concentró en el segmento de las microempresas, que siguen representando la principal vía de emprendimiento en el país.

Creación de empresas por tamaño

Tamaño	2024-1	2025-1	Variación %	Contribución
Microempresa	170.213	173.450	1,9%	1,9%
Pequeña	500	437	-12,6%	0,0%
Mediana	20	17	-15,0%	0,0%
Grande	8	3	-62,5%	0,0%
Total	170.741	173.907	1,9%	1,9%

Fuente: RUES – Registro Único Empresarial y Social.

En cuanto a las empresas constituidas por personas naturales, durante el primer semestre de 2025 se crearon 129.048, lo que representa un aumento del 2,5% frente a las 125.849 registradas en el mismo periodo de 2024. Este incremento se debió principalmente al crecimiento del 2,6% en las microempresas, que pasaron de 125.760 a 129.009. La constitución de empresas pequeñas pasó de 79 a 36 en el primer semestre de 2025, las empresas medianas pasaron de 9 a 3 y no se creó ninguna grande.

Nuevas empresas de personas naturales por tamaño

Tamaño	2024-1	2025-1	Variación %	Contribución
Microempresa	125.760	129.009	2,6%	2,58%
Pequeña	79	36	-54,4%	-0,03%
Mediana	9	3	-66,7%	0,00%
Grande	1	0	-100,0%	0,00%
Total	125.849	129.048	2,50%	2,50%

Fuente: RUES – Registro Único Empresarial y Social.

Creación de empresas por sectores económicos

Durante el primer semestre de 2025, se observó un aumento en la creación de empresas en los sectores de comercio, servicios y agricultura. El sector comercio fue el principal impulsor, con un

crecimiento del 3,3% en el número de nuevas empresas frente al mismo periodo de 2024, seguido por el sector servicios, que registró una variación positiva del 1,9%. En contraste, los sectores de construcción e industria presentaron una disminución en la creación de empresas, con caídas del 8,2% y 3,2%, respectivamente, en comparación con el primer semestre del año anterior.

Empresas creadas por sector económico

Sector económico	2024-1	2025-1	Variación %	Contribución
Comercio	64.500	66.626	3,3%	1,2%
Servicios	73.857	75.249	1,9%	0,8%
Agricultura	2.932	3.401	16,0%	0,3%
Resto	4.468	4.792	7,3%	0,2%
Extracción	461	472	2,4%	0,0%
Industria	17.037	16.498	-3,2%	-0,3%
Construcción	7.486	6.869	-8,2%	-0,4%
Total	**170.741**	**173.907**	**1,9%**	**1,9%**

Fuente: RUES – Registro Único Empresarial y Social.

Nota: El sector resto incluye administración pública y defensa, educación, actividades de los hogares, actividades de atención a la salud humana y actividades no clasificadas.

Durante el primer semestre de 2025, el subsector de comercio al por mayor y al por menor se mantuvo como el principal motor de la creación de empresas, con un total de 66.626 nuevas unidades, lo que representa un crecimiento del 3,3% frente al mismo periodo de 2024 y una contribución de 1,3 puntos porcentuales al crecimiento total. En el sector servicios, destacaron por su dinamismo los subsectores de otras actividades de servicios y el de alojamiento y servicios de comida. El primero registró un incremento del 8,8%, al pasar de 8.571 a 9.324 empresas, mientras que el segundo creció un 2,2%, con un aumento de 28.946 a 29.577 nuevas empresas. Las contribuciones relativas al crecimiento total fueron de 0,5 y 0,4 puntos porcentuales, respectivamente.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

Empresas creadas por subsectores económicos

Subsector económico	2024-1	2025-1	Variación %	Contribución
Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas	64.500	66.626	3,3%	1,3%
Otras actividades de servicios	8.571	9.324	8,8%	0,5%
Alojamiento y servicios de comida	28.946	29.577	2,2%	0,4%
Agricultura, ganadería, caza, silvicultura y pesca	2.932	3.401	16,0%	0,3%
Actividades inmobiliarias	3.161	3.445	9,0%	0,2%
Actividades de atención de la salud humana y de asistencia social	2.687	2.887	7,4%	0,1%
Educación	1.567	1.630	4,0%	0,0%
Información y comunicaciones	3.456	3.490	1,0%	0,0%
Actividades financieras y de seguros	1.465	1.476	0,8%	0,0%
Explotación de minas y canteras	461	472	2,4%	0,0%
Suministro de electricidad, gas, vapor y aire acondicionado	215	225	4,7%	0,0%
Actividades de los hogares	24	22	-8,3%	0,0%
Administración pública y defensa; planes de seguridad social de afiliación obligatoria	66	54	-18,2%	0,0%
Distribución de agua; evacuación y tratamiento de aguas residuales, gestión de desechos y actividades de saneamiento ambiental	877	857	-2,3%	0,0%
Actividades profesionales, científicas y técnicas	10.931	10.907	-0,2%	0,0%
Actividades artísticas, de entretenimiento y recreación	3.645	3.600	-1,2%	0,0%
Transporte y almacenamiento	4.576	4.476	-2,2%	-0,1%
Actividades de servicios administrativos y de apoyo	8.014	7.872	-1,8%	-0,1%
Industrias manufactureras	17.037	16.498	-3,2%	-0,3%
Construcción	7.486	6.869	-8,2%	-0,4%
No clasificado	124	199	60,5%	0,0%
Actividades de organizaciones y entidades extraterritoriales	0	0	0,0%	0,0%
Total	**170.741**	**173.907**	**1,9%**	**1,9%**

Fuente: RUES – Registro Único Empresarial y Social.

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

En contraparte, el sector construcción presentó la mayor caída, con una reducción del 8.2% al pasar de 7.486 a 6.869 nuevas empresas, lo que se tradujo en una contribución negativa de -0.4 puntos porcentuales al crecimiento total. Le siguió el subsector de industrias manufactureras que paso de 17.037 a 16.489 unidades, con una variación de -3.2% y una contribución de -0.3 puntos porcentuales. Por su parte las actividades de servicios administrativo y de apoyo disminuyeron u 1,8% con 7.872 empresas creadas frente a 8.014 e 2024, mientras que el subsector transporte y almacenamiento redujo su número de nuevas empresas en un 2,2% pasando de 4.576 a 4.476 ambos subsectores aportaron negativamente con -0.1 porcentuales cada uno.

Dado que el subsector de comercio al mayor y al por menor es el que más contribuyó en la creación de empresas, a continuación, se destacan las actividades económicas dentro del subsector que contribuyeron en mayor medida.



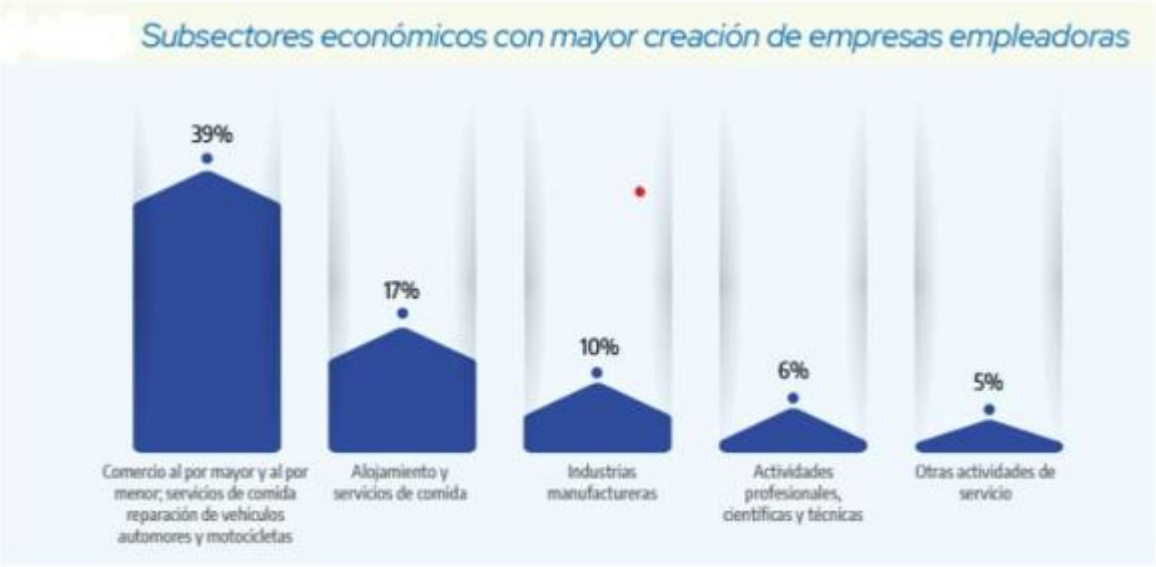
Por otro lado, el subsector de otras actividades de servicio, las siguientes actividades económicas contribuyeron de mayor manera en la variación registrada:



El subsector construcción presentó la mayor caída de la creación de empresas, principalmente en actividades como: construcción de otras obras de ingeniería civil (-13,7%); construcción de edificaciones residenciales (-9.3%); e instalaciones eléctricas (10.8%).

Creación de empresas y generación de empleo

De acuerdo con el RUES, el 43.8% de las empres nuevas crearon al menos un empleo; de estas el 39% pertenecen al sector comercio al por mayor y al por menor, 17% al subsector de alojamiento y servicio de comida, 10% al subsector de industrias manufactureras, 6% al subsector de actividades profesionales, científicas y técnicas y 5% al subsector de otras actividades de servicio.



Acceda al informe completo: Confecámaras. DINÁMICA DE CREACIÓN DE EMPRESAS EN COLOMBIA – 2025 dinamica-de-creacion-de-empresas-en-colombia-op2-web.pdf

Variación anual de las principales variables - Resultados generales I trimestre de 2026 Total nacional - Encuesta de Micronegocios (EMICRON)

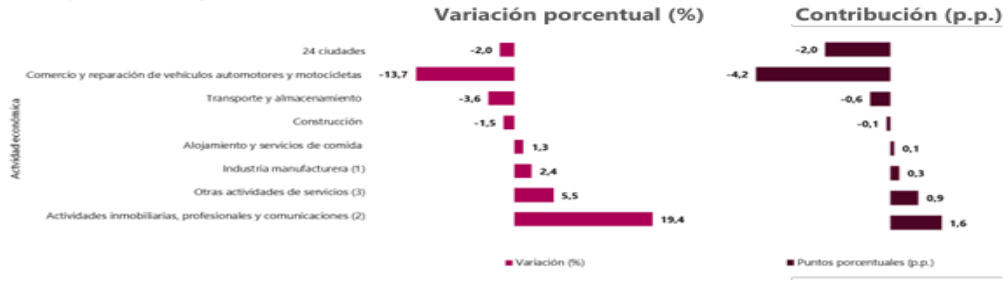
En el primer trimestre de 2026, la cantidad de micronegocios disminuyó 2,0% en comparación con el mismo periodo de 2025. Respecto al personal ocupado por estas unidades económicas aumentó 1,0%. De la misma manera, los ingresos de los micronegocios aumentaron 9,8% en este mismo intervalo de tiempo. (Cuadros C1 – C3, Anexo I Trimestre).

Variación anual de la cantidad de micronegocios según actividad económica (porcentaje)

Las actividades económicas que tuvieron mayor contribución positiva a la variación total de la cantidad de micronegocios en el tercer trimestre de 2025 fueron Transporte y almacenamiento (2,2 p.p.); Industria manufacturera (1,0 p.p.) y Comercio y reparación de vehículos y motocicletas (0,9 p.p.). Por su parte, Actividades inmobiliarias, profesionales y comunicaciones (-1,6 p.p.) y Otras actividades de servicios (-0,6 p.p.) contribuyeron negativamente a la variación total de la cantidad de micronegocios.

Variación anual del personal ocupado en los micronegocios según actividad económica (porcentaje)

Gráfico 2. Variación anual de la cantidad de micronegocios según actividad económica (porcentaje)
24 Ciudades[1]
I Trimestre (2026P/2025)

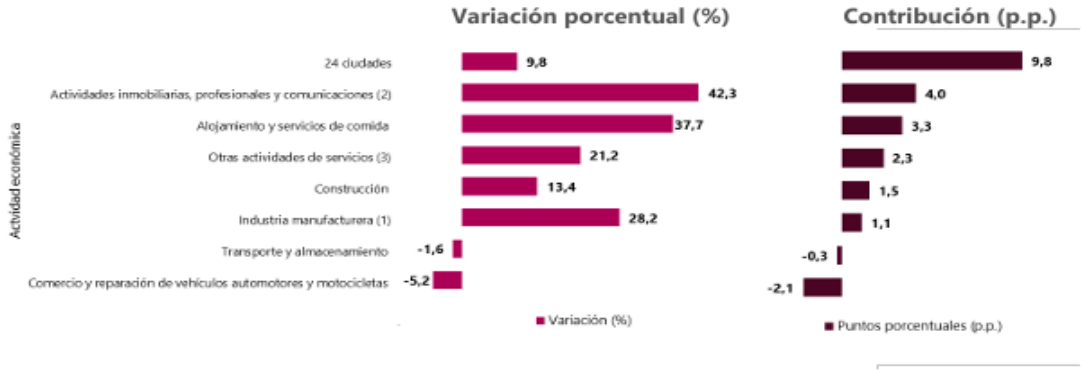


Fuente: DANE, EMICRON

Con respecto al personal ocupado, las actividades económicas que tuvieron mayor contribución positiva a la variación total del personal ocupado en el primer trimestre de 2026 fueron: Actividades inmobiliarias, profesionales y comunicaciones (2,4 p.p.); Alojamiento y servicios de comida (1,6 p.p.); Otras actividades de servicios (1,1 p.p.) y Construcción (0,3 p.p.). Por su parte, y Comercio y reparación de vehículos y motocicletas (-4,3 p.p.) y Transporte y almacenamiento (-0,3 p.p.) contribuyeron negativamente a la variación anual del personal ocupado en los micronegocios.

Variación anual de los ingresos nominales de los micronegocios según actividad económica (porcentaje)

Gráfico 4. Variación anual de los ingresos nominales de los micronegocios según actividad económica (porcentaje)
24 Ciudades[1]
I Trimestre (2026P/2025)



Fuente: DANE, EMICRON.

Las actividades de Actividades inmobiliarias, profesionales y comunicaciones (4,0 p.p.); Alojamiento y servicios de comida (3,3 p.p.) y Otras actividades de servicios (2,3 p.p.) contribuyeron, en mayor medida, positivamente a la variación anual de los ingresos nominales de los micronegocios en el

primer trimestre de 2026. Por el contrario, las ramas de Comercio y reparación de vehículos automotores y motocicletas (-2,1 p.p.) y Transporte y almacenamiento (0,3 p.p.) contribuyeron de manera negativa a la variación anual de los ingresos nominales de los micronegocios.

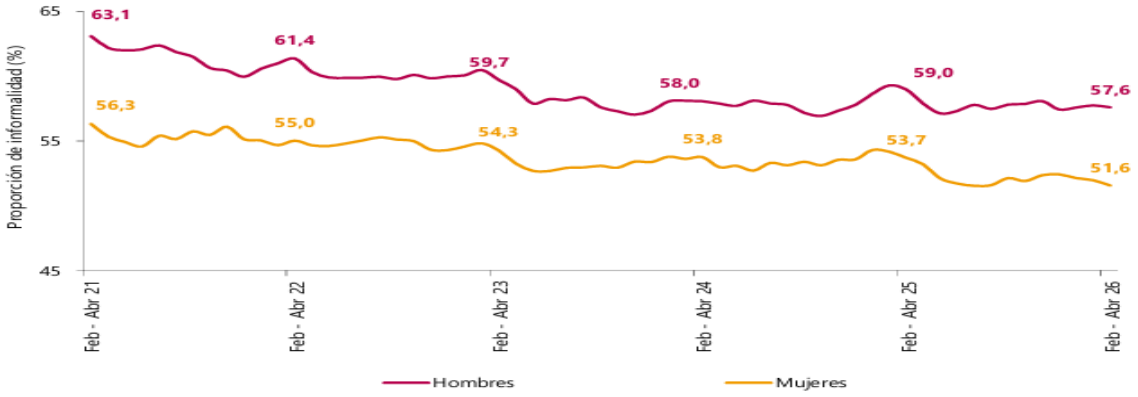
Medición del empleo informal - Informalidad total nacional, 13 y 23 ciudades y áreas metropolitanas

Para el total nacional, en el trimestre móvil febrero - abril 2026 la proporción de personas ocupadas informales fue 55,1%, lo que representó una disminución de 1,7 puntos porcentuales respecto al mismo trimestre del año anterior (56,8%). En las 13 ciudades y áreas metropolitanas esta proporción fue 41,2%, lo que significó una disminución de 1,4 puntos porcentuales frente al trimestre móvil febrero - abril 2025 (42,5%). Por su parte, en las 23 ciudades y áreas metropolitanas la proporción de población ocupada informal fue 42,4%, lo que representó una disminución de 1,6 puntos porcentuales respecto al mismo periodo del año anterior (43,9%). Para los centros poblados y rural disperso la proporción de población ocupada informal fue 83,0% en el trimestre móvil febrero - abril 2026.

Informalidad según sexo en el total nacional

Para el total nacional, la proporción de hombres ocupados informales en el trimestre móvil febrero - abril 2026 fue 57,6%, mientras que para las mujeres ocupadas informales se ubicó en 51,6%, lo que significó una diferencia de 6,0 puntos porcentuales.

Gráfico 3. Proporción de población ocupada informal según sexo
Total nacional
Trimestre móvil febrero - abril (2021-2026)



Fuente: DANE, GEIH.
Nota: datos expandidos con proyecciones de población, elaboradas con base en los resultados CNPV 2018.

Informalidad por ciudades

Para el periodo de análisis, de las 23 ciudades y áreas metropolitanas, aquellas que presentaron mayor proporción de informalidad fueron: Sincelejo (66,8%), Cúcuta A.M. (62,6%) y Riohacha (61,2%), mientras que las ciudades con menor proporción de informalidad fueron: Bogotá D.C. (34,3%), Tunja (34,8%) y Manizales A.M. (35,0%).

Gráfico 5. Proporción de la población ocupada informal según ciudades
Total nacional, 13 y 23 ciudades y áreas metropolitanas
Trimestre móvil febrero - abril 2026



Fuente: DANE, GEIH.

MEDICIÓN DEL EMPLEO INFORMAL SEGÚN TAMAÑO DE EMPRESA

En el total nacional, para el trimestre móvil febrero - abril 2026 el 84,6% de la población ocupada que trabajaba en microempresas era informal, mientras que la población ocupada informal en empresas pequeñas fue 21,3% Por su parte, en empresas medianas y grandes la proporción de población ocupada informal fue 4,6% y 2,2%, respectivamente.

Tabla 1. Proporción de población ocupada informal según tamaño de empresa donde trabaja
Total nacional
Trimestre móvil febrero - abril (2025-2026)

Tamaño de empresa	Febrero - abril 2025	Febrero - abril 2026	Diferencia en p.p.
Microempresa	85,4	**84,6**	-0,8
Empresa pequeña	20,1	**21,3**	1,2
Empresa mediana	5,7	**4,6**	-1,1
Empresa grande	2,6	**2,2**	-0,5

Fuente: DANE, GEIH.

Decreto 287 de 2026 Por el cual se modifican los artículos 2.2.1.2.4.2.6., 2.2.1.2.4.2.7. y 2.2.1.2.4.2.8. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación

El Decreto 287 de 2026 tiene por objeto modificar el Decreto 1082 de 2015 con el fin de reglamentar de manera integral el Sistema de Preferencias en favor de las personas con discapacidad en el marco de la contratación estatal, estableciendo un conjunto de medidas afirmativas obligatorias que deben ser aplicadas en todas las fases del proceso contractual planeación, selección, adjudicación y ejecución—, con el propósito de promover su participación efectiva como proponentes, contratistas o integrantes de la cadena de valor, eliminar barreras de acceso y garantizar condiciones reales de igualdad en consonancia con lo dispuesto en la Ley 1618 de 2013.
Decreto 287 de 2026 Planeación Nacional - Gestor Normativo - Función Pública

DESCRIPCIÓN DEL OBJETO A CONTRATAR, ESPECIFICACIONES E IDENTIFICACIÓN DEL CONTRATO CELEBRAR.

La Ley 1150 de 2007 establece que *"el uso de acuerdos marco de precios se hará obligatorio para las entidades de la Rama Ejecutiva del Poder Público en el Orden Nacional, sometidas al Estatuto General de Contratación de la Administración Pública"*.

Por lo tanto, cuando una entidad estatal del orden nacional de la Rama Ejecutiva, regida por dicha ley, necesite adquirir un bien con características técnicas uniformes, debe verificar si existe un Acuerdo Marco de Precios para realizar la compra de dicho bien o servicio bajo este esquema.

Sin embargo, tras revisar los Instrumentos de Agregación de Demanda vigentes en la plataforma de la Tienda Virtual del Estado Colombiano y los productos disponibles a través de Grandes Superficies, se ha determinado que actualmente no existe un acuerdo que cubra el objeto y las especificaciones técnicas requeridas para esta contratación.

En consecuencia, la Entidad, en razón a la cuantía y al objeto del contrato, llevará a cabo un proceso de contratación para el año 2026. Dadas las características propias de la contratación y conforme al Estatuto General de la Contratación de la Administración Pública, se planea realizar dicho proceso mediante SELECCIÓN ABREVIADA POR SUBASTA INVERSA.

Esta modalidad se justifica porque los bienes y servicios a adquirir poseen características técnicas uniformes y de común utilización, tal como se establece en el literal (a) del numeral 2 del artículo 2° de la Ley 1150 de 2007 y en el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015. Dichos bienes y servicios:

Cumplen con las mismas especificaciones técnicas, definidas objetivamente en términos de desempeño y calidad.

Son de uso generalizado, disponibles en el mercado y ofrecidos por múltiples proveedores.

Solo se diferencian en su precio, que se constituye en el único aspecto de evaluación en el proceso.

Por lo anterior, la Subasta Inversa permite seleccionar al proveedor que ofrezca la mejor cotización, garantizando eficiencia, transparencia y ahorro en la contratación de bienes y servicios de características técnicas uniformes.

5.1 OBJETO DEL CONTRATO

El objeto del contrato que resulte del proceso de selección respectivo será:

"*CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS*."

El objeto fue precisado con respecto al publicado en la solicitud de cotizaciones SIP-SUBG-OTIC-033-2026, con el fin de reflejar que los servicios protegen la infraestructura del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS; esta precisión no modifica el alcance técnico ni las especificaciones consultadas al mercado.

ALCANCE AL OBJETO

El Instituto Nacional de Vías — INVIAS opera una infraestructura tecnológica de naturaleza híbrida, compuesta por un datacenter propio, servicios y cargas de trabajo desplegados en la plataforma de nube Microsoft Azure, y una red de sedes departamentales interconectadas a nivel nacional. Esta arquitectura es protegida perimetralmente por treinta y uno (31) dispositivos de seguridad activos, distribuidos entre la sede principal en Bogotá D.C. y las sedes regionales, y soporta el funcionamiento de herramientas de productividad institucional en nube, entre ellas Microsoft Office 365 y Microsoft Copilot, así como aplicaciones web institucionales expuestas a internet.

El crecimiento sostenido de las ciberamenazas dirigidas al sector público colombiano, la sofisticación de los vectores de ataque modernos — que incluyen ransomware, amenazas persistentes avanzadas (APT), ataques de denegación de servicio distribuido y explotación de vulnerabilidades en aplicaciones web — y la expansión de la superficie de ataque derivada de la arquitectura híbrida

de la entidad, hacen necesaria la implementación de un modelo de seguridad continuo, proactivo e integrado que supere las capacidades de un esquema de protección tradicional basado únicamente en controles perimetrales.

