ESTUDIO DE SECTOR

OBJETO	Aunar esfuerzos técnicos, administrativos y financieros entre la Superintendencia de Transporte y la Agencia Nacional Digital – AND, para implementar la Fase II del proyecto institucional de ciberseguridad, orientada al fortalecimiento integral de la gestión de seguridad digital de la Entidad, mediante la adopción y puesta en operación de lineamientos, controles, procedimientos, capacidades y transferencia de conocimiento que permitan proteger los activos de información, fortalecer la resiliencia tecnológica institucional y asegurar la prevención, detección, respuesta y recuperación frente a riesgos y amenazas cibernéticas, en concordancia con los resultados del diagnóstico y el plan de mejoramiento definidos en la Fase I.
FECHA DE ELABORACIÓN	Enero 2026

CONTENIDO

INTRODUCCIÓN
1. DEFINICIÓN DE LA NECESIDAD
2. ASPECTOS GENERALES DEL SECTOR
3. ANÁLISIS DE LA OFERTA
4. ANALISIS DE LA DEMANDA
5. ANÁLISIS DEL SECTOR PARA DETERMINAR OTROS CRITERIOS DIFERENCIALES Y APLICACIÓN DE NORMATIVIDAD QUE LE APLIQUE (según corresponda)
6. FUNDAMENTO TEÓRICO Y METODOLOGIA UTILIZADA PARA ANÁLISIS DE PRECIOS
7. CONCLUSIONES Y/O RECOMENDACIONES
8. FUENTES DE INFORMACIÓN
9. ANEXOS

INTRODUCCIÓN

El artículo 2.2.1.1.1.6.1 del Decreto 1082 de 2015 establece el deber que tienen las Entidades Estatales de realizar un análisis para conocer el sector relativo al objeto del Proceso de Contratación desde la perspectiva legal, comercial, financiera, organizacional, técnica y de análisis de riesgo. En este sentido, se entiende a un sector como el conjunto de empresas que ofrecen diferentes productos o servicios que solucionan una necesidad en un mercado. De esta manera, el Estudio del Sector permite identificar las oportunidades disponibles en el mercado para atender la necesidad de la Entidad Estatal.

De acuerdo con lo anterior, dentro del proceso de estructuración se tuvieron en cuenta 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, dando cumplimiento a lo ordenado en el Artículo 2.1.4.3.2.1. del decreto 1600 de 2024, por medio del cual "(…) se modifica el Capítulo 1 y 3 del Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, Decreto Reglamentario Único del Sector Presidencia de la República, en lo relacionado con las Subcomisiones Técnicas de la Comisión Nacional de Moralización y la Estrategia Nacional de Lucha Contra la Corrupción.

1. DEFINICIÓN DE LA NECESIDAD

La Superintendencia de Transporte, en el ejercicio de sus funciones misionales de inspección, vigilancia y control del sector transporte, enfrenta desafíos crecientes asociados a la transformación digital de sus procesos, la gestión de información sensible y el aseguramiento de la continuidad de los servicios institucionales en un entorno caracterizado por riesgos cibernéticos cada vez más complejos y sofisticados.

La progresiva digitalización de los procedimientos de supervisión, sanción, atención al ciudadano e interoperabilidad con otras entidades del Estado ha incrementado la dependencia de infraestructuras tecnológicas, sistemas de información y servicios digitales, los cuales constituyen activos estratégicos cuya confidencialidad, integridad y disponibilidad resultan esenciales para garantizar la eficiencia administrativa, la transparencia institucional y la confianza digital de la ciudadanía.

En este contexto, la Entidad ha identificado la necesidad de fortalecer su infraestructura tecnológica y su gestión de la seguridad digital, con el fin de asegurar la resiliencia de los servicios tecnológicos, la protección de los datos institucionales y la adecuada respuesta frente a incidentes de seguridad de la información. Esta necesidad se enmarca en los lineamientos del Plan Nacional de Desarrollo 2022–2026 “Colombia Potencia Mundial de la Vida” (Ley 2294 de 2023), el cual reconoce la transformación digital y la ciberseguridad como ejes transversales para la modernización del Estado, así como en las políticas nacionales de Gobierno Digital, Confianza y Seguridad Digital.