En este contexto, la Oficina de Tecnologías de la Información y las Comunicaciones — OTIC del INVIAS identifica como necesidad institucional la contratación de un proyecto integral de ciberseguridad que centralice la visibilidad, detección, respuesta y gestión de amenazas sobre el universo de activos de la infraestructura del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS, a través de la operación de un Centro de Operaciones de Seguridad (SOC) y los servicios complementarios de protección perimetral descritos en la presente ficha técnica.

Por lo anterior, el proceso de contratación tiene por alcance la adquisición, implementación y operación de un proyecto integral de ciberseguridad sobre la infraestructura tecnológica del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS — Datacenter propio, entorno de nube Microsoft Azure y sedes departamentales — conforme a los once (11) ítems descritos en la tabla de bienes y servicios, agrupados en los siguientes tres (3) componentes:

Componente A — Operación del Centro de Operaciones de Seguridad (SOC)

Comprende la implementación, despliegue y operación continua durante las veinticuatro (24) horas del día, los siete (7) días de la semana y los trescientos sesenta y cinco (365) días del año (24×7×365), de las plataformas tecnológicas y del equipo humano especializado necesarios para el monitoreo, detección y respuesta ante eventos e incidentes de seguridad sobre el universo de activos a proteger de la infraestructura del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS.

El SOC operará en modalidad tercerizada (MSSP), con un equipo de analistas organizados en tres niveles de atención (L1, L2 y L3), y deberá garantizar a INVIAS acceso propio e independiente a las consolas de monitoreo, dashboards ejecutivos y reportes operativos en tiempo real, sin intermediación del proveedor.

Este componente integra los siguientes servicios: (i) correlación centralizada de eventos de seguridad (SIEM), con ingesta de logs provenientes de los treinta y uno (31) dispositivos de seguridad perimetral existentes, la plataforma EDR/XDR, el WAF, el AntiDDoS, Microsoft Office 365 y los activos desplegados en Microsoft Azure; (ii) detección y respuesta en endpoints (EDR/XDR), que reemplazará la solución antivirus existente y cubrirá hasta tres mil (3.000) activos incluyendo equipos de cómputo y servidores; (iii) orquestación, automatización y respuesta con módulo integrado de gestión del ciclo de vida de incidentes (SOAR/IRP), que incluirá playbooks automatizados por tipo de amenaza, triaje por niveles, análisis forense digital y documentación de lecciones aprendidas; (iv) inteligencia de amenazas, con actualización continua de indicadores de compromiso (IoCs), monitoreo de amenazas dirigidas al sector público colombiano y un mínimo de dos (2) ejercicios mensuales de búsqueda proactiva de amenazas (threat hunting); y (v) gestión de vulnerabilidades, con escaneo continuo de activos sobre la infraestructura híbrida de la entidad,

priorización por riesgo real y un mínimo de dos (2) pruebas de penetración (pentesting) anuales sobre infraestructura interna y externa.

Componente B — Protección perimetral y control de acceso integrados al SOC

Comprende el suministro, instalación y puesta en operación de un dispositivo físico (appliance) de mitigación de ataques de denegación de servicio distribuido (AntiDDoS) en capas 3 y 4 de red sobre la infraestructura del INVIAS, el suministro, instalación y puesta en operación de la solución de control de acceso a la red (NAC) con sus licencias asociadas, y la renovación con ampliación de capacidades del firewall de aplicaciones web (WAF) de la entidad, en modalidad nube, de cincuenta (50) Mbps y diez (10) sitios a cien (100) Mbps y treinta (30) sitios.

Ambos componentes deberán integrarse al SOC mediante el envío de alertas, eventos y logs hacia la plataforma SIEM, garantizando la correlación centralizada de todos los eventos de seguridad perimetral. La protección de capa 3 y 4 será responsabilidad del appliance AntiDDoS, mientras que la protección de capa 7 (aplicación) será responsabilidad del WAF, cubriendo de forma complementaria la totalidad del espectro de ataques volumétricos y de aplicación.

Componente C — Servicios profesionales

Comprende dos (2) servicios: (i) Implementación y despliegue integral: instalación, configuración e integración de la totalidad de plataformas contratadas, incluyendo la incorporación de los treinta y uno (31) dispositivos de seguridad perimetral existentes como fuentes primarias del SIEM, la migración de la solución antivirus actual hacia la plataforma EDR/XDR sin interrupción del servicio, la configuración de playbooks base en el SOAR, el tuning inicial de reglas de correlación y casos de uso específicos para INVIAS, y un mínimo de cuarenta (40) horas de transferencia de conocimiento al equipo de la OTIC. El plazo máximo para la puesta en producción completa del SOC es de doce (12) semanas contadas desde la firma del acta de inicio. (ii) Bolsa de horas especializadas prepagadas: doscientas (200) horas prepagadas de servicios especializados de alto nivel, disponibles desde la firma del contrato y consumibles bajo demanda durante la vigencia de la suscripción a un año adquirida, mediante autorización previa del supervisor designado por INVIAS. Esta bolsa está reservada exclusivamente para situaciones críticas que superen la operación rutinaria del SOC, tales como la atención de ciberataques de alto impacto, mesas de crisis institucionales, análisis forense con cadena de custodia formal, ejercicios de simulación de ataques (Red Team), acompañamiento a auditorías externas e incidentes con afectación a la continuidad operacional de la entidad.

Universo de activos a proteger y justificación de las cantidades

Las cantidades y capacidades requeridas en el presente proceso se dimensionaron a partir del universo de activos a proteger, entendido como el conjunto de activos que conforman la infraestructura del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS. No se discrimina cuáles activos son de uso exclusivo de VIITS y cuáles son de uso compartido, toda vez que la seguridad de la plataforma depende de la protección del conjunto. El universo se estima así:

(i) Estaciones de trabajo: aproximadamente dos mil quinientos (2.500) equipos de cómputo corporativos. La entidad cuenta actualmente con 1.800 licencias de antivirus, que no cubren servidores.

(ii) Servidores: Ciento veinticuatro (124) máquinas virtuales identificadas en el inventario de Microsoft Azure junto con sus aplicaciones web (61) y direcciones IP públicas (85) expuestas, dejando una holgura de hasta 220 servidores acorde con el plan de capacidad estimado para el 2027.

(iii) Equipos de red: aproximadamente setenta (70) switches de acuerdo con el inventario de la entidad.

(iv) Seguridad perimetral: treinta y un (31) dispositivos de seguridad (firewalls), fuentes primarias del SIEM.

(v) Holgura de crecimiento: cien (100) dispositivos adicionales asociados a la operación y ampliación de VIITS.

Con base en este universo, la solución EDR/XDR se dimensiona con un techo de hasta tres mil (3.000) activos, que corresponden a los equipos de cómputo y servidores físicos y virtuales, e incluye la holgura de crecimiento. El SIEM, el SOAR/IRP, la inteligencia de amenazas y la gestión de vulnerabilidades se dimensionan sobre este mismo universo de activos y sobre las fuentes de log descritas en el Componente A.

Para la vigencia de la suscripción será de un (1) año, contado desde la activación de la totalidad de los productos contratados y la puesta en operación del personal del SOC, condiciones que deberán cumplirse de forma simultánea y quedar acreditadas mediante acta de inicio suscrita por ambas partes. Mientras no se suscriba el acta de inicio, la suscripción no se considerará en ejecución para efectos del cómputo de la vigencia, sin perjuicio de las obligaciones del contratista derivadas de la etapa de implementación y despliegue.

La totalidad de licencias de software adquiridas en el marco del presente contrato deberán quedar registradas a nombre del INVIAS, independientemente del proveedor que las gestione u opere. Al vencimiento de la suscripción, el contratista deberá entregar al INVIAS la totalidad de reglas de correlación, playbooks, casos de uso, configuraciones y documentación técnica desarrollados durante la vigencia, como condición para la liquidación del contrato.

INVIAS tendrá acceso propio, permanente e independiente a las consolas de monitoreo, dashboards ejecutivos, reportes operativos y registros de incidentes del SOC, sin necesidad de intermediación del contratista. El proveedor no podrá restringir, limitar o condicionar este acceso en ninguna circunstancia durante la vigencia de la suscripción adquirida.

El contratista deberá cumplir los siguientes tiempos mínimos de respuesta según la severidad del incidente: Crítico: tiempo de detección (MTTD) máximo quince (15) minutos y tiempo de respuesta (MTTR) máximo cuatro (4) horas. Alto: MTTD máximo una (1) hora y MTTR máximo ocho (8) horas. Medio: MTTD máximo cuatro (4) horas y MTTR máximo veinticuatro (24) horas. El incumplimiento reiterado de estos niveles de servicio constituirá causal de incumplimiento contractual.

Al vencimiento de la suscripción, el contratista deberá garantizar un período de transición mínimo de sesenta (60) días calendario, durante el cual prestará soporte técnico al nuevo proveedor o al equipo interno de INVIAS para la transferencia ordenada de la operación del SOC, sin costo adicional para la entidad.

La arquitectura tecnológica implementada deberá permitir la habilitación futura de reportes e integración con organismos gubernamentales de ciberseguridad (MinTIC, ColCERT, CSIRT.gov) sin necesidad de modificación del contrato ni adquisición de nuevas licencias o plataformas.

5.2 MODALIDAD DE SELECCIÓN

De conformidad con el objeto, obligaciones del contrato que se requiere suscribir para satisfacer las necesidades del INVIAS, especificaciones técnicas del bien o servicio a adquirir, el presupuesto oficial estimado, la modalidad de selección que resulta aplicable es **SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES – SUBASTA INVERSA.**

5.3 FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

Debido a la cuantía y el objeto a contratar la presente contratación se efectuará a través de **SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES** procedimiento establecido en el Literal a) del Numeral 2 del Artículo 2 de la Ley 1150 de 2007, que define cuando aplicar esta modalidad, así:

> *a) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos. Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo*

derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos.

El INVIAS adelantará el proceso por la modalidad de **SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES POR SUBASTA INVERSA**, según el procedimiento establecido en la Ley 80 de 1993, según lo señalado en el Literal a) Numeral 2o, del Artículo 2o de la Ley 1150 de 2007 y los Artículos 2.2.1.2.1.2.2 y siguientes del Decreto 1082 de 2015 y las demás normas concordantes y complementarias sobre la materia La subasta se realizarán por importe agotable.

Lo anterior de acuerdo con lo establecido por Colombia Compra Eficiente para los Procesos de Selección Abreviada por Subasta en SECOP II. Finalmente, es importante precisar que el INVIAS requiere el aumento de la capacidad, disponibilidad y confiabilidad de sus servicios tecnológicos. Para este caso, estos servicios no se encuentran estandarizados en Colombia Compra Eficiente; por lo tanto, se realizará el proceso contractual mediante la modalidad mencionada.

De acuerdo con el análisis de las condiciones del mercado y las necesidades de la Entidad, se determina que el objeto contractual corresponde a un servicio con características técnicas uniformes, en la medida en que las especificaciones pueden ser estandarizadas, comparables y evaluadas objetivamente por los proponentes. El alcance del contrato ha sido estructurado con base en especificaciones técnicas previamente definidas por la Entidad, sin espacio para adaptaciones particulares, propuestas creativas o desarrollos a medida, sin alterar la funcionalidad de los bienes o servicios, bajo estándares técnicos reconocidos a nivel nacional e internacional, y con patrones de desempeño y calidad homogéneos. Las condiciones del servicio han sido diseñadas para que todos los posibles oferentes puedan identificar claramente los requerimientos, entender el alcance y presentar ofertas comparables entre sí.

La principal contribución del Centro de Operaciones de Seguridad consiste en cerrar la brecha existente entre las herramientas de seguridad actualmente desplegadas y la capacidad institucional para analizar, correlacionar e interpretar la información generada por estas soluciones. Esto permitirá transformar grandes volúmenes de registros y eventos de seguridad en alertas accionables e incidentes gestionables de manera oportuna fortaleciendo la capacitad institucional de detección y respuesta. Para el PSCN-VIITS, esto significa que los eventos generados por sus dispositivos de campo, plataformas de datos y centros de control pueden integrarse al monitoreo del Instituto e interpretarse junto con los del resto de la infraestructura, de manera que un comportamiento anómalo en un sensor, una cámara o un enlace de comunicaciones se detecte y se atienda como un posible incidente de seguridad y no solo como una falla operativa.

De igual forma, los servicios y productos que se pretenden adquirir o renovar de acuerdo con el anexo técnico no varían sustancialmente entre los diferentes oferentes como se evidencia en las

cotizaciones presentadas.

Por consiguiente, este proceso asegura la disponibilidad de servicios de soporte con especificaciones técnicas y estándares de calidad homogéneos, que corresponden a bienes y servicios de común utilización, en concordancia con lo establecido en el literal (a) del numeral 2 del artículo 2° de la Ley 1150 de 2007.

En consecuencia, al ser un proceso de selección abreviada para adquirir bienes y servicios técnicos uniformes y de uso común, la modalidad de contratación es por subasta inversa, prevista en el literal a) del numeral 2 del artículo 2 de la Ley 1150 de 2007, y tendrá como único factor de elección el menor precio, que se seleccionará mediante subasta inversa, según el artículo 2.2.1.2.1.2.1. y siguientes del Decreto 1082 de 2015.

Que, según lo regulado en el artículo 5 del Decreto 1860 de 2021 por el que modifica el artículo 2.2.1.2.1.2.2. de la Subsección 2 de la Sección 2 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015. Modifíquese el artículo 2.2.1.2.1.2.2. de la Subsección 2 de la Sección 1 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, el cual quedará así:

> *"Artículo 2.2.1.2.1.2.2. Procedimiento para la subasta inversa. Además de las reglas generales previstas en la ley y en el presente título, las siguientes reglas son aplicables a la subasta inversa:*
>
> *1. Los pliegos de condiciones deben indicar: a) la fecha y hora de inicio de la subasta; b) la periodicidad de los Lances; y c) el Margen Mínimo para mejorar la oferta durante la subasta inversa.*
>
> *2. La oferta debe contener dos parles, la primera en la cual el interesado acredite su capacidad de participar en el Proceso de Contratación y acredite el cumplimiento de la ficha técnica; y la segunda parle debe contener el precio inicial propuesto por el oferente.*
>
> *3. La Entidad Estatal debe publicar un informe de habilitación de los oferentes, en el cual debe indicar si los bienes o servicios ofrecidos por el interesado cumplen con la ficha técnica y si el oferente se encuentra habilitado.*
>
> *4. Hay subasta inversa siempre que haya como mínimo dos oferentes habilitados cuyos bienes o servicios cumplen con la ficha técnica.*
>
> *5. Si en el Proceso de Contratación se presenta un único oferente cuyos bienes o servicios cumplen con la ficha técnica y está habilitado, la Entidad Estatal puede adjudicarle el contrato al único oferente si el valor de la oferta es igualo inferior a la*

disponibilidad presupuesta l para el contrato, caso en el cual no hay lugar a la subasta inversa.

6. La subasta debe iniciar con el precio más bajo indicado por los oferentes y, en consecuencia, solamente serán válidos los Lances efectuados durante la subasta inversa en los cuales la oferta sea mejorada en por lo menos el Margen Mínimo establecido (2%)

7. Si los oferentes no presentan Lances durante la subasta, la Entidad Estatal debe adjudicar el contrato al oferente que haya presentado el precio inicial más bajo.

8. Al terminar la presentación de cada Lance, la Entidad Estatal debe informar el valor del Lance más bajo.

9. Si al terminar la subasta inversa hay empate, la Entidad Estatal debe aplicar los criterios del artículo 35 de la Ley 2069 de 2020 conforme con los medios de acreditación del artículo 2.2.1.2.4.2.17 del Decreto 1860 de 2021.

El Instituto Nacional de Vías adelantará el proceso de contratación cumpliendo los principios de transparencia, economía y responsabilidad, según la Ley 80 de 1993, el literal a) del numeral 2 del artículo 2 de la Ley 1150 de 2007, acorde a los artículos 2.2.1.2.1.2.2. y siguientes del Decreto 1082 de 2015, para lo cual desarrollará un proceso de **SELECCIÓN ABREVIADA - SUBASTA INVERSA ELECTRONICA**.

CONDICIONES LIMITADA A MIPYMES:

De acuerdo con lo señalado 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, el cual modifica la Subsección 2 de la Sección 4 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, y teniendo en cuenta que el valor del presente proceso de selección es superior a los ciento veinticinco mil dólares de los EEUU (US 125.000) es decir $511.708.497 liquidados con la tasa de cambio que para el efecto determina el Ministerio de Comercio, Industria y Turismo, por lo que la Entidad **NO** convoca a las Mipyme Nacionales, por lo tanto teniendo en cuenta la cuantía del presente proceso, **NO le aplica la limitación a Mipyme.**

BUENAS PRÁCTICAS PARA LA CONTRATACIÓN TRANSPARENTE.

De conformidad con lo establecido en el literal b del artículo 2.1.4.3.2.1. del Decreto 1600 de 2024, la Entidad garantiza que aplico las guías y manuales definidos por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, para la definición de criterios que permitan garantizar la pluralidad de oferentes, se aplican al presente proceso de selección; y que dicha

información fue tenida en cuenta para la definición de criterios que permitan garantizar la pluralidad de oferentes, se apliquen en la organización.

5.4 CLASIFICADOR DE BIENES Y SERVICIOS A CONTRATAR – CÓDIGOS UNSPSC

Teniendo en cuenta que el Decreto 1082 de 2015, exige que, para efectos de acreditación de experiencia, las empresas deben encontrarse clasificados en el "Clasificador de Bienes, Obras y Servicios de las Naciones Unidas" se validó que de acuerdo con el presente proceso y con el ánimo de propiciar la mayor participación de oferentes los interesados deben estar inscritos en el Registro Único de Proponentes (RUP) en el código UNSPSC publicado en la página www.colombiacompra.gov.co.

El objeto contractual se clasifica en los siguientes códigos del Clasificador de Bienes y Servicios:

Códigos UNSPSC

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	PRODUCTOS
43233203	Tecnología de la Información, Radiodifusión y Telecomunicacio	Software	Software de seguridad y protección	**Software de manejo de seguridad de red o de redes**
43233205	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Software	Software de seguridad y protección	**Software de seguridad de transacciones y de protección contra virus**
43232908	Tecnología de la Información, Radiodifusión y Telecomunicacio	Software	Software de red	**Software de interruptor o enrutador**
43222605	Tecnología de la Información, Radiodifusión y Telecomunicacio	Equipos o plataformas y accesorios de redes	Equipo de servicio de red	**Puerta de acceso de redes**
81111801	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes	**Seguridad de los computadores, redes o internet**

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	PRODUCTOS
81111808	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	**Servicio de análisis de sistemas**
81111809	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	**Servicio de instalación de sistemas**
81111811	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes	**Servicios de soporte técnico o de mesa de ayuda**
81111508	Servicios Basados en Ingeniería, Investigación y	Servicios informáticos	Ingeniería de software o hardware	**Servicios de implementación de aplicaciones**

Fuente: Elaboración propia con datos de la PLATAFORMA COLOMBIA COMPRA EFICIENTE.

5.5 CERTIFICACIÓN PLAN ANUAL DE ADQUISICIONES

Existe la apropiación disponible para cubrir la necesidad con la descripción ***'CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS*****,** actividad que se incluyó oportunamente en el plan de adquisiciones del año 2026 en el portal de contratación pública SECOP II, garantizando así la disponibilidad de los recursos para la contratación.

5.6 CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

Para atender el valor del contrato a celebrarse la entidad cuenta con el Certificado de Disponibilidad Presupuestal No. **266026** de fecha **28 de octubre de 2026** con recursos propios disponibles en la vigencia 2026 por valor de **$ 3.135.458.435,00**. Asimismo, para garantizar la financiación de las obligaciones contractuales correspondientes a la vigencia fiscal 2027, se tiene prevista la asignación de recursos propios mediante la autorización de vigencias futuras, por valor de **$2.894.706.492.** una vez finalizado el trámite correspondiente para su aprobación se remitirá la autorización expedida por el Ministerio de Hacienda la cual es requisito indispensable para la publicación del pliego definitivo de condiciones.

5.7 LUGAR DE EJECUCIÓN

El lugar de ejecución será la Ciudad de Bogotá D.C. en la dirección Calle 25G # 73B-90 piso 8 Dirección general INVIAS - Complejo Empresarial Central Point; Bogotá.

5.8 PLAZO DE EJECUCIÓN DEL CONTRATO

El plazo de ejecución del contrato se contará a partir de la suscripción del acta de inicio y previo cumplimiento de los requisitos de perfeccionamiento, ejecución y legalización del contrato hasta el **31 de marzo de 2027**, mismo que podrá prorrogar según el desarrollo del contrato, por necesidades del servicio.

El contratista garantizará durante el tiempo de ejecución del contrato y de vigencia de las garantías contractuales la correcta ejecución del contrato y el cumplimiento de las especificaciones técnicas establecidas en el documento "**ANEXO 1 – ANEXO TECNICO – CIBERSEGURIDAD**"

5.9 TIPOLOGÍA CONTRACTUAL

Prestación de servicios

5.10 COMPROMISO DEL INSTITUTO NACIONAL DE VIAS

El Instituto Nacional de Vías brindará al contratista el apoyo necesario para el desarrollo del contrato, así, entregará toda la información que sea necesaria y facilitará el ambiente para la realización de la gestión y las reuniones de trabajo y ejecución de labores entre el contratista, el supervisor del contrato y demás funcionarios que sea necesario para cumplir con el objeto contractual.

5.11 PRESUPUESTO ESTIMADO Y JUSTIFICACIÓN

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

El presupuesto oficial total establecido por el INVIAS para el presente proceso asciende a la suma de **SEIS MIL TREINTA MILLONES CIENTO SESENTA Y CUATRO MIL NOVECIENTOS VEINTISIETE PESOS M/CTE**. (**$ 6.030.164.927,00)** incluido IVA (en los ítems que apliquen o correspondan) y todos los costos directos e indirectos que se ocasionen por el hecho de la suscripción, ejecución y terminación del contrato.

Para atender el valor del contrato a celebrarse la entidad cuenta con el Certificado de Disponibilidad Presupuestal No. **266026** de fecha **28 de octubre de 2026** con recursos propios disponibles en la vigencia 2026 por valor de **$ 3.135.458.435,00**. Asimismo, para garantizar la financiación de las obligaciones contractuales correspondientes a la vigencia fiscal 2027, se tiene prevista la asignación de recursos propios mediante la autorización de vigencias futuras, por valor de **$2.894.706.492.** una vez finalizado el trámite correspondiente para su aprobación se remitirá la autorización expedida por el Ministerio de Hacienda la cual es requisito indispensable para la publicación del pliego definitivo de condiciones.

VIGENCIA	CDP	RUBRO	FUENTE	VALOR
2026	266026	C-2409-0600-9-20301C-2409010-02	Propios	$ 3.135.458.435,00
2027	VFO	C-2409-0600-9-20301C	Propios	$ 2.894.706.492,00
Total presupuesto estimado				**$ 6.030.164.927,00**

5.12 FORMA DE PAGO

El INSTITUTO NACIONAL DE VIAS pagará al CONTRATISTA el valor del contrato en moneda legal colombiana así:

Pago 1 — Suscripciones de soluciones de seguridad: Corresponde al valor de las suscripciones anuales de los ítems 2 (SIEM), 3 (EDR/XDR), 4 (SOAR/IRP), 5 (Threat Intelligence), 6 (Gestión de Vulnerabilidades) y 8 (WAF Imperva), que se pagará en un desembolso, dentro de los sesenta (60) días siguientes a la radicación de la factura electrónica:

Condiciones de verificación del desembolso por cada suscripción:

Suscripción	Condición de verificación
SIEM	Activación de la suscripción con evidencia de registro ante el fabricante.
EDR/XDR	Activación de la suscripción con evidencia de registro ante el fabricante.