De manera específica, el Plan Estratégico de Tecnologías de la Información – PETI 2023–2026, aprobado por el Comité Institucional de Gestión y Desempeño, prioriza el fortalecimiento de la seguridad y privacidad de la información como componente esencial de la arquitectura tecnológica institucional. Dicho plan establece acciones orientadas al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), la ejecución de pruebas de vulnerabilidad y penetración, la gestión de incidentes, la actualización de controles de seguridad y el desarrollo de capacidades institucionales en ciberseguridad, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano.

En desarrollo de estos lineamientos, la Superintendencia de Transporte adelantó previamente la Fase I del proyecto de ciberseguridad, mediante la cual se realizó un diagnóstico técnico que permitió identificar el nivel de madurez institucional, las brechas existentes, los riesgos asociados a la infraestructura tecnológica y a los sistemas de información, así como la necesidad de adoptar medidas técnicas, organizacionales y procedimentales para fortalecer su postura de seguridad digital. Como resultado de esta fase, se definió un plan de mejoramiento, evidenciando que la gestión de la seguridad digital no podía limitarse a ejercicios de evaluación, sino que requería avanzar hacia una fase de implementación efectiva y controlada.

En consecuencia, surge la necesidad de desarrollar la Fase II del proyecto de ciberseguridad, orientada a materializar, consolidar e implementar los lineamientos, controles, procedimientos y capacidades identificadas como prioritarias en el diagnóstico previo. La no ejecución de esta fase implicaría mantener a la Entidad en un escenario de riesgo conocido, sin medidas suficientes de mitigación, lo cual resulta incompatible con los principios de eficiencia, prevención del daño y gestión responsable de los recursos públicos.

La necesidad que se pretende satisfacer no corresponde a la contratación de servicios aislados ni a actividades rutinarias, sino a la continuación lógica, técnica y metodológicamente justificada de un proceso institucional previamente iniciado, que exige coherencia, articulación con los resultados ya obtenidos y una ejecución que garantice la apropiación institucional del conocimiento y la sostenibilidad de la gestión de la seguridad digital en el mediano y largo plazo.

En este marco, se hace necesaria la articulación interinstitucional mediante la suscripción de un convenio específico derivado con la Agencia Nacional de Gobierno Digital, que permita Aunar esfuerzos técnicos, administrativos y financieros entre la Superintendencia de Transporte y la Agencia Nacional Digital – AND, para implementar la Fase II del proyecto institucional de ciberseguridad, orientada al fortalecimiento integral de la gestión de seguridad digital de la Entidad, mediante la adopción y puesta en operación de lineamientos, controles, procedimientos, capacidades y transferencia de conocimiento que permitan proteger los activos de información, fortalecer la resiliencia tecnológica institucional y asegurar la prevención, detección, respuesta y recuperación frente a riesgos y amenazas cibernéticas, en concordancia con los resultados del diagnóstico y el plan de mejoramiento definidos en la Fase I.

El propósito final de esta contratación es garantizar la protección de la información institucional, la continuidad de los servicios misionales y la resiliencia tecnológica de la Entidad frente a amenazas cibernéticas, contribuyendo a una gestión pública más segura, eficiente y confiable, alineada con los lineamientos normativos y estratégicos del Estado colombiano.

2. ASPECTOS GENERALES DEL SECTOR

a. Aspectos de Tipo Económico (Macroeconómico y Microeconómico)

El sector objeto del presente estudio corresponde al sector de ciberseguridad y seguridad digital en el ámbito del Estado colombiano, entendido como el conjunto de políticas, capacidades institucionales, marcos normativos, procesos técnicos y mecanismos de coordinación orientados a garantizar la protección de los activos de información, la continuidad de los servicios digitales y la resiliencia tecnológica de las entidades públicas frente a riesgos y amenazas cibernéticas.

Este sector se caracteriza por su naturaleza estratégica y transversal, en la medida en que soporta el funcionamiento de los procesos misionales de las entidades estatales y habilita la transformación

digital. A diferencia de otros sectores económicos, la ciberseguridad en el ámbito público no se limita a la provisión de bienes o servicios tecnológicos, sino que involucra la gestión integral del riesgo digital, la adopción de estándares técnicos, la gobernanza institucional y la articulación interadministrativa.