Suscripción	Condición de verificación
SOAR/IRP	Activación de la suscripción con evidencia de registro ante el fabricante.
Threat Intelligence	Activación de la suscripción con evidencia de registro ante el fabricante.
Gestión de Vulnerabilidades	Activación de la suscripción con evidencia de registro ante el fabricante.
WAF Imperva	Activación de la renovación y ampliación de la suscripción con certificado oficial de Imperva.

En todos los casos, el desembolso estará condicionado a la suscripción del acta de recibo a satisfacción por parte del supervisor del contrato, que certifique la verificación de cada suscripción activa.

Pago 2 — Appliances físicos y sus licencias: Corresponde al valor de los appliances físicos y las licencias de software asociadas de los ítems 7 (AntiDDoS) y 9 (NAC). Se realizará dentro de los sesenta (60) días siguientes a la radicación de la factura electrónica, previa verificación y acreditación simultánea de las siguientes condiciones:

1. Entrega física de los appliances en las instalaciones del INVIAS en Bogotá D.C., en condiciones nuevas y en caja sellada de fábrica.
2. Instalación y puesta en operación de los appliances a entera satisfacción del supervisor del contrato.
3. Activación de las licencias de software asociadas con evidencia de registro ante el fabricante.
4. Incorporación de los bienes al inventario institucional del INVIAS con soporte de entrada al almacén suscrito por el almacenista de la entidad.
5. Suscripción del acta de recibo a satisfacción de los bienes y sus licencias por parte del supervisor del contrato.

Pago 3 — Implementación, Monitoreo SOC y Bolsa de horas especializadas: Corresponde al valor de los ítems 10 (Implementación y despliegue), 1 (Monitoreo SOC) y 11 (Bolsa de horas especializadas prepagadas). Se realizará dentro de los sesenta (60) días siguientes a la radicación de la factura electrónica, previa verificación y acreditación simultánea de las siguientes condiciones:

1. Puesta en operación completa del SOC con la totalidad de las plataformas contratadas funcionando de forma integrada y verificada.
2. Suscripción del acta de inicio operativo del SOC por ambas partes, que certifique el cumplimiento simultáneo de los diez (10) criterios de arranque operativo definidos en la ficha técnica.

Confirmación escrita de la disponibilidad inmediata de los perfiles especializados de la bolsa de horas, con datos de contacto 24×7 aceptada por el supervisor del contrato.

Para efectos de presentar las cuentas de cobro o facturas, el contratista aportará las certificaciones de cumplimiento por parte del Supervisor, certificación de pago de aportes a seguridad social y legales y demás documentos exigidos para el trámite respectivo.

Adicionalmente el contratista deberá presentar certificación de Paz y Salvo de Aportes legales y de Seguridad Social, la acreditación de estos aportes se requerirá para la realización de cada pago derivado del presente contrato al tenor de lo dispuesto por el artículo 23 de la Ley 1150 de 2007. El pago se efectuará dentro de los sesenta (60) días siguientes a la correcta presentación de los documentos requeridos para tal fin ante el Área de Cuentas por pagar de la Subdirección Financiera. Se entiende que la factura de cobro respectiva es presentada correctamente, cuando cumpla con el lleno de los requisitos exigidos por EL INSTITUTO o hayan sido subsanadas las glosas formuladas por el área de Cuentas por Pagar de la Subdirección Financiera. Se establece como fecha de pago, la fecha de consignación de los recursos en la respectiva cuenta bancaria de la entidad financiera, informada con anterioridad por EL CONTRATISTA. En el evento en que EL INSTITUTO no efectúe el pago de la factura de cobro respectiva, pasados los sesenta (60) días para el pago, siempre y cuando se hayan presentado correctamente dichos documentos con el cumplimiento de los anteriores requisitos, deberá cancelar al CONTRATISTA un interés equivalente al interés legal civil, según el Artículo, según el artículo 2.2.1.1.2.4.2 decreto 1082 de 2015, por configurarse mora en el pago, salvo que se trate la citada mora por circunstancias de PAC, caso en el cual el contratista no podrá cobrar los intereses aludidos.

CUENTA BANCARIA. - Para el pago de las facturas, El CONTRATISTA presentará certificación bancaria con la información necesaria para que el Grupo de Cuentas por pagar de la Subdirección Financiera del INSTITUTO abone los pagos en desarrollo de la ejecución del contrato. Cualquier cambio en la información bancaria deberá reportarla adjuntando copia de la nueva certificación.

Nota 1: El pago se cancelará a través de abono en cuenta mediante transferencia electrónica a la cuenta de ahorros o corriente que el contratista haya reportado con los documentos exigidos para la contratación, a través de las entidades financieras afiliadas al sistema automático de pagos, previos los descuentos de ley.

Para efectos del pago el contratista deberá adjuntar factura y Certificación de los pagos de aportes al Sistema de Seguridad Social Integral en salud, pensiones, ARL y de aportes parafiscales a que haya lugar, o de la certificación respectiva expedida por el contador o Revisor Fiscal.

Los pagos serán previamente aprobados por la supervisión que designe el INVIAS para la vigilancia

de este contrato, de acuerdo con la disponibilidad de PAC.

6 REQUISITOS HABILITANTES

Son requisitos y documentos mínimos habilitantes la capacidad jurídica, garantía de seriedad del ofrecimiento, la capacidad financiera, organizacional y el cumplimiento de las especificaciones técnicas que la entidad ha definido como condiciones mínimas que deberán cumplir los proponentes para que su propuesta sea habilitada. Estos requisitos no otorgan puntaje y la entidad los verificará como CUMPLE o NO CUMPLE.

De acuerdo con lo establecido en el numeral 1 del artículo 5 de la Ley 1150 de 2007 y en el artículo 2.2.1.1.1.5.3, 2.2.1.1.1.6.1 y 2.2.1.1.1.6.2 del Decreto Nacional 1082 de 2015, la entidad procederá a verificar y evaluar las condiciones jurídicas, financieras y técnicas de los interesados en participar, con el propósito de habilitar las propuestas presentadas.

En el momento señalado en el pliego de condiciones los proponentes presentaran una propuesta completa, que incluya la información sobre la capacidad jurídica y técnica, capacidad financiera y la propuesta económica o inicial de precio.

De acuerdo con el artículo 2.2.1.1.1.5.3. del Decreto 1082 de 2015, los requisitos habilitantes son:

a) Capacidad Jurídica

b) Capacidad Financiera.

c) Organizacional y de experiencia.

7 CAPACIDAD JURÍDICA

Los interesados podrán participar como proponentes bajo alguna de las siguientes modalidades siempre y cuando cumplan los requisitos exigidos en el pliego de condiciones:

Individualmente como:

a) personas naturales nacionales o extranjeras,

b) personas jurídicas nacionales o extranjeras.

Conjuntamente, como proponentes plurales en cualquiera de las formas de asociación previstas en el artículo 7 de la Ley 80 de 1993.

Los proponentes deben:

A. Tener capacidad jurídica para la presentación de la oferta.

B. Tener capacidad jurídica para la celebración y ejecución del contrato.

C. No estar incursos en ninguna de las circunstancias de inhabilidad, incompatibilidad, conflicto de interés o prohibición para contratar previstas en la Constitución y en la Ley.

D. No estar reportados en el último Boletín de responsables Fiscales vigente publicado por la Contraloría General de la República. Esta disposición aplica para el proponente e integrantes de un proponente plural con domicilio en Colombia. Tratándose de proponentes extranjeros sin domicilio o sin sucursal en Colombia, deben declarar que no son responsables fiscales por actividades ejercidas en Colombia en el pasado y que no tienen sanciones vigentes en Colombia que impliquen inhabilidad para contratar con el Estado.

E. Presentar el certificado del Registro de Deudores Alimentarios Morosos REDAM en el cual demuestre no estar inhabilitado en los términos de la Ley 2097 de 2021.

F. Las personas jurídicas oferentes y/o de los proponentes plurales que se presenten como proponentes en el proceso de selección, deberán poner de presente la existencia o no de situaciones de control de las que participen y, en particular, si son controlantes, controladas o comparten alguna de estas condiciones con otras personas que se encuentren participando en el mismo procedimiento de contratación en el término máximo de tres (3) días **después** del momento en que se cierre definitivamente la presentación de ofertas, conforme lo establece el literal a) del Artículo 2.1.4.3.2.1. del Decreto 1600 de 2024. Para el caso de los proponentes plurales, deberán indicar si las personas que los conforman se encuentran en alguna de las situaciones descritas anteriormente.

   Por lo anterior, para la acreditación de este requisito se deberá diligenciar el formato denominado “FORMATO INFORMACION PARTICIPACION DE SOCIEDADES CONTROLANTES Y CONTRALADAS (Decreto 1600 de 2024)” que hace parte de los documentos del proceso y el cual deberá ser allegado en el término establecido en la norma y en el Cronograma del Proceso".

7.1 CARTA DE PRESENTACIÓN DE LA OFERTA

El proponente debe presentar el Formato 1 – Carta de Presentación de la Oferta el cual debe ir firmado por la persona natural proponente o por el representante legal del proponente individual o

plural o por el apoderado de acuerdo con el modelo suministrado y los requisitos establecidos en los presentes pliegos de condiciones.

Quien suscriba la carta de presentación de la propuesta deberá:

A. Con la presentación del formato 1, “CARTA DE PRESENTACIÓN DE LA PROPUESTA” el proponente acepta todos y cada uno de los puntos contenidos dentro del mismo y se allana a las disposiciones de los literales B, C, D Y E del presente proceso de selección

B. Tener la calidad de representante legal o apoderado del proponente, con facultad expresa de actuar en nombre y representación del mismo. En este último caso, la facultad de representación debe comprender las de presentar la propuesta, celebrar el contrato (en caso de resultar adjudicatario) y liquidarlo. Si la presentación de la propuesta implica la transgresión del deber establecido en el numeral 7° del artículo 23 de la ley 222 de 1995, el proponente individual o el integrante de la propuesta conjunta deberá, además, allegar autorización de la junta de socios o asamblea general de accionistas, según corresponda.

C. En el evento de que la propuesta sea presentada y suscrita por apoderado, se deberá adjuntar el poder legalmente expedido que así lo faculte.

D. En caso de ser consorcio o unión temporal: Tener la calidad de representante del consorcio o unión temporal, con facultad expresa de actuar en nombre y representación del mismo. Tal facultad de representación debe comprender la de presentar la propuesta, celebrar el contrato (en caso de resultar adjudicatarios) y liquidarlo.

La fecha de expedición de tales documentos no podrá ser posterior a la fecha definitiva de cierre del presente proceso de selección.

7.2 EXISTENCIA Y REPRESENTACIÓN LEGAL

La existencia y representación legal de los proponentes individuales o miembros de los proponentes Plurales se acreditará de acuerdo con las siguientes reglas:

7.2.1 PERSONAS NATURALES

Deben presentar los siguientes documentos en copia simple:

a. Persona natural de nacionalidad colombiana: cédula de ciudadanía.

b. Persona natural extranjera con residencia en Colombia: cédula de extranjería

vigente expedida por la autoridad competente.

c. Persona natural extranjera sin domicilio en Colombia: pasaporte.

7.2.2 PERSONAS JURÍDICAS

Deben presentar los siguientes documentos:

- Persona jurídica nacional o extranjera con sucursal en Colombia:

I. Certificado de existencia y representación legal expedido por la Cámara de Comercio o autoridad competente, en el que se verificará:

a. Fecha de expedición del certificado no mayor a treinta (30) días calendario anteriores a la fecha de cierre del proceso de contratación. En caso de modificarse la fecha de cierre del proceso, se tendrá como referencia para establecer el plazo de vigencia del certificado de existencia y representación legal la fecha originalmente establecida en el pliego de condiciones definitivo.

b. Que el objeto de la sociedad permita ejecutar las actividades descritas en el objeto del presente proceso de contratación.

c. Las personas jurídicas nacionales y extranjeras deberán acreditar que su duración no será inferior a la del plazo del contrato y un año más.

d. Si el representante legal de la sociedad tiene restricciones para contraer obligaciones en nombre de la misma, deberá acreditar su capacidad a través de una autorización suficiente otorgada por parte del órgano social competente respectivo para cada caso.

e. El nombramiento del revisor fiscal en caso de que exista.

f. Que las personas jurídicas extranjeras con actividades permanentes en la República de Colombia (contratos de obra o servicios) deberán estar legalmente establecidas en el territorio nacional de acuerdo con los artículos 471 y 474 del Código de Comercio.

II. Certificación del revisor fiscal en caso de ser sociedad anónima colombiana, en la que conste si es abierta o cerrada.

III. Fotocopia del documento de identificación del representante legal.

En el caso de las sucursales de las personas jurídicas extranjeras y como quiera que la sucursal en Colombia no es una persona jurídica diferente a la matriz, se tendrá en cuenta la fecha de constitución de esta última.

Si la oferta es suscrita por una persona jurídica extranjera a través de la sucursal debidamente constituida en Colombia, deberá acreditar la existencia de la sucursal y la capacidad jurídica de su representante o apoderado, mediante la presentación del Certificado del Registro Único de Proponentes y certificado de existencia y representación legal con fecha de expedición máximo de 30 días calendario antes de la fecha de cierre del presente proceso de selección por la Cámara de Comercio. Cuando el representante legal de la sucursal tenga restricciones para contraer obligaciones, deberá acreditar autorización suficiente del órgano competente social respectivo para contraer obligaciones en nombre de la sociedad. La ausencia definitiva de autorización suficiente o el no aporte de dicho documento una vez solicitado por la entidad, determinará la falta de capacidad jurídica para presentar la oferta

- Persona jurídica extranjera sin sucursal o domicilio en Colombia: Documentos que acrediten la existencia y representación legal de la sociedad extranjera, presentados de conformidad con lo establecido en el presente pliego de condiciones, en el que debe constar, como mínimo, los siguientes aspectos:

  I. Nombre o razón social completa.

  II. Nombre del representante legal o de la persona facultada para comprometer a la persona jurídica.

  III. Que el objeto de la sociedad permita ejecutar las actividades descritas en el objeto del presente proceso de selección.

  IV. Facultades del representante legal o de la persona facultada para comprometer a la persona jurídica, en la que se señale expresamente que el representante no tiene limitaciones para contraer obligaciones en nombre de la misma o aportando la autorización o documento correspondiente del órgano social competente respectivo para cada caso.

  V. Tipo, número y fecha del documento de constitución o creación.

  VI. Fecha y clase de documento por el cual se reconoce la personería jurídica.

  VII. Acreditar que su duración no será inferior a la del plazo del contrato y un año más.

VIII. Fotocopia del documento de identificación del representante legal.

Si no existiera ninguna autoridad o entidad que certifique la totalidad de la información de existencia y representación legal, el proponente o miembro extranjero del proponente plural debe presentar una declaración juramentada de una persona con capacidad jurídica para vincular y representar a la sociedad en la que conste que: i) no existe autoridad u organismo que certifique lo solicitado en el presente numeral; ii) la información requerida en el presente literal, y iii) la capacidad jurídica para vincular y representar a la sociedad de la persona que efectúa la declaración, así como de las demás personas que puedan representar y vincular a la sociedad, si las hay.

- Entidades estatales: Deben presentar los siguientes documentos para acreditar su existencia:

Acto de creación de la entidad estatal. Este puede ser ley, decreto, ordenanza, acuerdo o certificado de existencia y representación legal (este último no mayor a treinta (30) días calendario anteriores a la fecha de cierre del proceso de contratación) o documento equivalente que permita conocer la naturaleza jurídica, funciones, órganos de dirección, régimen jurídico de contratación de la entidad estatal.

NOTA: En el evento de personas jurídicas no obligadas a aportar el certificado de existencia y representación legal, deberán aportar un documento equivalente que acredite su existencia, junto con los documentos que demuestren la capacidad del representante legal de la entidad o sociedad a contratar, en el cual se verificará:

- Fecha de expedición del documento equivalente que acredite su existencia.
- Que el objeto incluya las actividades principales objeto del presente proceso.
- La duración deberá ser por lo menos igual al plazo estimado del contrato y un (1) año más.
- El plazo de ejecución del contrato será el indicado en el numeral n Si el representante legal tiene restricciones para contraer obligaciones en nombre de la misma, deberá acreditar autorización suficiente del órgano competente social respectivo para contraer obligaciones en nombre de la sociedad o entidad.
- La ausencia definitiva de autorización suficiente o el no aporte de dicho documento una vez solicitado por la entidad, determinará la falta de capacidad jurídica para presentar la oferta, y por tanto su rechazo.

- El nombramiento del revisor fiscal en caso de que exista.

7.2.3 PROPONENTES PLURALES

El documento de conformación de proponentes plurales debe:

A. Acreditar la existencia del proponente plural y clasificarlo en Unión Temporal o Consorcio. En este documento los integrantes deben expresar su intención de conformar el proponente plural. En caso de que no exista claridad sobre el tipo de asociación se solicitará la aclaración. Los proponentes deben incluir como mínimo la información requerida en el FORMATO 2 – CONFORMACIÓN DE PROPONENTE PLURAL (Formato2A – Consorcios) (Formato 2B – Uniones Temporales). Los proponentes podrán incluir información adicional que no contradiga lo dispuesto en los documentos del proceso.

B. Acreditar el nombramiento de un representante y un suplente cuya intervención deberá quedar definida en el Formato 2 – Conformación de Proponente Plural (Formato – Consorcios) (Formato – Uniones Temporales), de todas las personas naturales y/o jurídicas asociadas, con facultades suficientes para la representación sin limitaciones de todos y cada uno de los integrantes, en todos los aspectos que se requieran para la presentación de la oferta, para la suscripción y ejecución del contrato, así como también la facultad para firmar el acta de terminación y liquidación.

C. Aportar copia del documento de identificación del representante principal y suplente de la estructura plural.

D. Acreditar que la vigencia de la estructura plural no sea inferior a la del plazo del contrato y un año adicional. Para efectos de la evaluación, este plazo será contado a partir de la fecha del cierre del proceso de contratación.

E. El proponente plural debe señalar expresamente cuál es el porcentaje de participación de cada uno de sus miembros. La sumatoria del porcentaje de participación no podrá ser diferente al 100%.

F. En la etapa contractual, no podrán ser modificados los porcentajes de participación sin el consentimiento previo de la entidad.

Dicho documento debe estar firmado por todos y cada uno de los integrantes del proponente plural y en el caso del integrante persona jurídica, por el representante legal de dicha o por el apoderado de cualquiera de los anteriores.

REGISTRO ÚNICO DE PROPONENTES

Todos los proponentes obligados a encontrarse inscritos en el RUP, y cuando se trate de Consorcio o Unión Temporal, cada uno de los integrantes, que aspiren a celebrar el o los contratos que se deriven del presente proceso contractual, deberán acreditar su inscripción vigente y en firme en el RUP, de conformidad con lo establecido en el artículo 6º de la Ley 1150 de 2007 y el Decreto 1082 de 2015 y demás normas que regulan la materia.

Para efectos de la evaluación se tendrá en cuenta lo siguiente:

- La fecha de expedición del certificado no mayor a treinta (30) días calendarios anteriores a la fecha de cierre del presente proceso.
- La Entidad verificará que la inscripción en el RUP se encuentre en firme y vigente a la fecha de la presentación de la oferta, y que no existan sanciones que puedan inhabilitar al proponente.
- En el evento que la propuesta se presente por un consorcio o unión temporal o promesa de sociedad futura, cada uno de los integrantes deberá aportar el registro, cumpliendo con los requisitos aquí previstos

NOTA 1: De conformidad con lo establecido en el artículo 6 de la Ley 1150 de 2007, modificado por el artículo 221 del Decreto – Ley 019 de 2012 y lo impuesto en el artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015, es un deber del inscrito, mantener actualizada la información que obra en el Registro Único de Proponentes.

NOTA 2: De conformidad con el artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015, los proponentes deben presentar la información para renovar su registro a más tardar el quinto día hábil del mes de abril de cada año, de lo contrario cesan los efectos de este. El INVÍAS se reserva la posibilidad de consultar en el RUES, la veracidad de la información aportada, conforme a la potestad verificadora.

7.3CERTIFICACIÓN DE PAGOS DE SEGURIDAD SOCIAL Y APORTES LEGALES

7.3.1 PERSONAS JURÍDICAS

El proponente persona jurídica debe presentar el Formato 4 – Pagos de seguridad social y aportes legales suscrito por el revisor fiscal, de acuerdo con los requerimientos de ley o por el representante legal, bajo la gravedad del juramento, cuando no se requiera revisor fiscal, en el que conste el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes

a las Cajas de Compensación Familiar, al Instituto Colombiano de Bienestar Familiar, al Servicio Nacional de Aprendizaje.

La entidad no exigirá las planillas de pago. Bastará el certificado suscrito por el revisor fiscal, en los casos requeridos por la ley, o por el representante legal que así lo acredite.

Cuando la persona jurídica está exonerada en los términos previstos en el artículo 65 de la Ley 1819 de 2016 debe indicarlo en el Formato – Pagos de seguridad social y aportes legales

Esta misma previsión aplica para las personas jurídicas extranjeras con domicilio o sucursal en Colombia, las cuales deben acreditar este requisito respecto del personal vinculado en Colombia

7.3.2 PERSONAS NATURALES

La proponente persona natural, debe acreditar la afiliación a los sistemas de seguridad social en salud y pensiones, aportando los certificados de afiliación respectivos o con el certificado de pago de la correspondiente planilla.

Los certificados de afiliación se deben presentar con fecha de expedición no mayor a treinta (30) días calendario, anteriores a la fecha del cierre del proceso de contratación. En caso de modificarse la fecha de cierre del proceso, se tendrá como referencia para establecer el plazo de vigencia de los certificados de afiliación la fecha originalmente establecida en el pliego de condiciones definitivo.

La persona natural que reúna los requisitos para acceder a la pensión de vejez, o se pensione por invalidez o anticipadamente, presentará el certificado que lo acredite y, además, la afiliación al sistema de salud.

Esta misma previsión aplica para las personas naturales extranjeras con domicilio en Colombia las cuales deberán acreditar este requisito respecto del personal vinculado en Colombia.

7.4 ANTECEDENTES DISCIPLINARIOS, FISCALES, JUDICIALES Y SISTEMAS DE MEDIDAS CORRECTIVAS Y REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS - REDAM.

De conformidad con lo consagrado en el artículo 60 Ley 610 de 2000, en el parágrafo primero del artículo 42 de la Ley 1952 de 2019, y la Ley 1238 de 2008, ningún proponente, ni los integrantes de Consorcios o Uniones Temporales, nacionales o extranjeros, con domicilio en Colombia, podrán estar registrados en el Boletín de Responsabilidad Fiscal de la Contraloría General de la República vigente a la fecha de cierre del presente proceso de selección, ni presentar sanciones, que impliquen inhabilidad para contratar con el Estado.

Con la presentación de la oferta se entenderá que ni el proponente ni los integrantes de la estructura plural están incursos en las situaciones antes señaladas, sin perjuicio de que el INVÍAS efectúe la respectiva verificación tanto en el Boletín de Responsabilidad Fiscal de la Contraloría General de la República como en la página web de la Procuraduría General de la Nación.

La Entidad debe consultar los Antecedentes Judiciales en línea en los registros de las bases de datos, al igual que los Antecedentes Fiscales, acorde con el artículo 60 de la Ley 610 de 2000, los Antecedentes Disciplinarios, según el artículo 1 de la Ley 1238 de 2008 y el Registro Nacional de Medidas Correctivas del Ministerio de Defensa Nacional – Policía Nacional, de acuerdo con lo dispuesto en el artículo 183 de la Ley 1801 de 2016 –Código Nacional de Seguridad y Convivencia. De igual manera, la persona natural o el representante de la persona jurídica que se presente al proceso deberá remitir el certificado de Registro de Deudores Alimentarios Morosos- REDAM. En el caso de consorcios o uniones temporales, se realizarán las mismas verificaciones para cada uno de sus integrantes.

7.5GARANTÍA DE SERIEDAD DE LA PROPUESTA

El proponente debe presentar con la propuesta una garantía de seriedad de la oferta que cumpla con los parámetros, condiciones y requisitos que se indican en este numeral.

Cualquier error o imprecisión en el texto de la garantía presentada, será susceptible de aclaración por el proponente hasta el término de traslado del informe de evaluación.

Las características de las garantías son las siguientes:

Característica	Condición
Clase	Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) contrato de seguro contenido en una póliza, (ii) patrimonio autónomo y (iii) garantía Bancaria.
Asegurado/ beneficiario	Instituto Nacional de Vías identificada con NIT 800.215.807 -2.
Amparos	Los perjuicios derivados del incumplimiento del ofrecimiento en los eventos señalados en el artículo 2.2.1.2.3.1.66 del Decreto 1082 de 2015.
Vigencia	3 meses contados a partir de la fecha de cierre del proceso de contratación.

Valor asegurado	Se deberá presentar garantía de seriedad de la oferta de por lo menos del diez (10%) del presupuesto oficial del proceso de selección.
Tomador	• Para las personas jurídicas: la garantía deberá tomarse con el nombre o razón social y tipo societario que figura en el certificado de existencia y representación legal expedido por la Cámara de Comercio respectiva, y no solo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera. • Para los proponentes plurales: la garantía deberá ser otorgada por todos los integrantes del proponente plural, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de la misma.

Si en desarrollo del proceso de selección se modifica el cronograma, el proponente deberá ampliar la vigencia de la garantía de seriedad de la oferta hasta tanto no se haya perfeccionado y cumplido los requisitos de ejecución del respectivo contrato.

La propuesta tendrá una validez igual al término de vigencia establecido para la garantía de seriedad de la oferta. Durante este período la propuesta será irrevocable, de tal manera que el proponente no podrá retirar ni modificar los términos o condiciones de la misma, so pena de que la entidad pueda hacer efectiva la garantía de seriedad de la oferta.

NOTA: Se aplicarán las reglas descritas en el art 5 de la ley 1882 de 2018 parágrafo 3° el cual reza a la letra lo siguiente***: Parágrafo 3°. La no entrega de la garantía de seriedad junto con la propuesta no será subsanable y será causal de rechazo de la misma*.**

7.6 DOCUMENTO DE IDENTIDAD

El proponente individual persona natural, el representante legal del proponente individual persona jurídica, el representante legal de la estructura plural y las personas naturales integrantes de la estructura plural deberán aportar fotocopia de la cédula de ciudadanía, o cédula de extranjería, o pasaporte.

7.7 PROPONENTES PLURALES

Cada uno de los integrantes del proponente plural debe acreditar por separado los requisitos de que tratan los numerales anteriores.

7.8 REQUISITOS HABILITANTES FINANCIEROS

7.8.1 REQUISITOS HABILITANTES DE CARÁCTER FINANCIERO Y ORGANIZACIONAL:

Estos requisitos exigidos por la Entidad obedecen para que los posibles oferentes tengan la disponibilidad de recursos suficientes y las garantías de orden financiero que permitan de un lado, atender el objeto del contrato de acuerdo con el presupuesto oficial y de otro modo garantizar una estabilidad financiera del contrato.

Considerando los principios de la contratación pública consagrados en la Ley 80 de 1993, la Entidad está interesada en que sus contratistas estén en condiciones de generar flujos de caja suficientes que les permitan cubrir ágilmente los eventos relacionados al objeto de los proyectos a contratar. De tal forma que le permite a la administración, mitigar el riesgo de dilación en la ejecución de los contratos por falta de liquidez, dado que la liquidez, tiene relación directa con la capacidad de la empresa de generar flujo de caja.

Por ello, en aras de otorgarle mayor pluralidad de oferentes a este proceso, se tendrán en cuenta los indicadores financieros que se relacionan a continuación, los cuales deberán cumplir los proponentes que se presenten, y ofrezcan las garantías financieras y de capacidad organizacional que anticipen una buena ejecución contractual por parte del proponente adjudicatario.

7.8.2 INDICADORES DE CAPACIDAD FINANCIERA

Con base en el análisis del sector realizado por la entidad, y con el ánimo que exista pluralidad de oferentes, los proponentes que pretenden presentar oferta en marco del proceso de selección, deben acreditar como requisito habilitante de Capacidad Financiera, los siguientes indicadores:

- **ÍNDICE DE LIQUIDEZ:**

  FORMULA:

  LIQUIDEZ: $\frac{\text{Activo Corriente}}{\text{Pasivo Corriente}}$ **≥ 1,58 vez**

- **ÍNDICE DE ENDEUDAMIENTO:**

  FORMULA:

  NIVEL DE ENDEUDAMIENTO: $\frac{\text{Pasivo Total}}{\text{Activo Total}}$ **<= 60%**

- **ÍNDICE DE RAZON DE COBERTURA DE INTERESES:**

FORMULA:

RAZON DE COBERTURA DE INTERESES: $\frac{\text{Utilidad Operacional}}{\text{Gastos Interes}}$ **. ≥ 2,48 veces**

<u>Si el proponente es plural cada indicador debe calcularse así:</u>

$$\text{Indicador} = \frac{(\sum_{i=1}^{n} \text{Componente 1 del indicador}_i)}{(\sum_{i=1}^{n} \text{Componente 2 del indicador}_i)}$$

Donde n es el número de integrantes del proponente plural (unión temporal o consorcio).

El proponente que no tiene pasivos corrientes está habilitado respecto del índice de liquidez.

Nota: Al realizar la verificación de la razón de cobertura de interés, si el oferente no presenta obligaciones financieras, registrando el saldo de su cuenta de Gastos por Interés en cero ($0); y el resultado indique INDETERMINADO, se establecerá como CUMPLE en la evaluación financiera, para el caso del indicador en mención.

CAPITAL DE TRABAJO:

Este indicador representa la liquidez operativa del proponente, es decir el remanente del proponente luego de liquidar sus activos corrientes (convertirlos en efectivo) y pagar el pasivo de corto plazo. Un capital de trabajo positivo contribuye con el desarrollo eficiente de la actividad económica del proponente. Es recomendable su uso cuando la Entidad Estatal requiere analizar el nivel de liquidez en términos absolutos.

El capital de trabajo es la medida de efectivo y activos líquidos disponibles para financiar las operaciones diarias de una empresa. Tener esta información puede ayudar a administrar el contrato y tomar buenas decisiones.

Mediante el cálculo del capital de trabajo, se determinará por cuánto tiempo el oferente puede cumplir con las obligaciones del contrato. Una empresa con un capital muy bajo o nulo probablemente no tenga la capacidad para ejecutar los servicios. Calcular el capital de trabajo también es útil para evaluar si una empresa hace un uso eficaz de sus recursos.

Por lo anteriormente expuesto, los proponentes que pretenden presentar oferta en marco del proceso de selección deben acreditar como requisito habilitante, un indicador de Capital de Trabajo **mayor o igual al 70% del presupuesto oficial del proceso.**

FORMULA = ACTIVO CORRIENTE – PASIVO CORRIENTE

CAPITAL DE TRABAJO: DEBERÁ SER MAYOR O IGUAL (≥70%) DEL PRESUPUESTO OFICIAL DEL PROCESO.

Si el proponente es plural el indicador debe calcularse así:

$$\text{CTProponente plural} = \sum_{i=1}^{n} \text{CT}_i$$

7.8.3 INDICADORES DE CAPACIDAD ORGANIZACIONAL

Con base en el análisis del sector realizado por la entidad, y con el ánimo que exista pluralidad de oferentes, los proponentes que pretenden presentar oferta en marco del proceso de selección, deben acreditar como requisito habilitante de Capacidad Organizacional los siguientes indicadores:

- **RENTABILIDAD DEL PATRIMONIO (ROE)**

FORMULA:

ROE = *UTILIDAD OPERACIONAL* ≥ 13%
PATRIMONIO

- **RENTABILIDAD DEL ACTIVO (ROA)**

FORMULA:

ROA = *UTILIDAD OPERACIONAL* ≥ 9%
ACTIVO TOTAL

Si el proponente es plural cada indicador debe calcularse así:

$$\text{Indicador} = \frac{(\sum_{i=1}^{n} \text{Componente 1 del indicador}_i)}{(\sum_{i=1}^{n} \text{Componente 2 del indicador}_i)}$$

Donde *n* es el número de integrantes del proponente plural (unión temporal o consorcio).

7.8.4 ACREDITACION DE LA CAPACIDAD FINANCIERA Y ORGANIZACIONAL

7.8.4.1 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.

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 en el siguiente numeral.

7.8.4.2 PERSONAS NATURALES O JURÍDICAS EXTRANJERAS SIN DOMICILIO O SUCURSAL EN COLOMBIA

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, indicando la taza de conversión de estos, debidamente firmados por el contador colombiano que los hubiere convertido

B. Copia de la tarjeta profesional del Contador Público o Revisor Fiscal y certificado de

antecedentes disciplinarios vigentes a la fecha de cierre del proceso expedido por la Junta Central de Contadores de quien realiza la conversión.

C. El Formato acreditación– Capacidad financiera y organizacional para extranjeros debidamente diligenciado (FORMATO 6. CAPACIDAD FINANCIERA Y ORGANIZACIONAL PARA PROPONENTE EXTRANJERO) En caso de presentarse discrepancias entre la información consignada en el Formato acreditación – Capacidad financiera y organizacional para extranjeros y los documentos señalados en el Literal A, prevalecerá la información consignada en los estados financieros incluidos en la oferta.

Las fechas de corte de los documentos señalados en el literal A, serán al 31 de diciembre de 2025 acompañado del Informe de Auditoría, salvo que se acredite en debida forma que la legislación propia del país de origen establece una fecha de corte diferente a la prevista en este pliego.

Si alguno de estos requerimientos no aplica en el país del domicilio del proponente extranjero, el Representante Legal o el apoderado en Colombia deberán hacerlo constar bajo la gravedad de juramento en el Formato acreditación – Capacidad financiera y organizacional para extranjeros. El Proponente podrá acreditar este requisito con un documento que así lo certifique emitido por una firma de auditoría externa.

7.8.4.3 REQUISITOS PARA PRESENTACIÓN DE MONEDA EXTRANJERA

La información deberá ser presentada en pesos de Colombia, en este orden, cuando los Estados Financieros estén expresados en monedas extranjeras deberán convertirse a pesos colombianos, siguiendo el procedimiento que a continuación se describe:

1. Si está expresado originalmente en dólares de los Estados Unidos de Norte América los valores se convertirán a pesos colombianos, utilizando para ello el valor de la tasa representativa del mercado (TRM) correspondiente a la fecha de cierre del balance, certificadas por el Banco de la República, para lo cual el proponente deberá indicar la tasa representativa del mercado utilizada para la conversión.

2. Si los valores del contrato están expresados originalmente en una moneda diferente a Dólares de los Estados Unidos de América, estos deberán convertirse inicialmente a esta moneda, utilizando para ello el valor correspondiente a las tasas de cambio vigentes entre el dólar y dicha moneda a la fecha de cierre del balance (utilizando para tal efecto la página web https://www.oanda.com/lang/es/currency/converter/). Hecho esto, se procederá en la forma señalada en el numeral anterior.

NOTA: En el caso de contratos ejecutados antes de la entrada en vigencia del EURO, el valor ejecutado se debe acreditar en la moneda que se encontraba vigente a la fecha de terminación del contrato.

8 REQUISITOS HABILITANTES TÉCNICOS

1. **CUMPLIMIENTO DEL ANEXO TÉCNICO:** El proponente persona jurídica o proponente plural o proponente persona natural, deberá allegar el **FORMATO 3 – CUMPLIMIENTO ANEXO FICHA TÉCNICA** debidamente suscrito por el representante legal del proponente, por el cual acredita y se compromete a dar cumplimiento en su totalidad a las especificaciones técnicas de verificación y de obligatorio cumplimiento descritas en dicho documento, así como las demás obligaciones contenidas los documentos que componen la etapa de planeacion.

2. **CERTIFICACIÓN DE DISTRIBUIDOR AUTORIZADO**

   El proponente deberá aportar, con su propuesta, una certificación expedida por cada uno de los fabricantes de las plataformas principales del ecosistema de ciberseguridad ofertado (SIEM, SOAR/IRP, AntiDDoS y NAC), en la que conste:

   a) Que el oferente es distribuidor autorizado del software para Colombia.
   b) Que se encuentra registrado y vigente en el los dos máximos niveles del programa de partners del fabricante.

   c) Que dicho nivel acredita capacidad autorizada para prestar servicios profesionales y soporte técnico de primer y segundo nivel sobre sus plataformas.

   d) La relación de los productos ofertados.

   e) Que cuenta con especialización técnica vigente, expedida por el fabricante, en al menos cuatro (4) de las siguientes áreas, entre las cuales deberán incluirse obligatoriamente la LAN segura y la tecnología operativa (OT): seguridad de redes y firewall; redes de área local seguras (LAN segura); seguridad de tecnología operativa (OT); operación de centros de seguridad (Security Operations); acceso seguro en el borde del servicio (SASE); redes de área extensa definidas por software (SD-WAN); y seguridad en la nube (Cloud Security).

   La certificación deberá tener fecha de expedición no mayor a treinta (30) días anteriores a la fecha de cierre del proceso de selección y estar vigente al momento de presentar la

oferta. Si un mismo fabricante provee varias de las plataformas, bastará una sola certificación que las relacione.

En caso de uniones temporales o consorcios, cualquiera de los integrantes podrá aportar la certificación donde se demuestre el cumplimiento según las características antes mencionadas.

NOTA 1: Las certificaciones expedidas en idioma extranjero deberán acompañarse de traducción oficial al castellano, sin perjuicio de que inicialmente se aporten con traducción simple. La ausencia de traducción oficial será subsanable dentro del término otorgado por la Entidad, que deberá vencer antes del inicio de la subasta. Si el proponente no atiende el requerimiento dentro de dicho término, se rechazará su oferta por no acreditar el requisito habilitante. La subsanación no podrá acreditar circunstancias ocurridas después del cierre del proceso

NOTA 2: Para el caso de la acreditación de CERTIFICACIÓN DE DISTRIBUIDOR AUTORIZADO, de Proponentes Plurales, es suficiente la acreditación por parte de uno de los integrantes.

JUSTIFICACIÓN DE LA SOLICITUD DE LA CERTIFICACIÓN: De manera previa a la justificación específica de cada exigencia, es necesario precisar el fundamento que sustenta, en conjunto, la totalidad de los requisitos habilitantes de orden técnico del presente proceso. Dada la naturaleza del objeto contractual —la operación de un Centro de Operaciones de Seguridad sobre infraestructura crítica de transporte del orden nacional, con acceso directo a información institucional sensible, credenciales privilegiadas y sistemas misionales— y considerando que el presente proceso se adelanta bajo la modalidad de subasta inversa, en la cual, una vez superada la etapa de habilitación, la adjudicación se define exclusivamente por el menor precio ofertado, la totalidad de la valoración sobre la idoneidad, la capacidad técnica y la trayectoria del futuro contratista debe concentrarse necesariamente en la etapa de verificación de requisitos habilitantes, por ser esta la única fase del proceso en la que dicha idoneidad puede ser evaluada.

Los riesgos derivados de contratar a un proponente sin la competencia técnica real para operar un SOC de esta criticidad no pueden ser mitigados con posterioridad a la adjudicación ni compensados por un menor precio, motivo por el cual la exigencia de certificaciones expedidas por terceros técnicos independientes —fabricantes, organismos de certificación acreditados y organizaciones internacionales de reconocimiento técnico— no constituye una preferencia discrecional de la entidad, sino el mecanismo

idóneo y proporcional para acreditar objetivamente dicha idoneidad desde esta única etapa disponible para ello.

Este fundamento encuentra respaldo directo en el artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015, que exige que los requisitos habilitantes de todo proceso de contratación pública sean adecuados y proporcionales a la naturaleza del contrato a suscribir y a su valor, así como en el deber de selección objetiva consagrado en el artículo 5 de la Ley 1150 de 2007, que impone a la entidad estatal la obligación de escoger el ofrecimiento más favorable únicamente entre proponentes que hayan demostrado, de manera verificable, la capacidad de ejecutar el objeto contractual en condiciones que protejan el interés público.

La jurisprudencia del Consejo de Estado ha reiterado que la proporcionalidad de un requisito habilitante se mide precisamente frente a los riesgos reales y específicos del contrato que se pretende celebrar, y no frente a un estándar genérico aplicable a cualquier proceso — estándar que, en el presente caso, exige un nivel de exigencia superior al ordinario, dado que el objeto contractual involucra directamente la protección de infraestructura crítica nacional y se estructura precisamente como respuesta a un incidente de ciberseguridad ya materializado contra la propia entidad.

Sobre esta base, la exigencia de certificación de distribuidor autorizado del software para Colombia, en el nivel máximo del programa de partners del fabricante, minimiza el riesgo de que el proponente carezca de la mayor capacidad de implementación disponible en el mercado para el ecosistema tecnológico ofertado. Dado que en la subasta inversa la adjudicación recae en el menor precio entre habilitados, esta exigencia garantiza que la totalidad de los competidores por precio cuenten con la curva de implementación más corta y confiable posible, minimizando el riesgo de retrasos en la puesta en producción del SOC y de fallas de configuración derivadas de experiencia insuficiente, riesgo cuya materialización resultaría especialmente grave considerando el antecedente del incidente de ciberseguridad de diciembre de 2025.

La exigencia de que el oferente esté en capacidad de proveer servicios profesionales autorizados por el fabricante minimiza el riesgo de que la entidad contrate con un proponente que, contando con relación comercial de reventa, carezca de la capacidad técnica real para implementar, configurar y operar las plataformas contratadas.

Respecto de las especialidades técnicas exigidas, cada una responde a un riesgo concreto y verificable derivado de la infraestructura específica del INVIAS y no a una lista genérica de la industria. La especialización en **seguridad de redes y firewall** minimiza el riesgo de que el proponente carezca de dominio técnico sobre la tecnología de seguridad perimetral que ya opera en la entidad y que deberá integrarse como fuente primaria del SIEM, exponiendo a la entidad a una correlación de eventos deficiente desde el primer día de operación. La especialización en **LAN segura** minimiza el riesgo de que

la segmentación de red prometida por la solución de control de acceso a la red (NAC) no se materialice en la práctica, dado que dicha segmentación depende de la interacción técnica entre el NAC y los switches y puntos de acceso inalámbrico de la entidad —precisamente la condición de segmentación insuficiente que facilitó la propagación del incidente de diciembre de 2025. La especialización en **seguridad de tecnología operativa (OT)** minimiza el riesgo de que los dispositivos de Internet de las Cosas conectados de manera creciente a la red del INVIAS —cámaras, sensores, sistemas de control de acceso físico— queden sin un tratamiento de seguridad técnicamente diferenciado, dado que dichos dispositivos no admiten agentes de seguridad tradicionales. La especialización en **operación de centros de seguridad (Security Operations)** minimiza el riesgo de que el proponente no cuente con la madurez operativa necesaria para sostener un servicio de monitoreo 24×7×365 con los niveles de escalamiento, triaje y acuerdos de servicio exigidos en la ficha técnica, más allá de la sola posesión de las plataformas tecnológicas. La especialización en **acceso seguro en el borde del servicio (SASE)** minimiza el riesgo de aplicación inconsistente de políticas de seguridad sobre la sede principal y las veintiséis (26) direcciones territoriales del INVIAS, distribuidas en todo el territorio nacional. La especialización en **redes de área extensa definidas por software (SD-WAN)** minimiza el riesgo de que el proponente no cuente con la competencia técnica para integrar de manera segura la conectividad entre sedes que la entidad ya opera bajo esta tecnología, conforme a lo descrito en los antecedentes de contratación del presente estudio. Y la especialización en **seguridad en la nube (Cloud Security)** minimiza el riesgo de protección insuficiente de las cargas de trabajo que el INVIAS mantiene desplegadas en la nube pública de Microsoft Azure, entorno que forma parte integral de la infraestructura híbrida objeto de protección del presente proceso.

Sobre la exigencia de membresía FIRST, es necesario precisar que el Forum of Incident Response and Security Teams no es un gremio comercial ni una asociación de mercadeo, sino la organización internacional de mayor reconocimiento técnico en la coordinación de la respuesta a incidentes de ciberseguridad a nivel mundial, de la cual el colCERT —ente coordinador nacional de ciberseguridad y ciberdefensa de Colombia, creado en el marco del CONPES 3701 de 2011— es miembro pleno desde el año 2013.

Exigir esta membresía, con antigüedad mínima de tres (3) años, minimiza el riesgo de que el operador del SOC carezca de acceso a los canales de intercambio de inteligencia de amenazas de alcance internacional que FIRST reserva exclusivamente para sus miembros; el riesgo de que, ante un incidente que deba escalarse al ente coordinador nacional, no exista articulación técnica ágil con el colCERT; y el riesgo de contratar a un operador cuya madurez operativa no haya sido evaluada por un tercero técnico independiente, dado que la admisión a FIRST exige verificación externa de capacidades reales y no una simple declaración del interesado. Esta exigencia encuentra respaldo en el modelo de gobernanza de seguridad digital establecido en el Decreto 338 de 2022, que

reconoce expresamente al colCERT como la instancia de coordinación nacional con la cual las entidades públicas deben articularse ante eventos de ciberseguridad.

Sobre la exigencia de certificación ISO/IEC 27001:2022, debe precisarse que esta norma no corresponde a un sistema de gestión de calidad, sino específicamente a un **Sistema de Gestión de Seguridad de la Información**, cuyo objeto es la identificación, evaluación y tratamiento sistemático de los riesgos que afectan la confidencialidad, la integridad y la disponibilidad de la información de una organización. Se trata del estándar internacional pertinente para evaluar objetivamente si un proponente gestiona su propia seguridad de la información —y, por extensión, la de la entidad cuya infraestructura operará— bajo un esquema auditado externamente por un organismo de certificación acreditado.

Esta exigencia encuentra fundamento legal directo en la Resolución 500 de 2021, mediante la cual el Ministerio de Tecnologías de la Información y las Comunicaciones adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital, modelo fundamentado expresamente en los requisitos y controles de la norma ISO/IEC 27001. Al exigir que el alcance certificado del proponente cubra específicamente los servicios de operación de SOC o de seguridad gestionada objeto del presente contrato, la entidad minimiza el riesgo de contratar a un operador cuyo certificado corresponda a una línea de negocio distinta y ajena a la actividad que efectivamente prestará al INVIAS.

La concentración de esta exigencia en la etapa de habilitación resulta, además, la única alternativa jurídicamente disponible para la entidad bajo la modalidad de subasta inversa seleccionada, dado que una vez superada dicha etapa, el precio se convierte en el criterio exclusivo de adjudicación, sin que exista posibilidad posterior de ponderar la idoneidad técnica del proponente.