Desde el punto de vista institucional, el sector de la seguridad digital en Colombia se encuentra fuertemente regulado y coordinado por el Gobierno Nacional, a través de políticas públicas, lineamientos técnicos y modelos de referencia que orientan la actuación de las entidades del Estado. En este marco, la ciberseguridad se configura como una responsabilidad institucional permanente, cuya implementación requiere capacidades técnicas especializadas, conocimiento del entorno normativo y experiencia en la gestión de infraestructuras y sistemas de información del sector público.

Así mismo, el sector presenta una alta especificidad técnica, dado que las soluciones de seguridad digital deben ser diseñadas e implementadas de manera contextualizada, atendiendo el nivel de madurez institucional, la arquitectura tecnológica existente y los riesgos particulares de cada entidad. En consecuencia, no se trata de soluciones estandarizadas de mercado, sino de estrategias integrales que combinan evaluación, implementación, seguimiento y mejora continua.

En este contexto, la ejecución de proyectos de ciberseguridad en entidades públicas se desarrolla, de manera predominante, a través de esquemas de articulación interinstitucional, que permiten aunar esfuerzos técnicos, administrativos y financieros, aprovechar capacidades instaladas del Estado y garantizar la alineación con las políticas nacionales de Gobierno Digital, Confianza y Seguridad Digital.

Por lo anterior, el sector objeto de análisis se estructura bajo un enfoque de colaboración estatal, en el cual entidades públicas con competencias técnicas especializadas actúan como aliados estratégicos para el fortalecimiento de las capacidades institucionales de otras entidades, garantizando la sostenibilidad de las soluciones implementadas y la apropiación del conocimiento al interior de la administración pública.

Con el fin de clasificar y contextualizar la necesidad de contratación dentro del Sistema de Clasificación de las Naciones Unidas (UNSPSC), se identifican los siguientes códigos, los cuales guardan relación directa con el objeto contractual y con los componentes definidos en el Anexo Técnico:

CÓDIGO	***SEGMENTO***	***FAMILIA***	***CLASE***	***PRODUCTO***
80101507	Servicios de Gestión, Servicios Profesionales	Servicios de asesoría de gestión	Servicios de consultoría de negocios y administración	Servicios de asesoramiento sobre tecnologías de la información

CÓDIGO	***SEGMENTO***	***FAMILIA***	***CLASE***	***PRODUCTO***
	de Empresa y Servicios Administrativos		corporativa	
93151512	Servicios políticos y de asuntos cívicos	servicios de administración y financiación pública	Administración pública	Servicios de instituciones publicas
93151508	Servicios políticos y de asuntos cívicos	servicios de administración y financiación pública	Administración pública	Servicios de departamentos gubernamentales
93151505	Servicios políticos y de asuntos cívicos	servicios de administración y financiación pública	Administración pública	Servicios de organismos administrativos
81102702	Servicios basados en ingeniería, investigación y tecnología	Servicios profesionales de ingeniería y arquitectura	Servicios de diseño e ingeniería de sistemas instrumentados de control	Servicios de ingeniería y diseño para sistemas de control de procesos
81111800	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	No aplica
81111808	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	Servicios de análisis de sistemas
81111500	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Ingeniería de software o hardware	No aplica

Análisis Macroeconómico

El sector de tecnologías de la información y las comunicaciones (TIC), particularmente en lo relacionado con la ciberseguridad y la seguridad digital, se desarrolla en un contexto macroeconómico caracterizado por la creciente digitalización de los procesos productivos, administrativos y de prestación de servicios, tanto en el ámbito público como privado. Esta dinámica ha consolidado a los servicios tecnológicos como un componente estratégico para la eficiencia institucional, la continuidad operativa y la sostenibilidad de la gestión pública.

En primer lugar, **la inflación (Índice de Precios al Consumidor – IPC)**, constituye una variable macroeconómica relevante para el sector de tecnologías de la información y las comunicaciones (TIC), particularmente en lo relacionado con los servicios especializados de ciberseguridad y seguridad digital, en la medida en que incide directamente en la estructura de costos asociada a la planeación, implementación y sostenibilidad de este tipo de proyectos.