En consecuencia, la OTIC considera que los requisitos habilitantes aquí desarrollados constituyen el mecanismo proporcional, objetivo y jurídicamente idóneo para que el INVIAS contrate un servicio de ciberseguridad gestionada con la garantía razonable de que quien resulte adjudicatario cuenta con la capacidad técnica real para proteger la infraestructura crítica de la entidad, minimizando los riesgos que la propia experiencia institucional reciente ha demostrado que no pueden asumirse nuevamente.

8.1EXPERIENCIA ESPECÍFICA REQUERIDA.

En el presente proceso de selección los proponentes acreditarán su experiencia a través de la información consignada en el certificado del Registro Único de Proponentes (para personas naturales y jurídicas nacionales y extranjeras con domicilio en Colombia), relacionando, en el formulario respectivo, la experiencia que pretendan hacer valer en el presente proceso, en donde se acrediten MÁXIMO CINCO (5) contratos terminados cuya ejecución o cuyo objeto y/o actividades

dentro del mismo hayan sido o se encuentren relacionadas con:

" PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD Y/O CIBERSEGURIDAD GESTIONADA Y/O SEGURIDAD INFORMÁTICA Y/O ADMINISTRACIÓN Y/O OPERACIÓN DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y/O MONITOREO Y CORRELACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y/O GESTIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA Y/O SUMINISTRO Y/O RENOVACIÓN Y/O IMPLEMENTACIÓN Y/O INSTALACIÓN Y/O CONFIGURACIÓN Y/O INTEGRACIÓN Y/O ADMINISTRACIÓN Y/O MANTENIMIENTO Y/O SOPORTE DE SOLUCIONES DE CIBERSEGURIDAD, SEGURIDAD PERIMETRAL, PROTECCIÓN DE REDES, SISTEMAS, APLICACIONES Y DATOS, DETECCIÓN Y RESPUESTA EN ENDPOINTS, GESTIÓN DE VULNERABILIDADES, INTELIGENCIA DE AMENAZAS, MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (AntiDDoS), FIREWALL DE APLICACIONES WEB (WAF) Y/O CONTROL DE ACCESO A LA RED (NAC) *".*

La sumatoria del valor de los contratos válidos para la acreditación de la experiencia, expresado en SMMLV, debe ser igual o mayor al cien por ciento (100%) del presupuesto oficial. El valor de los contratos para efectos de evaluación será el indicado en el RUP, expresado en SMMLV.

NOTA 1: La experiencia será validada mediante los documentos establecidos en el presente proceso, a partir del objeto contractual y/o alcance, siempre y cuando este se enmarque o se encuentre relacionado con las exigencias indicadas arriba; de igual forma la experiencia podrá acreditarse mediante actividades ejecutadas descritas en los documentos establecidos en el numeral 4.4.5 del Pliego de Condiciones (DOCUMENTOS VÁLIDOS PARA LA ACREDITACIÓN DE LA EXPERIENCIA).

NOTA 2: Para efectos de la validez de la oferta de los proponentes plurales se tendrá en cuenta lo siguiente: todos los integrantes deben acreditar experiencia valida en los términos del pliego de condiciones al menos el diez por ciento (10%) de la experiencia requerida expresada en SMMLV. Ninguno de los integrantes del proponente plural estará exento de aportar contratos válidos para la acreditación de la experiencia. Es decir que al final de la evaluación todos los integrantes del proponente plural deberán contar con al menos un contrato valido de mínimo el diez por ciento (10%) del PO y en total los contratos validos aportados por el proponente plural superen el cien por ciento 100% del PO.

NOTA 3: Para efectos de la acreditación de la experiencia requerida en el presente proceso no se aceptarán SUBCONTRATOS.

NOTA 4: las autocertificaciones del propio proponente, integrantes o grupo empresarial no sirven

para demostrar la experiencia.

NOTA 5: Si los contratos incumplen cualquiera de las condiciones requeridas, NO SERÁN tenidos en cuenta para la evaluación.

NOTA 6: Los valores de los documentos aportados en la propuesta deben presentarse en pesos colombianos. Cuando un valor se exprese en moneda extranjera debe convertirse a pesos colombianos teniendo en cuenta lo siguiente:

I. Si los valores de un contrato están expresados originalmente en Dólares de los Estados Unidos de América, los valores se convertirán a pesos colombianos, utilizando el valor correspondiente al promedio entre la TRM de la fecha de inicio del contrato y la TRM de la fecha de terminación del contrato. Para esto, el proponente deberá indicar la tasa representativa del mercado utilizada para la conversión de cada contrato en el Formulario 3 - Experiencia; la TRM utilizada será la certificada por la Superintendencia Financiera de Colombia.

II. Si los valores del contrato están expresados originalmente en una moneda diferente a dólares de los Estados Unidos de América, estos deberán convertirse inicialmente a esta moneda, utilizando para ello el valor correspondiente al promedio entre la tasa de cambio de la fecha de inicio del contrato y la tasa de cambio de la fecha de terminación del contrato. Para tales efectos, se puede utilizar la información certificada por el Banco de la República. Para el cálculo se recomienda acudir al siguiente link: https://www.oanda.com/lang/es/currency/converter/ Hecho esto, se procederá en la forma señalada en el numeral anterior.

- Conversión a Salarios Mínimos Mensuales Legales Vigentes (SMMLV)

Cuando los Documentos del proceso señalen que un valor debe expresarse en Salarios Mínimos Mensuales Legales Vigentes (SMMLV) se seguirá el siguiente proceso:

i. Los valores convertidos a pesos colombianos, aplicando el proceso descrito en el literal anterior, o cuya moneda de origen sea el peso colombiano, deben convertirse a SMMLV, para lo cual se emplearán los valores históricos de SMMLV señalados por el Banco de la República (http://www.banrep.gov.co/es/mercado-laboral/salarios), del año correspondiente a la fecha de terminación del contrato.

ii. Los valores convertidos a SMMLV, se deben ajustar a la unidad más próxima de la siguiente forma: hacia arriba para valores mayores o iguales a cero puntos cinco (0.5) y hacia abajo para valores menores a cero punto cinco (0.5).

Si el proponente aporta documentos en los que no indican el día, sino solamente el mes y el año, se

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

procederá así:

- Fecha (mes, año) de suscripción y/o inicio del contrato: se tendrá en cuenta el último día del mes señalado en la documentación válida aportada.

- Fecha (mes, año) de terminación del contrato: se tendrá en cuenta el primer día del mes señalado en la documentación válida aportada.

CLASIFICACIÓN UNSPSC

Los contratos aportados para efectos de acreditación de experiencia deben encontrarse clasificados en el "Clasificador de Bienes, Obras y Servicios de las Naciones Unidas" ***hasta el tercer nivel***, en alguna de las siguientes clasificaciones de la tabla que se relaciona a continuación:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	PRODUCTOS
43233203	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Software	Software de seguridad y protección	**Software de manejo de seguridad de red o de redes privadas virtuales VPN**
43233205	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Software	Software de seguridad y protección	**Software de seguridad de transacciones y de protección contra virus**
43232908	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Software	Software de red	**Software de interruptor o enrutador**
43222605	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Equipos o plataformas y accesorios de redes	Equipo de servicio de red	**Puerta de acceso de redes**
81111801	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	**Seguridad de los computadores, redes o internet**

81111808	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	**Servicio de análisis de sistemas**
81111809	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	**Servicio de instalación de sistemas**
81111811	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	**Servicios de soporte técnico o de mesa de ayuda**
81111508	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Ingeniería de software o hardware	**Servicios de implementación de aplicaciones**

La acreditación de los Códigos de Clasificación relacionados con los bienes, obras o servicios ejecutados será verificada, según corresponda, así:

Para las PERSONAS NATURALES Y JURÍDICAS NACIONALES Y EXTRANJERAS CON DOMICILIO EN COLOMBIA, cada uno de los contratos aportados para efectos de acreditación de la EXPERIENCIA REQUERIDA, deben encontrarse inscritos en el Registro Único de Proponentes – RUP, y se deberá relacionar en el **FORMULARIO No. 3 DE EXPERIENCIA** el número consecutivo del reporte en el RUP.

8.2CONSIDERACIONES PARA LA VALIDEZ DE LA EXPERIENCIA REQUERIDA

Con el fin que la experiencia acreditada sea validada como experiencia requerida se deben cumplir los siguientes requisitos:

1. En caso de que el proponente relacione o anexe más de un formulario para obtener calificación de hábil por el factor de experiencia, únicamente se tendrá en cuenta el más reciente y de este

se tomarán los primeros **CINCO (5)** contratos terminados de mayor valor.

2. En caso de que el proponente relacione o anexe un número superior a **CINCO (5)** contratos, para efectos de evaluación de la experiencia, únicamente se tendrán en cuenta los **CINCO (5)** contratos terminados de mayor valor relacionados en el Formulario de experiencia.

3. Cuando los documentos considerados como válidos para acreditar la experiencia aportados por el proponente generen dudas a la entidad respecto del cumplimiento de los requisitos de experiencia exigidos, el proponente podrá presentar ACLARACIONES aportando documentos que den alcance al objeto del contrato en el cual se evidencien las actividades y obligaciones ejecutadas a fin de que la entidad realice una evaluación integral de la experiencia del proponente.

4. En caso de que el proponente no aporte el **FORMULARIO 3 DE EXPERIENCIA**, para efectos de la verificación del cumplimiento de requisitos habilitantes, se tendrán en cuenta los **CINCO (5)** contratos de mayor valor.

5. Cuando el contrato que se pretende acreditar como experiencia especifica haya sido ejecutado en consorcio o unión temporal, deberá relacionar en el Formulario de EXPERIENCIA el porcentaje del participación del integrante en la ejecución del contrato que se quiera hacer valer dentro del proceso y además, dicho porcentaje de participación deberá venir especificado claramente en uno o algunos de los documentos que se establecen como válidos para efectos de acreditación de experiencia, en el presente pliego de condiciones.

6. Si el contrato aportado para acreditar la experiencia se ejecutó bajo la modalidad de consorcio o unión temporal, el valor a considerar será el equivalente al porcentaje de participación que tuvo el integrante o los integrantes que la pretendan hacer valer.

7. Para efectos de la acreditación de experiencia de contratos que hayan sido objeto de cesión antes de la ejecución del 50% de la ejecución total, se admitirán como experiencia para el cesionario y no se reconocerá experiencia alguna por ellos al cedente, esta situación deberá ser certificada en uno o alguno de los documentos considerados como válidos para efectos de acreditación de experiencia en el presente pliego de condiciones. En caso de que la cesión se haya producido después del cincuenta (50%) por ciento de ejecución del valor del contrato no se admitirá como experiencia ni para el cedente, ni para el cesionario.

8. En el evento que un contrato que se aporte para la experiencia haya sido ejecutado por un Consorcio o Unión Temporal, y dos (2) o más de sus integrantes conformen un proponente plural para participar en el presente proceso, dicho contrato se entenderá aportado como un (1)

solo contrato y se tendrá en cuenta para el aporte de la experiencia, la sumatoria de los porcentajes de los integrantes del Consorcio o Unión Temporal que ejecutaron el contrato, y que están participando en el presente proceso. Cuando se presente este caso se tendrá en cuenta el contrato en la totalidad de la participación de los integrantes que conformaron el proponente plural que adquirió la experiencia y que se encuentren participando en el presente proceso de selección.

9. Cuando en la revisión del formulario se encuentren errores de trascripción en cifras, en fechas, en números o en letras, prevalecerá la información contenida en los soportes que acompañan dicho formulario.

10. En caso de que la entidad requiera verificar la veracidad de la información aportada para acreditar la experiencia aceptable, podrá solicitarla y el oferente está en la obligación de allegarla, de lo contrario los contratos no serán tenidos en cuenta para la verificación.

11. La información deberá ser presentada en moneda legal colombiana, en este orden, cuando el valor de los contratos este expresado en monedas extranjeras **(Y el contrato haya sido ejecutado por una persona que no tenga la obligación de estar inscrita en el RUP)** éste deberá convertirse en pesos colombianos, siguiendo el procedimiento que a continuación se describe:

    - Si está expresado originalmente en dólares de los Estados Unidos de Norte América, los valores se convertirán a pesos colombianos, utilizando para ello el valor correspondiente al promedio de las tasas representativas del mercado, certificadas por el Banco de la República, a la fecha de terminación del contrato, para lo cual el proponente deberá indicar la tasa representativa del mercado utilizada para la conversión.

    - Si está expresado originalmente en una moneda o unidad de cuenta diferente a dólares de los Estados Unidos de Norte América, deberá convertirse a esta moneda, utilizando para ello el valor correspondiente al promedio de las tasas de cambio vigentes entre el dólar y dicha moneda (utilizando para tal efecto la página web http://www.oanda.com en la pestaña Currency Converter, (Conversor de Divisas), a la fecha de terminación del contrato. Hecho esto se procederá en la forma que señala el numeral anterior.

    - Junto con el Formulario de Experiencia, debe presentarse los valores antes obtenidos, en un “Cuadro de Conversión de valores” que presente los Valores de los contratos en su moneda original, la tasa de cambio utilizada, los Valores convertidos de los Contratos en Moneda Colombiana. Así mismo, los valores facturados tanto en moneda original como en Moneda Colombiana.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

NOTA: En el caso de contratos ejecutados antes de la entrada en vigencia del EURO, el valor ejecutado se debe acreditar en la moneda que se encontraba vigente a la fecha de terminación del contrato.

8.3ACREDITACIÓN DE LA EXPERIENCIA REQUERIDA

Los Proponentes acreditarán para cada uno de los contratos aportados la siguiente información mediante alguno de los documentos señalados en el presente documento como DOCUMENTOS VÁLIDOS PARA LA ACREDITACIÓN DE LA EXPERIENCIA:

1. Contratante.
2. Objeto del contrato.
3. Principales actividades ejecutadas requeridas (en caso de que el objeto del contrato no presente relación con lo solicitado en el numeral correspondiente).
4. La fecha de iniciación de la ejecución del contrato: Esta fecha es diferente a la de suscripción del contrato, a menos que de los documentos aportados de forma expresa así se determine. Si en los documentos válidos aportados para la acreditación de experiencia solo se evidencia fecha (mes, año) de suscripción y/o inicio del contrato: se tendrá en cuenta el último día del mes que se encuentre señalado en el documento aportado.
5. La fecha de terminación de la ejecución del contrato. LA FECHA DE TERMINACION, PODRÁ SER HOMOLOGADA POR, FECHA DE RECIBO FINAL O LIQUIDACIÓN. Si en los documentos válidos aportados para la acreditación de experiencia solo se evidencia fecha (mes, año) de terminación del contrato: se tendrá en cuenta el primer día del mes que se encuentre señalado en el documento aportado.
6. Nombre y cargo de la persona que expide la certificación.

8.4DOCUMENTOS VÁLIDOS PARA LA ACREDITACIÓN DE LA EXPERIENCIA REQUERIDA

En aquellos casos en que por las características del objeto a contratar se requiera verificar información adicional a la contenida en el RUP, el Proponente podrá aportar uno o algunos de los documentos que se establecen a continuación para que la Entidad realice la verificación en forma directa. Los mismos deberán estar debidamente diligenciados y suscritos por todas las partes involucradas, principalmente la entidad contratante.

NO SE ACEPTARÁN DOCUMENTOS DIFERENTES A LOS SEÑALADOS EN EL PRESENTE NUMERAL (como, por ejemplo: minutas de contrato, anexos técnicos, actas parciales, facturas, actas de pago, resoluciones de adjudicación, links de páginas web, catálogos, informes, etc. **ESTOS NO SERÁN TENIDOS EN CUENTA PARA EFECTOS DE EVALUACIÓN**).

En caso de existir discrepancias entre dos (2) o más documentos aportados por el Proponente para la acreditación de experiencia, se tendrá en cuenta el orden de prevalencia establecido a continuación:

1. **Acta de Liquidación:**

   Debidamente diligenciada y suscrita por todas las partes involucradas, en la cual conste la información requerida en el presente pliego de condiciones para efectos de acreditación de la experiencia.

2. **Acta final o de recibo definitivo:**

   Debidamente diligenciada y suscrita por todas las partes involucradas, en la cual conste la información requerida en el presente pliego de condiciones para efectos de acreditación de la experiencia.

3. **Acta de terminación:**

   Debidamente diligenciada y suscrita por todas las partes involucradas, en la cual conste la información requerida en el presente pliego de condiciones para efectos de acreditación de la experiencia.

4. **Certificación de experiencia:**

   Expedida con posterioridad a la fecha de terminación del contrato suscrita por quien esté en capacidad u obligación de hacerlo; así mismo, debe contener la información requerida en el presente pliego de condiciones para efectos de acreditación de la experiencia.

5. **Acta de inicio o la orden de inicio:**

   La misma sólo será válida para efectos de acreditar la fecha de inicio.

6. **Contratos Cedidos:**

   Para las personas naturales o jurídicas nacionales y extranjeras domiciliadas con sucursal en Colombia, para efectos de la acreditación de experiencia de contratos que hayan sido objeto de cesión, el contrato deberá encontrarse debidamente inscrito y clasificado de conformidad con el pliego de condiciones en el Registro Único de Proponentes de la empresa cesionaria. En todo caso, la experiencia se admitirá para el cesionario y no se

reconocerá experiencia alguna al cedente, en cuyo caso la experiencia que se contabilizará será la indicada en el RUP del cesionario.

NOTA 1: En caso de existir discrepancias entre la información registrada en el **FORMULARIO No. 3 DE EXPERIENCIA** y los documentos soporte de esta, prevalecerá lo consignado en los documentos soporte. Lo anterior no aplica para el caso que uno (1) o varios de los contratos relacionados en el formulario de EXPERIENCIA, no correspondan con los soportes allegados, para este caso únicamente se tendrán en cuenta los contratos relacionados en el formulario de EXPERIENCIA.

NOTA 2: En caso de que el contrato ejecutado por personas naturales o jurídicas nacionales y extranjeras domiciliadas con sucursal en Colombia, presente discrepancias entre la información registrada en el RUP y los documentos que aporte el proponente en su oferta para acreditar dicho contrato, prevalecerá la información consignada en el RUP.

NOTA 3: Las personas que objeten la experiencia de algún otro oferente, deberán aportar los documentos que prueben sus afirmaciones; por lo tanto, no es procedente efectuar manifestaciones temerarias respecto de los documentos aportados por los demás oferentes, sin contar con medios de prueba que acrediten tales manifestaciones. Cabe agregar que la entidad propende a garantizar el principio constitucional de la buena fe.

PARA CONTRATOS SUSCRITOS ENTRE PARTICULARES:

Los documentos válidos y requeridos son los siguientes:

1. Certificación expedida con posterioridad a la fecha de terminación del contrato, la cual debe encontrarse debidamente suscrita por el representante legal o por quien esté en capacidad u obligación de hacerlo de la empresa contratante.

2. Por otra parte, dicha certificación debe acompañarse del Certificado de Cámara de Existencia y Representación Legal de la persona contratante o documento equivalente que haga sus veces en el país donde se expide el documento; la fecha de expedición del certificado debe ser no mayor a treinta (30) días anteriores a la fecha de cierre del presente proceso.
3. Certificación de facturación expedida con posterioridad a la fecha de terminación del contrato emitida por el revisor fiscal o contador público del proponente que acredita la experiencia, según corresponda, con la copia de la tarjeta profesional y certificado de antecedentes disciplinarios vigente, expedido por la Junta Central de Contadores, o los documentos equivalentes que hagan sus veces en el país donde se expide el documento del profesional. debe contener la información requerida en el presente pliego de condiciones para efectos de acreditación de la experiencia.

NOTA 1: En caso de existir discrepancias entre la información registrada en el **FORMULARIO No. 3 DE EXPERIENCIA** y los documentos soporte de la misma, prevalecerá lo consignado en los documentos soporte. Lo anterior no aplica para el caso que uno (1) o varios de los contratos relacionados en el formulario de EXPERIENCIA, no correspondan con los soportes allegados, para este caso únicamente se tendrán en cuenta los contratos relacionados en el formulario de EXPERIENCIA.

NOTA 2: En caso de que el contrato ejecutado por personas naturales o jurídicas nacionales y extranjeras domiciliadas con sucursal en Colombia, presente discrepancias entre la información registrada en el RUP y los documentos que aporte el proponente en su oferta para acreditar dicho contrato, prevalecerá la información consignada en el RUP.

NOTA 3: Las personas que objeten la experiencia de algún otro oferente, deberán aportar los documentos que prueben sus afirmaciones; por lo tanto, no es procedente efectuar manifestaciones temerarias respecto de los documentos aportados por los demás oferentes, sin contar con medios de prueba que acrediten tales manifestaciones. Cabe agregar que la entidad propende a garantizar el principio constitucional de la buena fe.

NOTA 4: Los valores de los documentos aportados en la propuesta deben presentarse en pesos colombianos. Cuando un valor se exprese en moneda extranjera debe convertirse a pesos colombianos teniendo en cuenta lo siguiente:

I. Si los valores de un contrato están expresados originalmente en Dólares de los Estados Unidos de América, los valores se convertirán a pesos colombianos, utilizando el valor correspondiente al promedio entre la TRM de la fecha de inicio del contrato y la TRM de la fecha de terminación del contrato. Para esto, el proponente deberá indicar la tasa representativa del mercado utilizada para la conversión de cada contrato en el Formulario 3 - Experiencia; la TRM utilizada será la certificada por la Superintendencia Financiera de Colombia. ca

II. Si los valores del contrato están expresados originalmente en una moneda diferente a Dólares de los Estados Unidos de América, estos deberán convertirse inicialmente a esta moneda, utilizando para ello el valor correspondiente al promedio entre la tasa de cambio de la fecha de inicio del contrato y la tasa de cambio de la fecha de terminación del contrato. Para tales efectos, se puede utilizar la información certificada por el Banco de la República. Para el cálculo se recomienda acudir al siguiente link: https://www.oanda.com/lang/es/currency/converter/ Hecho esto, se procederá en la forma señalada en el numeral anterior.

- Conversión a Salarios Mínimos Mensuales Legales Vigentes (SMMLV)

Cuando los Documentos del proceso señalen que un valor debe expresarse en Salarios Mínimos Mensuales Legales Vigentes (SMMLV) se seguirá el siguiente proceso:

I. Los valores convertidos a Pesos Colombianos, aplicando el proceso descrito en el literal anterior, o cuya moneda de origen sea el peso colombiano, deben convertirse a SMMLV, para lo cual se emplearán los valores históricos de SMMLV señalados por el Banco de la República (http://www.banrep.gov.co/es/mercado-laboral/salarios), del año correspondiente a la fecha de terminación del contrato.

II. Los valores convertidos a SMMLV, se deben ajustar a la unidad más próxima de la siguiente forma: hacia arriba para valores mayores o iguales a cero punto cinco (0.5) y hacia abajo para valores menores a cero punto cinco (0.5).

Si el proponente aporta certificaciones en las que no indican el día, sino solamente el mes y el año, se procederá así:

- Fecha (mes, año) de suscripción y/o inicio del contrato: se tendrá en cuenta el último día del mes señalado en la certificación.
- Fecha (mes, año) de terminación del contrato: se tendrá en cuenta el primer día del mes señalado en la certificación.

8.3 CRITERIOS DIFERENCIALES

CRITERIOS DIFERENCIALES PARA LAS MIPYMES LOS EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD

El **Decreto 0287 de 2026** establece un sistema de preferencias para personas con discapacidad, y dispone criterios habilitantes diferenciales o ajustados en:

1. Experiencia
2. **Índices de capacidad financiera.**
3. Índices de capacidad organizacional.
4. Valor de la garantía de seriedad de la oferta.

Para MIPYMES, el artículo 2.2.1.2.4.2.18 del Decreto 1082 contempla expresamente los **índices de capacidad financiera y de capacidad organizacional** como posibles criterios diferenciales.

(…) De acuerdo con el numeral 1 del artículo 12 de la Ley 590 de 2000, según los resultados del análisis del sector, las Entidades Estatales indistintamente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos de las Mipyme domiciliadas en Colombia. Para el efecto, en función de los criterios de clasificación empresarial, los Documentos del Proceso deberán incorporar requisitos habilitantes diferenciales relacionados con alguno o algunos de los siguientes aspectos:

1. Tiempo de experiencia.
2. Número de contratos para la acreditación de la experiencia.
3. **Índices de capacidad financiera.**
4. Índices de capacidad organizacional.
5. Valor de la garantía de seriedad de la oferta.

De acuerdo con las condiciones habilitantes diferenciales previstas en la normativa aplicable para las MIPYMES y los emprendimientos y empresas de personas con discapacidad, se considera pertinente establecer criterios diferenciales en materia de capacidad financiera, teniendo en cuenta las características del presente proceso.

La selección de **indicadores de capacidad financiera** como criterio diferencial responde a la necesidad de mantener un equilibrio entre la verificación de la capacidad económica mínima requerida para la adecuada ejecución del contrato y la promoción de condiciones de participación más accesibles para las MIPYMES y los emprendimientos y empresas de personas con discapacidad.

En este sentido, se seleccionan indicadores que permiten evaluar diferentes componentes de la situación financiera de los proponentes. El **Índice de Liquidez** permite determinar la capacidad para atender obligaciones de corto plazo; el **Nivel de Endeudamiento** permite identificar el grado de apalancamiento financiero; la **Razón de Cobertura de Intereses** permite evaluar la capacidad para atender los gastos financieros con los resultados de la operación; y el **Capital de Trabajo** permite valorar la disponibilidad de recursos de corto plazo para atender las obligaciones asociadas a la ejecución contractual.

La selección de estos indicadores permite establecer condiciones habilitantes diferenciales que faciliten la participación de las MIPYMES y de los emprendimientos y empresas de personas con discapacidad, manteniendo al mismo tiempo condiciones mínimas de capacidad financiera acordes con el objeto, alcance, valor y riesgos del proceso.

CONTRATAR LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS DE CIBERSEGURIDAD PARA FORTALECER LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN, MONITOREO, CORRELACIÓN, RESPUESTA Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE SOPORTAN EL PROGRAMA DE SEGURIDAD DE CARRETERAS NACIONALES (PSCN) Y SU COMPONENTE VÍAS INTELIGENTES ITS (VIITS), MEDIANTE LA IMPLEMENTACIÓN Y OPERACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SUS SERVICIOS ASOCIADOS

Con base en el análisis efectuado, se consolidaron los valores promedio obtenidos en cada una de las fuentes consultadas (información financiera reportada por una muestra depurada de empresas de la Superintendencia de Sociedades, indicadores financieros exigidos por el INVÍAS en procesos contractuales con características similares, e indicadores financieros establecidos por otras entidades estatales en procesos de contratación adelantados a través de la plataforma SECOP II), con el propósito de establecer requisitos habilitantes acordes con las condiciones financieras del mercado, garantizando el equilibrio entre la adecuada capacidad económica de los futuros contratistas y la promoción de la pluralidad de oferentes.

Resultados de las diferentes métricas para la muestra Supersociedades

METRICA	LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD SOBRE PATRIMONIO	RENTABILIDAD SOBRE ACTIVO
MINIMO	1,1	0,19	1,1	0,06	0,04
MAXIMO	4,05	0,9	72,95	1,67	0,44
PROMEDIO	1,97	0,5	10,72	0,43	0,16
MEDIANA	1,63	0,52	3,53	0,34	0,13
MEDIA GEOMETRICA	1,86	0,47	4,94	0,32	0,13
MEDIA ARMONICA	1,76	0,43	3,21	0,23	0,11
MUESTRA	**1,76**	**52%**	**3,21**	**23%**	**16%**

Indicadores financieros exigidos por otras entidades estatales y exigidos por el INVIAS en procesos históricos

INDICADORES	INDICE DE LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
PROMEDIO INDICADORES OTRAS ENTIDADES PROCESOS SECOP II	1,47	65,0%	1,82	0,09	0,06

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844

PROMEDIO INDICADORES INVIAS	1,50	63,0%	2,40	0,07	0,05

Para la determinación de los valores diferenciales se tomaron como referencia los resultados estadísticos de las fuentes mencionadas anteriormente. En consecuencia, los valores adoptados buscan reducir el nivel de restricción de los requisitos financieros generales, sin eliminar la capacidad mínima necesaria para una adecuada ejecución contractual.

Dicho esto, y de acuerdo con el análisis de la muestra para determinar los indicadores de capacidad financiera y organizacional anteriormente expuesta, este Comité se permite establecer los indicadores de **CAPACIDAD FINANCIERA PARA CRITERIOS DIFERENCIALES PARA LAS MIPYMES LOS EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD**

CAPITAL DE TRABAJO

El Presupuesto Oficial asciende a **$ 6.030.164.927,00** En este contexto, y atendiendo las características del proceso y la necesidad de establecer condiciones habilitantes proporcionales, se determina un Capital de Trabajo equivalente al 60% del Presupuesto Oficial para las MIPYMES y los emprendimientos y empresas de personas con discapacidad, como condición diferencial orientada a facilitar su participación, manteniendo a su vez un nivel de disponibilidad de recursos que permita atender las obligaciones de corto plazo asociadas a la ejecución contractual.

El porcentaje adoptado del 60% representa una flexibilización frente al requisito general establecido para los demás proponentes, procurando equilibrar la promoción de la participación y pluralidad de oferentes con la necesidad de conservar una capacidad financiera mínima acorde con las condiciones y riesgos del contrato.

Concepto		Valor
Empresas analizadas		52
Unidad de información		Miles de pesos
Mediana del Capital de Trabajo		28.894.216
Promedio del Capital de Trabajo		37.395.193
Presupuesto Oficial		$ 6.030.164.927
Capital de Trabajo diferencial	60%	$ 3.618.098.956

Los valores adoptados fueron determinados a partir de los resultados estadísticos de la información analizada. Estos valores permiten establecer condiciones diferenciales frente a los requisitos generales, conservando referentes derivados del comportamiento financiero observado en la muestra.

CAPACIDAD FINANCIERA	ÍNDICE REQUERIDO
Índice de Liquidez: Activo Corriente/Pasivo Corriente	Mayor o igual (≥) a 1,47
Nivel de Endeudamiento: Pasivo Total / Activo Total	Menor o Igual (≤) a 52%
Razón de cobertura de intereses: Utilidad Operacional / Gastos Financieros	Mayor o Igual (>) a 1,82 o indeterminado
Capital de Trabajo: Activo Corriente - Pasivo Corriente	Mayor o igual (≥) al 60% del presupuesto del proceso

9 OBLIGACIONES DEL CONTRATISTA

9.1 OBLIGACIONES GENERALES

1. El CONTRATISTA debe constituir en favor de INVIAS, una garantía para avalar la adecuada ejecución del contrato y las obligaciones contraídas, de conformidad con lo dispuesto especialmente en el Artículo 7º de la Ley 1150 de 2007 y en el Título III de las Disposiciones Especiales del Decreto Nacional 1082 de 2015. Esta garantía deberá constituirse dentro de los tres (3) días hábiles siguientes a la suscripción del contrato y requerirá ser aprobada por el Instituto. La garantía deberá cubrir los amparos señalados en los estudios previos y el pliego de condiciones.
2. El objeto contractual deberá ejecutarse de conformidad con las finalidades y los principios de economía y transparencia, consagrados en la Ley 80 de 1993 y los postulados de la función administrativa consagrados en el artículo 209 de la Constitución Política. En desarrollo del objeto contractual el contratista se obliga a cumplir a cabalidad con las actividades que se describen en el presente contrato.
3. El contratista deberá tener en cuenta que las actividades descritas en su propuesta se prestarán bajo su exclusiva responsabilidad y, en consecuencia, deberá suministrar todos los recursos e implementos tendientes a lograr la adecuada, suficiente y eficiente prestación

del servicio que se solicita.

4. Acatar la Constitución Política, la Ley, las normas legales y procedimentales establecidas por el Gobierno Nacional y Distrital y demás normas pertinentes.
5. Cumplir con las condiciones técnicas, jurídicas, económicas, financieras y comerciales presentadas en la propuesta.
6. Responder por el pago de los tributos que se causen o llegaren a causarse por la celebración, ejecución y liquidación del contrato, cuando a esta hubiere lugar.
7. Reportar e informar al funcionario encargado del control y supervisión de la ejecución del contrato, de manera inmediata cualquier obstáculo, novedad, dificultad o anomalía que se presente en la ejecución del mismo.
8. Entregar al supervisor del Contrato los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos cuando así se requiera.
9. Acatar las instrucciones que durante el desarrollo del contrato le imparta el INVIAS, por conducto de los funcionarios que ejercerán el control de la ejecución.
10. Cumplir con las actividades y/o elementos requeridos durante la ejecución del contrato, conforme a las exigencias de los documentos precontractuales.
11. Cumplir con las condiciones pactadas en este Contrato, que solo podrán modificarse previo cumplimiento del trámite dispuesto, según el procedimiento establecido y una vez se alleguen los documentos pertinentes.
12. Mantener al INVIAS libre de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones o de las de sus subcontratistas o dependientes (si fueren autorizados). En consecuencia, EL CONTRATISTA mantendrá indemne al INVIAS contra todo reclamo, demanda, acción legal y costo que pueda causarse o surgir por daños o lesiones a personas o propiedades de terceros incluido el personal del INVIAS, ocasionados por EL CONTRATISTA o por sus subcontratistas o dependientes (si fueren autorizados) en la ejecución del objeto y las obligaciones contractuales.
13. Guardar estricta reserva sobre toda la información y documentos que tenga acceso, maneje en desarrollo de su actividad o que llegue a conocer en desarrollo del contrato y que no tenga el carácter de pública. En consecuencia, se obliga a no divulgar por ningún medio dicha información o documentos a terceros, sin la previa autorización escrita del INVIAS. Esta obligación permanecerá vigente aún después de la terminación por cualquier causa de la vinculación que ligue a las partes. Por lo tanto, en caso de que EL CONTRATANTE tenga prueba de que EL CONTRATISTA ha divulgado cualquier tipo de documentación o información que en forma alguna se relacione con el presente contrato, EL CONTRATISTA indemnizará los perjuicios que con tal hecho cause al CONTRATANTE. No se considerará incumplida esta cláusula cuando la información o documentos deban ser revelados por mandato judicial y/o legal o cuando la información manejada tenga el carácter de pública.
14. Cumplir con la política de buen trato para con los demás colaboradores internos y externos del INVIAS, y actuar con responsabilidad, eficiencia y transparencia.
15. Respetar la política medioambiental del INVIAS, política que incluye todas las normas internas sobre el uso de los recursos ambientales y públicos, como el agua y la energía,

racionamiento de papel, normas sobre parqueaderos y manejo de desechos residuales

16. No acceder a peticiones ni amenazas de quienes actúen por fuera de la ley, con el fin de obligarlo a hacer u omitir algún hecho o acto, debiendo informar inmediatamente, al INVIAS, por conducto del funcionario responsable del control de ejecución, la ocurrencia de tales peticiones o amenazas deberán ser comunicadas a las autoridades competentes, para que se adopten las medidas y correctivos que fueren necesarios.
17. Cumplir con los aportes parafiscales con destino al Instituto Colombiano de Bienestar Familiar (ICBF), a las Cajas de Compensación Familiar y Servicio Nacional de Aprendizaje (SENA), de conformidad con lo ordenado por el Decreto 562 de 1990, el artículo 50 de la Ley 789 de 2002, 828 de 2003 y el Articulo 23 de la Ley 1150 de 2007. PARÁGRAFO: Para cada pago de conformidad con normatividad antes señalada, en la ejecución del Contrato, el Contratista deberá acreditar, mediante la presentación de los respectivos comprobantes de pago, el cumplimiento de las obligaciones frente al Sistema de Seguridad Social Integral.
18. Mantener durante la ejecución del contrato, las condiciones exigidas y ofrecidas en su propuesta.
19. Cumplir a cabalidad con las condiciones pactadas en el presente Contrato, las cuales solamente podrán ser modificadas previo cumplimiento del trámite dispuesto, según el procedimiento establecido y una vez se alleguen los documentos pertinentes.
20. Mantener actualizadas las vigencias y el monto de los amparos de las garantías expedidas con ocasión de la suscripción del Contrato, acorde con lo indicado en el ítem de GARANTÍAS, teniendo en consideración el plazo de ejecución, valor, modificaciones en valor y/o plazo, suspensiones, etc., que afecten su vigencia o monto.
21. Presentar la respectiva factura o su documento equivalente cuando esté obligado a ello, acorde con el régimen tributario aplicable al objeto contratado, acompañada de los documentos soporte que permitan establecer el cumplimiento de las condiciones pactadas, incluido el Registro Único Tributario (RUT) expedido por la DIAN y el Registro de Información Tributaria (RIT) expedido por la Dirección Distrital de Impuestos, requisitos sin los cuales no se podrá tramitar el respectivo pago.
22. Es obligación del contratista conocer y presupuestar todos los gravámenes de los cuales es responsable al momento de presentar su propuesta y celebrar el presente Contrato, por tanto, asumirá la responsabilidad y los costos, multas y/o sanciones que se generen por la inexactitud de la información fiscal que se haya entregado al INVIAS. Para todos los efectos legales, presupuéstales y fiscales, se entenderá que el valor de la propuesta presentada por el contratista incluye IVA.
23. En el evento que el objeto contratado involucre la asignación de bienes devolutivos al Contratista, éste deberá suscribir el comprobante de traslado o salida a servicio (inventario) de los elementos entregados, documento al cual se anexará la solicitud del supervisor y copia del contrato; a la terminación del plazo pactado el Contratista entregará los bienes a la entidad a través del comprobante de reintegro que opere en la Entidad, para obtener el certificado de recibo a satisfacción, documento que deberá anexarlo al informe final del contrato como requisito para tramitar la aprobación del último pago.

24. Obrar con lealtad y buena fe en las distintas etapas contractuales evitando dilaciones o en trabamientos tanto en el cumplimiento de los requisitos de ejecución como en el desarrollo del contrato.

9.2 OBLIGACIONES ESPECÍFICAS.

Además de las derivadas de la esencia y naturaleza del contrato que se celebre, y de la ley, el contratista se obligará a:

1. Priorizar la contratación de personas naturales con discapacidad que acrediten los requisitos técnicos y de experiencia definidos para integrar el equipo de trabajo requerido para la ejecución del contrato. Presentar al supervisor, con cada solicitud de pago, los soportes correspondientes para verificar el cumplimiento de esta obligación. Si una circunstancia de fuerza mayor o caso fortuito impide cumplirla, informarlo y acreditarlo ante el supervisor.

2. Efectuar la entrega de la totalidad de los bienes y servicios objeto del contrato en el sitio y dentro de los plazos establecidos por el Supervisor del contrato, de conformidad con las especificaciones técnicas señaladas en la ficha técnica y sus anexos.
3. Cumplir integralmente con las condiciones, requisitos y especificaciones técnicas establecidas en la Ficha Técnica del proceso, garantizando su observancia durante toda la ejecución contractual.
4. Remitir, junto con el cronograma de ejecución contractual al supervisor del contrato, el certificado o constancia expedida por el Forum of Incident Response and Security Teams (FIRST), mediante el cual se acredite su condición de miembro activo y vigente de dicha organización, con una antigüedad mínima de tres (3) años.
5. Remitir al supervisor del contrato el certificado vigente ISO/IEC 27001:2022 de su Sistema de Gestión de Seguridad de la Información, expedido por un organismo de certificación acreditado, cuyo alcance certificado incluya expresamente los servicios de operación de Centro de Operaciones de Seguridad (SOC) o de servicios de seguridad gestionada (MSSP) que serán prestados en ejecución del presente contrato
6. Implementar, configurar, integrar y poner en operación el Centro de Operaciones de Seguridad (SOC) con la totalidad de las plataformas contratadas (SIEM, EDR/XDR, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, WAF, AntiDDoS y NAC), en un plazo máximo de doce (12) semanas contadas desde la firma del contrato, y suscribir con el INVIAS el acta de inicio operativo una vez se cumplan los criterios de arranque definidos en la ficha técnica.
7. Prestar el servicio de monitoreo, detección, correlación, respuesta y gestión de incidentes de seguridad de manera continua, durante las veinticuatro (24) horas del día, los siete (7) días de la semana y los trescientos sesenta y cinco (365) días del año, con analistas organizados en tres niveles de atención (L1, L2 y L3), sobre el universo de activos a proteger

de la infraestructura del INVIAS utilizada para el funcionamiento del PSCN y su componente VIITS.

8. Cumplir los acuerdos de nivel de servicio establecidos en la ficha técnica, en particular los tiempos máximos de detección (MTTD) y de respuesta (MTTR) por severidad: crítico, quince (15) minutos y cuatro (4) horas; alto, una (1) hora y ocho (8) horas; medio, cuatro (4) horas y veinticuatro (24) horas, respectivamente.
9. Activar y registrar ante los fabricantes las suscripciones de las soluciones contratadas (y obtener el certificado oficial de Imperva para el WAF), entregar al supervisor la evidencia de dicha activación y registro dentro del plazo señalado en el cronograma de implementación, y garantizar que la totalidad de las licencias queden registradas a nombre del INVIAS, independientemente de quién las gestione u opere.
10. Integrar al SIEM, como fuentes primarias, los treinta y un (31) dispositivos de seguridad perimetral existentes, la plataforma EDR/XDR, el WAF, el AntiDDoS, Microsoft 365 y los activos desplegados en Microsoft Azure, y migrar la solución antivirus actual hacia la plataforma EDR/XDR, sin interrupción del servicio, para un máximo de tres mil (3.000) activos.
11. Suministrar, instalar y poner en operación los appliances físicos (AntiDDoS y NAC) con sus licencias asociadas, entregándolos en las instalaciones del INVIAS en Bogotá D.C., en condición de nuevos y en caja sellada de fábrica, previo ingreso al inventario de la entidad mediante soporte de entrada al almacén.
12. Configurar los playbooks base del SOAR/IRP, las reglas de correlación y los casos de uso específicos para el INVIAS, y realizar el ajuste (tuning) inicial y continuo de los mismos durante la vigencia del contrato.
13. Garantizar al INVIAS acceso propio, permanente e independiente a las consolas de monitoreo, dashboards ejecutivos, reportes operativos y registros de incidentes del SOC, sin intermediación del contratista y sin restricciones durante la vigencia del contrato.
14. Poner a disposición del INVIAS la bolsa de doscientas (200) horas prepagadas de servicios especializados desde la firma del contrato, con confirmación escrita de la disponibilidad inmediata de los perfiles y datos de contacto 24×7, y reportar su consumo de manera periódica al supervisor.
15. Realizar un mínimo de cuarenta (40) horas de transferencia de conocimiento al equipo de la OTIC del INVIAS.
16. Presentar informes operativos y ejecutivos periódicos sobre eventos, incidentes, indicadores de nivel de servicio y estado de las plataformas, en los términos definidos en la ficha técnica y por el supervisor.
17. Garantizar que la operación del SOC no afecte la disponibilidad ni el funcionamiento continuo de la infraestructura del INVIAS utilizada para la operación de VIITS, y coordinar con la OTIC las ventanas de intervención sobre dichos activos.
18. Guardar la confidencialidad y reserva de la información a la que tenga acceso con ocasión del contrato, aplicar las medidas de seguridad necesarias para su protección y notificar de inmediato al supervisor cualquier incidente que la comprometa.
19. Al vencimiento de la suscripción, entregar al INVIAS la totalidad de reglas de correlación, playbooks, casos de uso, configuraciones y documentación técnica desarrollados durante

la vigencia, como condición para la liquidación, y garantizar un período de transición mínimo de sesenta (60) días calendario, sin costo adicional, para la transferencia ordenada de la operación.

20. Garantizar que los equipos entregados sean nuevos y originales, libres de defectos de fabricación, no remanufacturados ni reacondicionados, con plena vigencia de garantía de fábrica al momento de la entrega, y en ningún caso equipos de exhibición, demostración o con uso previo de cualquier naturaleza.
21. Entregar al supervisor del contrato los certificados, constancias y documentos que acrediten el registro de los bienes ante el los fabricantes, incluyendo los números de serie de cada dispositivo y la confirmación del estado activo del soporte y las licencias en los portales del fabricante.
22. Atender de manera oportuna las observaciones, requerimientos y solicitudes que le formule la Oficina de Tecnologías de la Información y las Comunicaciones por conducto del supervisor del contrato, y efectuar los ajustes o correcciones que sean necesarios dentro del plazo razonable que se le señale para tal efecto.
23. Entregar al supervisor del contrato los informes requeridos en los que se relacionen las actividades ejecutadas durante el desarrollo del contrato, así como la documentación soporte de la entrega de bienes, la activación del soporte técnico y el licenciamiento contratado.
24. Garantizar la oportuna, eficaz y eficiente ejecución del objeto contratado y responder por su calidad durante toda la vigencia del contrato, sin perjuicio de las garantías y amparos constituidos.
25. Las demás derivadas de la esencia y naturaleza del contrato que se celebre, de la ley, las que estén en relación con el objeto del contrato, las establecidas en el anexo técnico del presente proceso, y las que le sean solicitadas por el supervisor del contrato.

9.3 OBLIGACIONES DEL INVIAS

1. Verificar cumplimiento de la obligación de priorización y revisar los soportes que presente el contratista con cada solicitud de pago, así como los que sustenten una eventual fuerza mayor o caso fortuito.
2. Cancelar el valor del presente contrato como contraprestación por la prestación de los servicios especializados de ciberseguridad, el suministro de las suscripciones y equipos y los servicios complementarios objeto del contrato, de conformidad con lo establecido en el presente contrato.
2. Ejercer la supervisión y control del cumplimiento del objeto y las obligaciones del presente contrato.
3. Facilitar todos los medios necesarios para el buen desarrollo del contrato.
4. Suministrar oportunamente al contratista la información, los accesos y las autorizaciones que requiera para la implementación y operación del SOC sobre la infraestructura del INVIAS utilizada para el funcionamiento de VIITS, conforme a los lineamientos de seguridad

de la entidad.

5. Designar un punto de contacto técnico de la OTIC para la coordinación de la implementación, la atención de incidentes y la suscripción de las actas del contrato.
6. Las demás que se deriven de la naturaleza del presente contrato y que surjan del desarrollo de este.

9.4 SUPERVISIÓN

La supervisión del contrato que resulte de este proceso será ejercida por el **Coordinador del Grupo de Servicios Tecnológicos de la Oficina de Tecnologías de la Información y las Comunicaciones** o quien el ordenador del gasto designe y/o delegue, quien además de las obligaciones establecidas en el Manual de Contratación vigente deberá: 1) Velar porque el objeto del contrato y las obligaciones del mismo se cumplan a cabalidad.; 2) Expedir la certificación del cumplimiento del objeto y de las obligaciones del contrato en las condiciones exigidas; 3) Informar oportunamente sobre la necesidad de modificación o terminación de mutuo acuerdo siempre y cuando tales hechos estén plenamente justificados; 4) Impartir las directrices y sugerencias por escrito y formular las observaciones que estime convenientes sobre el desarrollo del contrato, 5) Informar cualquier irregularidad que se presente en desarrollo del contrato. 6) Proyectar el Acta de Liquidación del contrato, conforme a lo dispuesto en la Ley 80 de 1993 y modificado por la ley 1150 de 2007 y por el Decreto 0019 de 2012 y demás normas que los modifiquen, aclaren o adicionen y la reglamentación interna del INSTITUTO.

10 CRITERIOS PARA SELECCIONAR LA OFERTA MAS FAVORABLE

De conformidad con el numeral 3 del artículo 5 de la Ley 1150 de 2007, reglamentado por el Decreto 1082 de 2015, en las contrataciones cuyo objeto sea la adquisición o suministro de bienes y servicios de características técnicas uniformes y común utilización, las entidades estatales incluirán como único factor de evaluación el **MENOR PRECIO OFRECIDO**.

En razón a lo dispuesto anteriormente, **EL MENOR PRECIO** será el factor que permitirá identificar la oferta más favorable, y será el factor de selección del contratista, siempre y cuando cumpla con las especificaciones técnicas de cada uno de los ítems y los requisitos habilitantes**.**

En caso de persistir el empate la Entidad estatal debe aplicar las reglas contenidas en el art 35 de la ley 2069 de 2020.

10.1 INFORMACIÓN PREVIA

El proponente deberá analizar la información relacionada en el presente pliego de condiciones, sus anexos, las características y condiciones técnicas, y descripción de los ítems contenidos en el documento denominado ***03. FORMULARIO 2 OFERTA ECONOMICA*** de este proceso de selección, así como la normatividad vigente, a efectos de elaborar la oferta económica para ejecutar el objeto del contrato.

10.1.1 IMPUESTOS, TASAS Y CONTRIBUCIONES

Al formular la oferta, el proponente acepta que estarán a su cargo todos los impuestos, tasas y contribuciones establecidos por las diferentes autoridades nacionales, departamentales o municipales, que afecten el contrato y las actividades que se deriven.

10.2 APERTURA DEL SOBRE No. 2

Se efectuará la apertura de los sobres No. 2 de las ofertas que resultaron HABILITADAS en la evaluación de los requisitos habilitantes y el INVÍAS verificará que la oferta económica cumpla lo siguiente:

a. Que la oferta económica corresponda al proceso.

b. Que la oferta económica no presente tachadura o enmendadura, a menos que las hubiere salvado bajo su firma quien suscribió o autorizó el documento.

c. Que el valor total de la propuesta económica no sobrepase el presupuesto oficial del proceso ni el valor techo de los ítems unitarios.

d. Que se hayan consignado y ofrecido todos los ítems, y que el valor unitario no sobrepase el precio techo establecido por el INVÍAS y su valor no sea cero (0) para cada uno de los ítems que componen el presupuesto oficial.

En ningún caso podrán ofertar 0 en uno o algunos de los precios unitarios ofertados por los proponentes so pena de rechazo.

La inobservancia de cualquiera de los requisitos anteriores será causal de **RECHAZO**.

NOTA 1: Teniendo en cuenta que al momento de remitir los documentos por parte del proponente en el SECOP II a través del Portal Único de Contratación (PUC), link: http://community.secop.gov.co/sts/cce/login.aspx, tiene dicho portal el SELLO DE TIEMPO, el cual se trata un mecanismo de seguridad y validez jurídica de la fecha y hora exacta en la generación, envío y recepción de información electrónica, además que garantiza la integridad de la información

durante su ciclo de vida, sello este que se encuentra vinculado a la FIRMA DIGITAL (Ley 527 de 1999, Decreto 2364 de 2012 y demás normas que las modifiquen, aclaren o complementen), no es indispensable remitir este documento firmado por el proponente, pues el INVÍAS entenderá que con este SELLO DE TIEMPO, el representante legal está firmando la oferta.

NOTA 2: En caso de que se requiera, para efectos de poder determinar la presentación de precios presuntamente artificialmente bajos, se dará aplicación a lo señalado en la Guía elaborada por Colombia Compra Eficiente para tal efecto.

El INVÍAS sólo efectuará correcciones aritméticas originadas por:

1. Las correcciones aritméticas previstas en el pliego se efectuarán previo a la realización de la subasta, cuando a ello haya lugar, con el fin de garantizar que los valores económicos utilizados en el procedimiento correspondan a los cálculos correctos. Este ajuste se entiende únicamente como una verificación de operaciones matemáticas y no como una modificación de las condiciones de la propuesta, en concordancia con lo establecido en el Decreto 1082 de 2015 y la Ley 80 de 1993 respecto de la subsanabilidad de errores meramente aritméticos.

2. El ajuste al peso, ya sea por exceso o por defecto, se aplicará a los precios unitarios contenidos en la propuesta económica y, cuando corresponda, al valor del IVA, de acuerdo con lo establecido en la normatividad vigente. Así: cuando la fracción decimal del peso sea igual o superior a punto cinco (0.5) se aproximará por exceso al número entero siguiente, y cuando la fracción decimal del peso sea inferior a punto cinco (0.5) se aproximará por defecto al número entero.

10.2.1 SUBASTA INVERSA ELECTRÓNICA

La subasta inversa es una puja dinámica efectuada electrónicamente, mediante la reducción sucesiva de precios durante un tiempo determinado, de conformidad con las reglas previstas en la ley y en el respectivo pliego de condiciones.

Se fijará fecha y hora en el cronograma del proceso, para el desarrollo de la subasta inversa electrónica, en la cual los proponentes deberán estar conectados en línea a través de la plataforma electrónica SECOP II, para el desarrollo de la misma, atendiendo el procedimiento establecido por Colombia Compra Eficiente.

10.2.1.1 PROCEDIMIENTO PARA EL DESARROLLO DE LA SUBASTA

De conformidad con lo regulado en el ART 5 del decreto 1860 de 2021 por medio del cual 6. Modificación del artículo 2.2.1.2.1.2.2. de la Subsección 2 de la Sección 2 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015. Modifíquese el artículo 2.2.1.2.1.2.2. de la

Subsección 2 de la Sección 1 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, el cual quedará así:

"*Artículo 2.2.1.2.1.2.2. Procedimiento para la subasta inversa. Además de las reglas generales previstas en la ley y en el presente título, las siguientes reglas son aplicables a la subasta inversa:*

1. *Los pliegos de condiciones deben indicar: a) la fecha y hora de inicio de la subasta; b) la periodicidad de los Lances; y c) el Margen Mínimo para mejorar la oferta durante la subasta inversa.*

2. *La oferta debe contener dos parles, la primera en la cual el interesado acredite su capacidad de participar en el Proceso de Contratación y acredite el cumplimiento de la ficha técnica; y la segunda parle debe contener el precio inicial propuesto por el oferente.*

3. *La Entidad Estatal debe publicar un informe de habilitación de los oferentes, en el cual debe indicar si los bienes o servicios ofrecidos por el interesado cumplen con la ficha técnica y si el oferente se encuentra habilitado.*

4. *Hay subasta inversa siempre que haya como mínimo dos oferentes habilitados cuyos bienes o servicios cumplen con la ficha técnica.*

5. *Si en el Proceso de Contratación se presenta un único oferente cuyos bienes o servicios cumplen con la ficha técnica y está habilitado, la Entidad Estatal puede adjudicarle el contrato al único oferente si el valor de la oferta es igualo inferior a la disponibilidad presupuesta I para el contrato, caso en el cual no hay lugar a la subasta inversa.*

6. *La subasta debe iniciar con el precio más bajo indicado por los oferentes y en consecuencia, solamente serán válidos los Lances efectuados durante la subasta inversa en los cuales la oferta sea mejorada en por lo menos el Margen Mínimo establecido.*

7. *Si los oferentes no presentan Lances durante la subasta, la Entidad Estatal debe adjudicar el contrato al oferente que haya presentado el precio inicial más bajo.*

8. *Al terminar la presentación de cada Lance, la Entidad Estatal debe informar el valor del Lance más bajo.*"

Si al terminar la subasta inversa hay empate, se aplicara los criterios de desempate previstos en el artículo 35 ley 2069 de 2020, conforme con los medios de acreditación del artículo 2.2.1.2.4.2.17 del decreto 1860 de 2021, así:

"1. Preferir la oferta de bienes o servicios nacionales frente a la oferta de bienes o servicios extranjeros.

2. Preferir la propuesta de la mujer cabeza de familia, mujeres víctimas de la violencia intrafamiliar o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por mujeres cabeza de familia, mujeres víctimas de violencia intrafamiliar y/o personas jurídicas en las cuales participe o participen mayoritariamente.

3. Preferir la propuesta presentada por el oferente 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 a la que se refiere la Ley 361 de 1997. Si la oferta es presentada por un proponente plural, el integrante del oferente 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 el consorcio, unión temporal o promesa de sociedad futura y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

4. Preferir la propuesta presentada por el oferente que acredite la vinculación en mayor proporción de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la Ley.

5. Preferir la propuesta presentada por el oferente que acredite, en las condiciones establecidas en la ley, que por lo menos diez por ciento (10%) de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas.

6. Preferir la propuesta de personas en proceso de reintegración o reincorporación o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por personas en proceso de reincorporación, y/o personas jurídicas en las cuales participe o participen mayoritariamente.

7. Preferir la oferta presentada por un proponente plural siempre que:

(a) esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración, o una persona jurídica en la cual participe o participen mayoritariamente, y, que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural;

(b) la madre cabeza de familia, la persona en proceso de reincorporación o reintegración, o la persona jurídica aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y

(c) ni la madre cabeza de familia o persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.

8. Preferir la oferta presentada por una MiPymes o cooperativas o asociaciones mutuales; o un proponente plural constituido por Mipymes, cooperativas o asociaciones mutuales.

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

10. Preferir al oferente que acredite de acuerdo con sus estados financieros o información contable con corte a 31 de diciembre del año anterior, por lo menos el veinticinco por ciento (25%) del total de pagos realizados a MiPymes, cooperativas o asociaciones mutuales por concepto de proveeduría del oferente, realizados durante el año anterior; o, la oferta presentada por un proponente plural siempre que:

(a) esté conformado por al menos una MIPYME, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%);

(b) la MIPYME, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y

(c) ni la MIPYME, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.

11. Preferir las empresas reconocidas y establecidas como Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento MIPYMES.

12. Utilizar un método aleatorio para seleccionar el oferente, método que deberá haber sido previsto previamente en los Documentos del Proceso.PARÁGRAFO 1. Los factores de desempate serán aplicables en el caso de las cooperativas y asociaciones mutuales que cumplan con los criterios de clasificación empresarial, definidos por el Decreto 957 de 2019, priorizando aquellas que sean micro, pequeñas o medianas.

PARÁGRAFO 2. Para los criterios enunciados que involucren la vinculación de capital humano, el oferente deberá acreditar una antigüedad igual o mayor a un año. Para los casos de constitución inferior a un año se tendrá en cuenta a aquellos trabajadores que hayan estado vinculados desde el momento de constitución de la misma."

Margen mínimo de mejora del precio

En atención a lo establecido en el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015, para la presente Subasta Inversa Electrónica, la Entidad establece que el margen mínimo de mejora de ofertas para el presente proceso no podrá ser menor del DOS POR CIENTO (2%) DEL PRECIO DE ARRANQUE ESTABLECIDO AL INICIO de la subasta Inversa Electrónica.

Así mismo, la Entidad indica que respecto a los lances que se efectúen por los proponentes en desarrollo de la Subasta Inversa Electrónica, SÓLO SE TENDRÁN COMO VÁLIDOS, LOS LANCES QUE MEJOREN SU ÚLTIMO LANCE VÁLIDO, EN POR LO MENOS EL MARGEN MÍNIMO ESTABLECIDO DEL DOS POR CIENTO (2%).

Este margen de mejora de la oferta se estableció de acuerdo con los porcentajes de mejora históricos manejados por la entidad dentro de los contratos adelantados de similares características.

10.2.1.2 **PROCEDIMIENTO DEL EVENTO DE SUBASTA INVERSA**

Además de lo establecido en el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015 modificado por el artículo 6 del Decreto 1860 de 2021, se establecen las siguientes reglas:

4.1.1.1.1 Se realizará de acuerdo con la configuración establecida en la plataforma virtual de Colombia Compra Eficiente SECOP II y la guía “Guía para hacer un proceso de selección abreviada con subasta en el SECOP II”.

4.1.1.1.2 La subasta comienza cuando se cumple la fecha de inicio previamente programada en el cronograma establecido en el proceso el cual se encuentra publicado en SECOP II. No se requiere que la Entidad realice ninguna acción.

4.1.1.1.3 Los oferentes habilitados pueden ingresar a la subasta desde el gestor de subasta de la plataforma SECOP II, o desde el correo electrónico de invitación a la subasta que envía automáticamente la plataforma a los proveedores admitidos.

4.1.1.1.4 Desde la pestaña “lista de precios” puede hacer seguimiento en tiempo real a los lances. La lista le muestra el último lance realizado por cada proveedor. Cada vez que un proveedor hace un nuevo lance válido, el valor y la posición relacionada se actualizan.

4.1.1.1.5 Los proponentes habilitados que participen en el evento subasta electrónica deberán acceder a la misma a través de sus propios recursos. La Entidad no provee conexiones desde sus instalaciones para este evento.

4.1.1.1.6 El margen mínimo para que sea válido cada lance deberá ser del **DOS POR**

CIENTO (2%). Es importante tener en cuenta que el proponente deberá realizar sus lances estimando para ello dicho margen mínimo a su último lance. La diligencia de subasta electrónica tendrá una **DURACIÓN DE 30 MINUTOS.**

4.1.1.1.7 El precio de arranque de la subasta inversa electrónica será la oferta que presente el menor valor total ofrecido, el cual será tomado automáticamente por la plataforma del SECOP II subasta electrónica.

4.1.1.1.8 Si en el curso de la subasta electrónica dos o más proponentes presentan una postura del mismo valor, SECOP II permite generar un informe con el histórico de los lances en formato PDF o EXCEL. El reporte en PDF incluye una gráfica resumen de la subasta. El reporte en Excel tiene un mayor detalle sobre los lances, los registros incluyen el inventario de mensajes durante la subasta, de esta manera se podrá establecer cronológicamente cual proponente envío primero dicha postura.

4.1.1.1.9 Si terminada la subasta inversa se presenta empate, se dará aplicación a los criterios del artículo 35 de la Ley 2069 de 2020 conforme con los medios de acreditación del artículo 2.2.1.2.4.2.17 del Decreto 1860 de 2021.

4.1.1.1.10 Conforme avanza la subasta electrónica los proponentes podrán verificar en el sistema de recepción de su postura y la confirmación de su valor, así como de la ubicación en que se encuentra su propuesta, al llevar a cabo un lance.

4.1.1.1.11 La configuración de la Subasta Electrónica **NO contará con tiempo extra.**

4.1.1.1.12 Si en el curso de la subasta electrónica inversa se presentan fallas de la plataforma tecnológica como las previstas en el artículo 2.2.1.2.1.2.6 del Decreto 1082 de 2015, que impidan continuar con el curso normal de la misma, (..” la subasta debe ser suspendida y cuando la falla técnica haya sido superada la entidad estatal deberá reiniciar la subasta..”) se dará reinicio al evento de la subasta en las condiciones y fechas que establezca la Entidad y que serán comunicadas a los proponentes habilitados. Es importante que tengan en cuenta que si las fallas corresponden a los recursos propios de los proponentes se entenderá que los mismos desistieron de participar salvo que logren conectarse antes de la terminación del evento de conformidad con el artículo 2.2.1.2.1.2.6 del Decreto 1082 de 2015.

4.1.1.1.13 En ningún caso la herramienta virtual SECOP II determinara precios artificialmente bajos; este proceso lo determinara la Entidad una vez culminado el evento subasta y aplicara lo dispuesto en el artículo 2.2.1.1.2.2.4 del Decreto 1082 de

2015 así como la “Guía para el manejo de ofertas artificialmente bajas en procesos de contratación” suscritas por Colombia Compra Eficiente.

4.1.1.1.14 Cuando finalice la subasta, el SECOP II no permite que los proveedores sigan enviando lances y habilita la opción para que la entidad estatal genere el informe y adjudique el proceso de contratación.

4.1.1.1.15 Para la elaboración de los contratos, el total de los porcentajes de descuento ofertados se aplicarán uniformemente a todos los ítems, corriendo la formula en hoja Excel, para lo cual el proponente que resulte seleccionado deberá remitir a la entidad en un tiempo máximo a un (1) día hábil su propuesta económica ajustada conforme a los porcentajes de descuento que resulten del evento de subasta.

Para la elaboración de los contratos, el total de los porcentajes de descuento ofertados se aplicarán uniformemente a todos los ítems, corriendo la formula en hoja Excel, para lo cual el proponente que resulte seleccionado deberá remitir a la entidad en un tiempo máximo a un (1) día hábil su propuesta económica ajustada conforme a los porcentajes de descuento que resulten del evento de subasta.

Nota 1: Se entiende por lance el porcentaje de descuento que realiza cada uno de los oferentes en las diferentes pujas o rondas de la subasta.

Nota 2: Si el proponente en el cuestionario de SECOP II diligencia un valor diferente al que se encuentra registrado dentro del formato de oferta económica, esto no será causal de rechazo ni se invalidará la oferta. En todo caso, el valor que será verificado para efectos del desarrollo de la subasta será el que se encuentre relacionado en el Formulario 2 – Oferta Económica.

Nota 3: El proponente al cual se le adjudique el contrato deberá diligenciar su propuesta económica en la plataforma SECOP II, de conformidad con el valor total de la sumatoria de los ítems de su oferta. Adicionalmente, deberá presentar el formato de propuesta económica detallando los valores ofertados por cada ítem en el formato de propuesta económica (Excel y/o PDF), cumpliendo con la hora establecida en el cronograma del proceso. **EL NO DILIGENCIAMIENTO DE CUALQUIERA DE ESTOS REQUISITOS (SECOP II Y/O FORMATO EXCEL Y/O PDF) TIPIFICA LA CAUSAL DE RECHAZO CONTENIDA EN EL PLIEGO DE CONDICIONES.**

Nota 4: Señor proponente, recuerde que, para efectos de la subasta, su lance será por el valor resultante de la sumatoria de los valores unitarios propuestos de todos los ítems.

10.2.1.3 CONSIDERACIONES

- La apertura del módulo de subasta inversa electrónica se dará a la hora indicada en el cronograma establecido en el proceso.

- La metodología de la subasta se realizará de acuerdo a los lineamientos de la Guía de Colombia compra eficiente y lo establecido en los pliegos de condiciones.
- Si se tiene alguna duda durante el desarrollo de la subasta, se deberá manifestar oportunamente por mensaje antes de enviar el lance, respetando en todo caso los tiempos dados por el INVIAS.

En caso de presentarse inconvenientes para ingresar a la subasta y/o realizar lances dentro de la misma el proponente tendrá la carga de acreditar el fallo de la plataforma SECOP II tal y como lo establece la guía de indisponibilidad implementada por la agencia nacional de contratación pública Colombia compra eficiente la cual se puede consultar a través del siguiente link

https://colombiacompra.gov.co/sala-de-prensa/comunicados/nuevo-protocolo-de-indisponibilidad-para-usuarios-del-secop-ii#:~:text=Las%20fases%20que%20contempla%20el,aplicaci%C3%B3n%20de%20adendas%2C%20firma%20de

10.3 ANÁLISIS DE RIESGO Y LA FORMA DE MITIGARLO

De acuerdo con las disposiciones del artículo 4º de la ley 1150 de 2007 art 2.2.1.1.2.1.3. del DECRETO único reglamentario 1082 de 2015 y CONPES 3714 de 2011 se procede a la identificación, tipificación, valoración, y asignación de los riesgos y tratamiento, los cuales deben quedar plasmados en un documento denominado **"MATRIZ DE RIESGOS"** documento oficial del Instituto Nacional De Vías con el cual se le da cumplimiento a las normas vigentes

De conformidad con lo antes descrito el Instituto Nacional de Vías pone a disposición de los interesados en el presente proceso de selección el formato establecido para tal fin.

10.4 ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS DESTINADAS A AMPARAR LOS PERJUICIOS DE NATURALEZA CONTRACTUAL O EXTRACONTRACTUAL, DERIVADOS DEL INCUMPLIMIENTO DEL OFRECIMIENTO O DEL CONTRATO, SEGÚN EL CASO

- **GARANTÍAS CONTRACTUALES**

EL CONTRATISTA se obliga a constituir a favor del INSTITUTO NACIONAL DE VIAS, con NIT 800.215.807 como mecanismo de cobertura del riesgo, cualquiera de las garantías que se señalan a continuación, opciones señaladas en el artículo 2.2.1.2.3.1.2. Clases de garantías y ss del decreto único reglamentario 1082 de 2015, para lo cual deberá dar cumplimiento a las estipulaciones señaladas en el citado Decreto:

1. Contrato de seguro contenido en una póliza
2. Patrimonio autónomo
3. Garantía Bancaria

La garantía no podrá ser cancelada sin la autorización escrita del INSTITUTO NACIONAL DE VIAS.

El CONTRATISTA deberá cumplir con todos los requisitos necesarios para mantener vigente la garantía a que se refiera el contrato y deberá ser expedida por una entidad bancaria o por una compañía de seguros legalmente establecidas en Colombia, cuya póliza matriz haya sido aprobada por la Superintendencia Financiera de Colombia.

Será a cargo del CONTRATISTA el pago oportuno de todas las primas y erogaciones de constitución y mantenimiento de la garantía.

El contratista deberá restablecer el valor de la garantía cuando este se haya visto reducido por razón de las reclamaciones efectuadas por la entidad contratante.

En caso de que haya necesidad de adicionar, prorrogar o suspender la ejecución del contrato, o en cualquier otro evento, el contratista se obliga a ampliar el valor de la garantía otorgada o ampliar su vigencia, según el caso.

Todas las manifestaciones contenidas en la póliza o en las condiciones generales de la misma, contrarias o diferentes a las establecidas en este proceso y en especial para cada uno de los amparos solicitados, se tendrán por no escritas.

La garantía deberá expedirse de acuerdo con lo relacionado a continuación:

De conformidad con lo establecido en el Decreto 1082 de 2015y la Resolución 478 de 2012 expedida por el Instituto Nacional de Vías, el contratista se obliga a constituir, a favor del Instituto Nacional de Vías, una garantía única de cumplimiento, que ampare:

A. **EL CUMPLIMIENTO GENERAL DEL CONTRATO** y demás sanciones que se le impongan, por una cuantía equivalente al veinte por ciento (20%) del valor del contrato, con vigencia durante el plazo de ejecución del contrato y seis (6) meses adicionales, en todo caso, deberá estar vigente hasta la liquidación del contrato.

B. **LA CALIDAD DEL SERVICIO**, Por una cuantía equivalente al veinte por ciento (20%) del valor del contrato, con vigencia a partir de la orden de inicio y hasta doce (12) meses posteriores a la terminación del contrato, en todo caso, deberá

mantenerse hasta la liquidación.

C. **LA CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES** que se le impongan, Por una cuantía equivalente al veinte por ciento (20%) del valor del contrato, con vigencia a partir del recibo de los bienes y durante tres (3) años adicionales, en todo caso, deberá mantenerse hasta la liquidación del contrato.

D. **EL PAGO DE SALARIOS, PRESTACIONES SOCIALES E INDEMNIZACIONES LABORALES:** Por el equivalente al cinco por ciento (5%) del valor total del contrato y una vigencia igual al plazo del contrato y tres (3) años más.

E. **GARANTÍA DE RESPONSABILIDAD CIVIL EXTRACONTRACTUAL:** por una cuantía equivalente a 200 SMMLV con una vigencia igual a la del plazo del contrato.

NOTA 1: Esta garantía deberá presentarse al INSTITUTO dentro de los tres (3) días hábiles siguientes contados a partir de la firma del contrato y requerirá la aprobación del INSTITUTO.

NOTA 2: Teniendo en cuanta la diferencia que existe entre la fecha de perfeccionamiento del Contrato y la fecha de Orden de Inicio, EL CONTRATISTA, deberá ajusta la Garantía Única, modificando las vigencias en cuanto a su vencimiento, sin modificar la fecha de inicio de los amparos.

NOTA 3: El contratista se comprometerá a ampliar, modificar o prorrogar la garantía única de cumplimiento, en el evento que se aumente el valor del contrato o se prorrogue o suspenda su vigencia. Y deberá restablecer el valor de la garantía cuando éste se haya visto reducido por razón de las reclamaciones efectuadas por el INSTITUTO, al tenor de lo dispuesto en el artículo 2.2.1.2.3.1.18 del Decreto 1082 de 2015.

NOTA 4: REQUISITOS DE LAS GARANTÍAS Y SEGUROS. - Con respecto a cualquiera de las clases de garantías permitidas por el Artículo 2.2.1.2.3.1.2 del Decreto No. 1082 del 2015, se debe tener en cuenta las siguientes instrucciones: • El tomador debe ser el contratista. • Cuando se trate de contratista plural (Consorcio o Unión Temporal), la garantía debe ser otorgada por todos sus integrantes. • Se debe establecer clara y completamente el NIT del Instituto Nacional de Vías 800.215.807-2 y el NIT del Contratista, Incluir dígito de verificación (número después del guion). No se aceptan garantías a nombre del representante legal o de alguno de los integrantes del consorcio. • Cuando el contratista sea una Unión Temporal o Consorcio, se debe incluir razón social, NIT y porcentaje de participación de cada uno de los integrantes. • Debe incluir claramente el número y año del contrato. • Debe incluir el objeto del contrato. • Las garantías y el seguro deben ser firmados por el representante legal del contratista. • La fecha de inicio de la vigencia de los amparos y del

seguro debe ser la fecha de suscripción del contrato. No obstante, una vez impartida la orden de inicio de ejecución del contrato, la vigencia final de las garantías y del seguro se ajustará de conformidad con la fecha de inicio de la ejecución del plazo contractual. • En caso de no usar centavos, los valores deben aproximarse al mayor Ej. Cumplimiento si el valor a asegurar es $14.980.420,20 aproximar a $14.980.421. • Las garantías deben venir en original. • Anexar el comprobante de pago de la prima

10.5 INDICACIÓN DE SI LA CONTRATACIÓN ESTA COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE PARA COLOMBIA

Los acuerdos comerciales que aplican al presente proceso de contratación, conforme al Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación expedido por Colombia Compra Eficiente (CCE-EICP-MA-03), son los siguientes:

Acuerdo Comercial		Entidad Estatal incluida	Umbral	Excepción aplicable	Proceso de Contratación cubierto
Alianza Pacífico	Chile	SI	SI	SI	**NO**
	México	SI	SI	SI	**NO**
	Perú	SI	SI	SI	**NO**
Canadá		SI	SI	SI	**NO**
Chile		SI	SI	SI	**NO**
Corea		SI	SI	SI	**NO**
Costa Rica		SI	SI	SI	**NO**
Estados Unidos		SI	SI	SI	**NO**
Estados AELC		SI	SI	SI	**NO**
México		SI	SI	NO	**SI**
Triángulo Norte	El Salvador	SI	SI	NO	**SI**
	Guatemala	SI	SI	NO	**SI**
	Honduras	NO	N/A	N/A	**NO**

Acuerdo Comercial	Entidad Estatal incluida	Umbral	Excepción aplicable	Proceso de Contratación cubierto
Unión Europea	SI	SI	SI	**NO**
Israel	SI	SI	SI	**NO**
Reino Unido Irlanda del Norte	SI	SI	SI	**NO**
Comunidad Andina	SI	SI	NO	**SI**

México (Acuerdo de Complementación Económica ACE 33 / TLC Colombia — México)

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $341.973.443 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
No se identifica excepción del Anexo 4 aplicable a este Acuerdo para el presente objeto contractual	**NO**	No se configura ninguna de las excepciones del Anexo 4 del Manual. El objeto contractual (operación de SOC y servicios de ciberseguridad gestionada) no corresponde a servicios excluidos, y el INVIAS no figura excluido como entidad en el texto del Acuerdo.	**SÍ COBIJADO**

El Salvador (Tratado de Libre Comercio Colombia — Triángulo Norte, componente El Salvador)

Conforme a la Nota 4 del documento de umbrales vigentes de Colombia Compra Eficiente, el Acuerdo con el Triángulo Norte de Centroamérica (El Salvador, Guatemala y Honduras) no tiene umbrales establecidos para su aplicabilidad, por lo que el Proceso resulta cobijado

independientemente de su valor estimado, quedando sujeto únicamente a la revisión de las excepciones aplicables.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
No se identifica excepción del Anexo 4 aplicable a este Acuerdo para el presente objeto contractual	**NO**	No se configura ninguna de las excepciones del Anexo 4 del Manual. El objeto contractual (operación de SOC y servicios de ciberseguridad gestionada) no corresponde a servicios excluidos, ni exclusión nominal del INVIAS como entidad cobijada.	**SÍ COBIJADO**

Guatemala (Tratado de Libre Comercio Colombia — Triángulo Norte, componente Guatemala)

Conforme a la Nota 4 del documento de umbrales vigentes, el Acuerdo no tiene umbral establecido, por lo que el Proceso resulta cobijado independientemente de su valor, quedando sujeto a la revisión de las excepciones aplicables.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
No se identifica excepción del Anexo 4 aplicable a este Acuerdo para el presente objeto contractual	**NO**	No se configura ninguna de las excepciones del Anexo 4 del Manual. El objeto contractual (operación de SOC y servicios de ciberseguridad gestionada) no corresponde a servicios excluidos, ni exclusión nominal del INVIAS como entidad cobijada.	**SÍ COBIJADO**

Comunidad Andina (CAN)

El régimen comunitario de la Comunidad Andina no establece umbrales de aplicación en dólares, operando bajo un régimen de contratación pública comunitario propio. Verificado lo anterior, el Proceso resulta cobijado, quedando sujeto a la revisión de las excepciones aplicables.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
No se identifica excepción del Anexo 4 aplicable a este Acuerdo para el presente objeto contractual	**NO**	El régimen de la Comunidad Andina no contempla la excepción 32 ni excluye nominalmente al INVIAS; el proceso queda cobijado en los términos del régimen comunitario de contratación pública.	**SÍ COBIJADO**

Alianza del Pacífico (componentes Chile, México y Perú)

El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $272.951.066 COP (componentes Chile y México) y $518.607.026 COP (componente Perú). Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo en sus tres componentes, quedando sujeto a la revisión de las excepciones aplicables.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Canadá

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $433.332.253 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual

el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Chile (bilateral)

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $272.764.794 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de

procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Corea

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $382.000.000 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En

consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Costa Rica

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $432.974.981 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la

disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Estados Unidos

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $439.974.981 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado

garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Estados AELC (Asociación Europea de Libre Comercio)

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $735.297.922 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los

equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Unión Europea

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $735.297.922 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que

esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Reino Unido de Gran Bretaña e Irlanda del Norte

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación (CCE-EICP-MA-07 V.02), el primer paso del análisis consiste en verificar si el valor estimado del Proceso de Contratación supera el umbral establecido para el respectivo Acuerdo Comercial. El umbral vigente 2026-2027 para entidades del nivel central en bienes y servicios es de $709.188.464 COP. Verificado lo anterior frente al valor estimado de $ 6.030.164.927 COP, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables que se desarrolla a continuación.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de

Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Israel

De conformidad con el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación, el umbral aplicable para entidades del nivel central en bienes y servicios corresponde a 130.000 Derechos Especiales de Giro (DEG), convertidos a pesos colombianos utilizando la Tasa Representativa del Mercado (TRM) del día anterior a la fecha de publicación del aviso de convocatoria del presente proceso, conforme a la fórmula establecida por la Oficina de Asuntos Legales Internacionales (OALI). Dado que el valor estimado del proceso ($ 6.030.164.927 COP) supera ampliamente cualquier valor razonable resultante de dicha conversión, el Proceso resulta provisionalmente cobijado por el presente Acuerdo, quedando sujeto a la revisión de las excepciones aplicables.

El Decreto 1292 de 2021, en su Artículo 2°, asigna al INVIAS las funciones de adelantar investigaciones, estudios, análisis y proyectos para aportar lineamientos técnicos al sector (numeral 2.4) y de impulsar la innovación y sostenibilidad por medio de la investigación e implementación de nuevas tecnologías, proponiendo soluciones a las problemáticas de infraestructura de transporte (numeral 2.21). El cumplimiento de estas funciones depende de la capacidad institucional del INVIAS

para generar, recolectar, transmitir, almacenar y analizar datos técnicos sobre el estado de la red vial nacional, tales como estudios de tránsito, pavimento, puentes, riesgo vial y sostenibilidad ambiental. La infraestructura tecnológica objeto de este proceso — el Centro de Operaciones de Seguridad y sus componentes asociados (SIEM, SOAR/IRP, inteligencia de amenazas, gestión de vulnerabilidades, AntiDDoS, WAF y NAC) — constituye el mecanismo mediante el cual se protege la confidencialidad, integridad y disponibilidad de los sistemas, plataformas y repositorios en los que esa información técnica y científica se genera, procesa, almacena y pone a disposición de los equipos técnicos del Instituto. La operación continua del servicio de ciberseguridad contratado garantiza que dicha infraestructura no sea comprometida, interrumpida o vulnerada, preservando la disponibilidad de los sistemas que procesan la información científica y técnica del Instituto. En consecuencia, el objeto contractual constituye el soporte tecnológico habilitante de la función de procesamiento de datos técnicos, encuadrando dentro de la Clase 8596 del CPC, razón por la cual el presente proceso queda excluido de la cobertura de los acuerdos comerciales que contemplan la excepción número 32 del Anexo 4 del Manual.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
Clase 8596 — Servicios de procesamiento de datos requeridos en la ejecución de actividades científicas y tecnológicas (CPC v1.0, División 81, Grupo 835)	**SÍ**	El objeto contractual encuadra en la Clase CPC 8596 (soporte tecnológico habilitante de la protección del procesamiento de datos técnicos y científicos del INVIAS), configurando la excepción número 32 del Anexo 4 del Manual.	**NO COBIJADO**

Honduras (Tratado de Libre Comercio Colombia — Triángulo Norte, componente Honduras)

Conforme a la Nota 4 del documento de umbrales vigentes, el Acuerdo con el Triángulo Norte de Centroamérica no tiene umbrales establecidos para su aplicabilidad. A diferencia de los demás acuerdos analizados, la exclusión del presente Proceso respecto de Honduras no obedece a la excepción número 32 del Anexo 4, sino a que el propio Manual excluye nominalmente al INVIAS de la lista de Entidades Estatales cobijadas por este Acuerdo.

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
…así como las Entidades Estatales adscritas a estos,	**SÍ**	El INVIAS está expresamente excluido por nombre de la lista de entidades cobijadas por el Acuerdo	**NO COBIJADO**

Excepción del Anexo 4 analizada	¿Aplica?	Razón	Resultado
excepto el Instituto Nacional de Vías — INVIAS—.		con Honduras, independientemente del objeto contractual.	

Cuadro consolidado final

#	Acuerdo Comercial	Motivo	Resultado
1	México (ACE 33 / TLC Colombia — México)	No aplica excepción del Anexo 4	**SÍ COBIJADO**
2	El Salvador (TLC Triángulo Norte)	No aplica excepción del Anexo 4	**SÍ COBIJADO**
3	Guatemala (TLC Triángulo Norte)	No aplica excepción del Anexo 4	**SÍ COBIJADO**
4	Comunidad Andina (CAN)	No aplica excepción del Anexo 4	**SÍ COBIJADO**
5	Alianza del Pacífico (Chile, México, Perú)	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
6	Canadá	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
7	Chile (bilateral)	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
8	Corea	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
9	Costa Rica	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
10	Estados Unidos	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
11	Estados AELC (EFTA)	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
12	Unión Europea	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**

#	Acuerdo Comercial	Motivo	Resultado
13	Reino Unido de Gran Bretaña e Irlanda del Norte	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
14	Israel	Excepción 32, Anexo 4 (CPC 8596)	**NO COBIJADO**
15	Honduras (TLC Triángulo Norte)	Exclusión nominal del INVIAS en el Acuerdo	**NO COBIJADO**

Del análisis efectuado sobre los quince (15) Acuerdos Comerciales vigentes para Colombia, conforme a la metodología del Manual CCE-EICP-MA-07 V.02 y a un valor estimado del proceso de $ 6.030.164.927 COP, se concluye que el presente Proceso de Contratación queda cobijado únicamente por los Acuerdos suscritos con México (bilateral), El Salvador, Guatemala y la Comunidad Andina.

Los diez (10) Acuerdos restantes — Alianza del Pacífico, Canadá, Chile (bilateral), Corea, Costa Rica, Estados Unidos, Estados AELC, Unión Europea, Reino Unido de Gran Bretaña e Irlanda del Norte e Israel — quedan excluidos en virtud de la excepción número 32 del Anexo 4 del Manual, por corresponder el objeto contractual a servicios de ciberseguridad gestionada que constituyen soporte tecnológico habilitante del procesamiento de datos científicos y técnicos del INVIAS, encuadrados en la Clase 8596 del CPC.

El Acuerdo con Honduras queda excluido por una razón distinta e independiente del objeto contractual: el propio Manual excluye nominalmente al INVIAS de la lista de Entidades Estatales cobijadas por dicho Acuerdo.

En consecuencia, la Entidad deberá aplicar el principio de trato nacional y las reglas procedimentales derivadas exclusivamente frente a los cuatro (4) Acuerdos identificados como aplicables, y tramitar el Proceso conforme a las reglas generales de la Selección Abreviada Subasta Inversa Electrónica respecto de los demás Acuerdos analizados.

11. GLOSARIO ESPECÍFICO

- **AntiDDoS (Mitigación de Ataques de Denegación de Servicio Distribuido):** Sistema que detecta y contiene ataques volumétricos, de protocolo o de reflexión dirigidos a saturar el ancho de banda o los recursos de procesamiento de una infraestructura, protegiendo la disponibilidad de los servicios expuestos a internet.

- **ANS (Acuerdo de Nivel de Servicio):** Compromiso formal que establece los tiempos máximos de detección y respuesta ante un evento de seguridad, diferenciados según su severidad.
- **APT (Amenaza Persistente Avanzada):** Ataque cibernético sofisticado, dirigido y sostenido en el tiempo, en el cual un actor malicioso mantiene presencia oculta dentro de una red durante períodos prolongados con el fin de exfiltrar información o comprometer sistemas críticos.
- **CAN (Comunidad Andina):** Organismo de integración regional conformado por Colombia, Bolivia, Ecuador y Perú, cuyo régimen comunitario incluye disposiciones en materia de contratación pública.
- **colCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia):** Ente coordinador nacional de ciberseguridad y ciberdefensa de Colombia, creado en el marco del CONPES 3701 de 2011, miembro pleno de FIRST desde 2013.
- **CONPES (Consejo Nacional de Política Económica y Social):** Máxima autoridad de planeación en Colombia, cuyos documentos orientan la política pública del país en distintas materias, incluida la seguridad digital.
- **CPC (Clasificador Central de Productos):** Sistema de clasificación de bienes y servicios de las Naciones Unidas, utilizado en el Manual de Acuerdos Comerciales de Colombia Compra Eficiente para identificar excepciones sectoriales a la aplicación de dichos acuerdos.
- **CSIRT / CERT (Equipo de Respuesta a Incidentes de Seguridad Informática):** Equipo especializado en la coordinación y gestión de la respuesta a incidentes de ciberseguridad dentro de una organización o a nivel nacional.
- **CVSS (Common Vulnerability Scoring System):** Sistema estandarizado de puntuación de severidad de vulnerabilidades informáticas, mantenido por FIRST y adoptado universalmente por la industria.
- **DEG (Derechos Especiales de Giro):** Unidad de cuenta internacional definida por el Fondo Monetario Internacional, utilizada por algunos acuerdos comerciales para establecer sus umbrales de aplicación.
- **EDR/XDR (Endpoint Detection and Response / Extended Detection and Response):** Plataforma de detección y respuesta avanzada en equipos de cómputo y servidores, con capacidad de correlación extendida hacia red, correo electrónico y nube.
- **FIRST (Forum of Incident Response and Security Teams):** Organización internacional que agrupa a más de 800 equipos de respuesta a incidentes de seguridad en más de 110 países, y que mantiene estándares de adopción universal como el CVSS y el TLP.
- **IoC (Indicador de Compromiso):** Evidencia técnica —dirección IP, dominio, hash de archivo, entre otros— que revela la presencia o actividad de una amenaza cibernética.

- **IoT (Internet de las Cosas):** Conjunto de dispositivos conectados a una red —cámaras, sensores, sistemas de control de acceso físico, entre otros— que, por su naturaleza, no admiten agentes de seguridad tradicionales.
- **IRP (Incident Response Platform):** Módulo de gestión del ciclo de vida de los incidentes de seguridad, que documenta de manera estructurada cada caso desde su apertura hasta su cierre.
- **ISO/IEC 27001:** Norma técnica internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información, certificable por organismos acreditados.
- **MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones):** Entidad rectora de la política de tecnologías de la información en Colombia.
- **MSPI (Modelo de Seguridad y Privacidad de la Información):** Modelo adoptado mediante la Resolución 500 de 2021, habilitador de la Política de Gobierno Digital, fundamentado en la norma ISO/IEC 27001.
- **MSSP (Managed Security Service Provider):** Proveedor especializado en la prestación de servicios de seguridad gestionada, que opera un SOC en nombre de la entidad contratante.
- **MTTD (Mean Time To Detect):** Tiempo promedio transcurrido entre la ocurrencia de un evento de seguridad y su detección.
- **MTTR (Mean Time To Respond):** Tiempo promedio transcurrido entre la detección de un evento de seguridad y su contención efectiva.
- **NAC (Network Access Control):** Solución de control de acceso a la red que verifica la identidad y la postura de seguridad de todo dispositivo antes de permitirle conectarse, y que segmenta la infraestructura según el perfil de riesgo de cada dispositivo.
- **NIST (National Institute of Standards and Technology):** Instituto Nacional de Estándares y Tecnología de los Estados Unidos, desarrollador del NIST Cybersecurity Framework (NIST CSF), marco de referencia de adopción global para la gestión del riesgo cibernético.
- **OT (Operational Technology / Tecnología Operativa):** Tecnología utilizada para el control y monitoreo de dispositivos y procesos físicos, cuya seguridad requiere un tratamiento técnico diferenciado al de los sistemas de tecnología de la información tradicional.
- **Playbook:** Flujo de trabajo predefinido que automatiza una secuencia de acciones de contención ante un tipo específico de amenaza de seguridad.
- **RUP (Registro Único de Proponentes):** Registro que acredita la experiencia, capacidad financiera y organizacional de personas naturales y jurídicas que participan en procesos de contratación pública en Colombia.
- **SASE (Secure Access Service Edge):** Modelo de seguridad que integra funciones de red y seguridad en un servicio unificado entregado desde la nube, aplicado a la conexión segura de sedes distribuidas.

- **SD-WAN (Software-Defined Wide Area Network):** Tecnología de red de área extensa definida por software, que optimiza y asegura la conectividad entre sedes geográficamente distribuidas.
- **SIEM (Security Information and Event Management):** Plataforma que recolecta, normaliza y correlaciona en tiempo real los eventos de seguridad generados por la totalidad de la infraestructura tecnológica de una organización.
- **SMMLV (Salario Mínimo Mensual Legal Vigente):** Unidad de referencia utilizada en Colombia para expresar valores contractuales en procesos de contratación pública.
- **SOAR (Security Orchestration, Automation and Response):** Plataforma que orquesta y automatiza la ejecución de acciones de contención ante amenazas confirmadas, mediante flujos de trabajo predefinidos (playbooks).
- **SOC (Security Operations Center / Centro de Operaciones de Seguridad):** Función organizacional, tecnológica y de talento humano especializado que monitorea, detecta, analiza y responde de manera continua ante eventos de seguridad de la información.
- **Threat Hunting (Búsqueda proactiva de amenazas):** Ejercicio mediante el cual especialistas examinan deliberadamente una infraestructura en busca de indicios de compromisos que no hayan activado alertas automáticas.
- **Threat Intelligence (Inteligencia de amenazas):** Servicio que provee información actualizada y contextualizada sobre las tácticas, técnicas y procedimientos utilizados por actores de amenaza a nivel global.
- **TLP (Traffic Light Protocol):** Protocolo estandarizado de clasificación y manejo de información sensible de inteligencia de amenazas, mantenido por FIRST.
- **TLC (Tratado de Libre Comercio):** Acuerdo comercial internacional suscrito por Colombia que puede incluir compromisos en materia de contratación pública.
- **WAF (Web Application Firewall / Firewall de Aplicaciones Web):** Solución que protege las aplicaciones institucionales expuestas a internet frente a los principales vectores de ataque a aplicaciones web.
- **Zero Trust:** Modelo de seguridad basado en el principio de verificación continua de identidad y postura de seguridad, sin conceder confianza implícita a ningún dispositivo o usuario por su ubicación dentro de la red.

12. ANEXOS

Se anexa al presente estudio previo los siguientes anexos:

A. ANEXO TÉCNICO
B. FORMATO 1 – CARTA DE PRESENTACION DE LA OFERTA
C. FORMATO 2 – CONFORMACION DE PROPONENTE PLURAL (Formato2A –

Consorcios) (Formato 2B – Uniones Temporales)

D. FORMATO 3 – CUMPLIMIENTO ANEXO TÉCNICO
E. FORMATO 4 – PAGOS DE SEGURIDAD SOCIAL Y APORTES LEGALES
F. COTIZACIONES
G. MATRIZ DE RIESGOS
H. FORMULARIO 1 – PRESUPUESTO OFICIAL
I. FORMULARIO 2 – OFERTA ECONÓMICA
J. FORMULARIO 3 – EXPERIENCIA
K. FORMATO 5 – CAPACIDAD FINANCIERA Y ORGANIZACIONAL PARA PROPONENTE EXTRANJERO
L. FORMATO - INFORMACION PARTICIPACION DE SOCIEDADES CONTROLANTES Y CONTROLADAS

Bogotá D. C., 5 de noviembre de 2026

ALVAREZ VELEZ LEONARDO RODOLFO

LEONARDO RODOLFO ALVAREZ VÉLEZ
Jefe Oficina de Tecnologías de la Información y las Comunicaciones (E)

Revisó y Proyectó Coordinador Grupo de Servicios Tecnológicos	José Ernesto Chauta Martínez	
Proyectó Contratista OTIC:	Andrés Felipe Munevar Cortés	
Proyectó Contratista OTIC:	Vanessa Alejandra Mondragón Arévalo	
Proyectó Contratista OTIC:	Jorge Miguel Garcia Aguilar	

Instituto Nacional de Vías - INVIAS
Dirección: Calle 25G # 73B-90, Bogotá D.C., Colombia
Conmutador: (+57) 601 377 0600
Línea Gratuita: (+57) 01 8000 117844