El incremento del IPC impacta principalmente los costos laborales, operativos y administrativos vinculados a la prestación de servicios de ciberseguridad, los cuales dependen en alta medida de talento humano altamente especializado, perfiles técnicos y profesionales con formación avanzada y experiencia específica en gestión del riesgo tecnológico, seguridad de la información, análisis de vulnerabilidades y respuesta a incidentes. Así mismo, la inflación afecta los costos asociados a la operación continua de infraestructuras tecnológicas, actividades de monitoreo, soporte técnico especializado, capacitación y transferencia de conocimiento.

De igual forma, el comportamiento del IPC incide en los costos de mantenimiento, actualización y fortalecimiento de las capacidades de seguridad digital, así como en la adquisición y uso de herramientas, servicios tecnológicos complementarios y recursos necesarios para garantizar la resiliencia, disponibilidad y confiabilidad de los sistemas de información y de la infraestructura crítica de las entidades públicas.

Índice de Precios al Consumidor (IPC)

Variación anual y mensual
Total nacional
2024 - 2025 (diciembre)

IPC	Diciembre			
	Variación anual		Variación mensual	
	2024	2025	2024	2025
IPC total	5,20	**5,10**	0,46	**0,27**

Fuente: DANE, IPC

En diciembre de 2025 la variación anual del IPC fue 5,10%, y la variación mensual 0,27%.
En diciembre de 2025 la variación anual del IPC fue 5,10%, es decir, 0,10 puntos porcentuales menor que la reportada en el mismo periodo del año anterior, cuando fue de 5,20%.
El comportamiento anual del IPC total en diciembre de 2025 (5,10%) se explicó principalmente por la variación anual de las divisiones Alojamiento, agua, electricidad, gas y otros combustibles y Alimentos y bebidas no alcohólicas.

Fuente: Dane.gov.co[1]

De acuerdo con la información publicada por el DANE, en diciembre de 2025 la variación anual del Índice de Precios al Consumidor (IPC) total nacional fue del 5,10%, lo que evidencia una leve desaceleración frente al mismo periodo del año 2024, cuando se ubicó en 5,20%, representando una disminución de 0,10 puntos porcentuales. Este comportamiento indica una moderación en las presiones inflacionarias al cierre del año 2025, aunque se mantiene un nivel de inflación que continúa afectando el poder adquisitivo de los agentes económicos.

[1] https://www.dane.gov.co/index.php/estadisticas-por-tema/precios-y-costos/indice-de-precios-al-consumidor-ipc/ipc-informacion-tecnica

En cuanto a la variación mensual, el IPC registró en diciembre de 2025 un incremento del 0,27%, inferior al observado en diciembre de 2024 (0,46%), lo que refleja una menor aceleración de los precios en el corto plazo. No obstante, este resultado confirma la persistencia de incrementos en el nivel general de precios, acumulados a lo largo del año.
Según el DANE, el comportamiento anual del IPC en diciembre de 2025 estuvo explicado principalmente por las variaciones en las divisiones de alojamiento, agua, electricidad, gas y otros combustibles, así como en alimentos y bebidas no alcohólicas, componentes que tienen un impacto directo sobre el costo de vida de personas naturales y sobre los costos operativos de las personas jurídicas.

En este contexto, la inflación se configura como un factor relevante para la planeación presupuestal y financiera de los proyectos de ciberseguridad, en la medida en que influye en la definición de los valores asociados a la ejecución de las actividades técnicas, al sostenimiento de las capacidades implementadas y a la evaluación de la razonabilidad de los recursos requeridos. No obstante, tratándose de un Convenio Interadministrativo, el impacto del IPC se analiza desde una perspectiva de optimización del gasto público, orientada a la eficiencia, la sostenibilidad y la mitigación de riesgos.

Adicionalmente, **Las tasas de interés del sistema financiero** se encuentran determinadas por las decisiones de política monetaria adoptadas por el Banco de la República. De acuerdo con el Informe de Política Monetaria publicado en octubre de 2025[2], dichas decisiones han estado orientadas a controlar las presiones inflacionarias y preservar la estabilidad macroeconómica, lo cual ha incidido en las condiciones de financiamiento y liquidez de los agentes económicos.

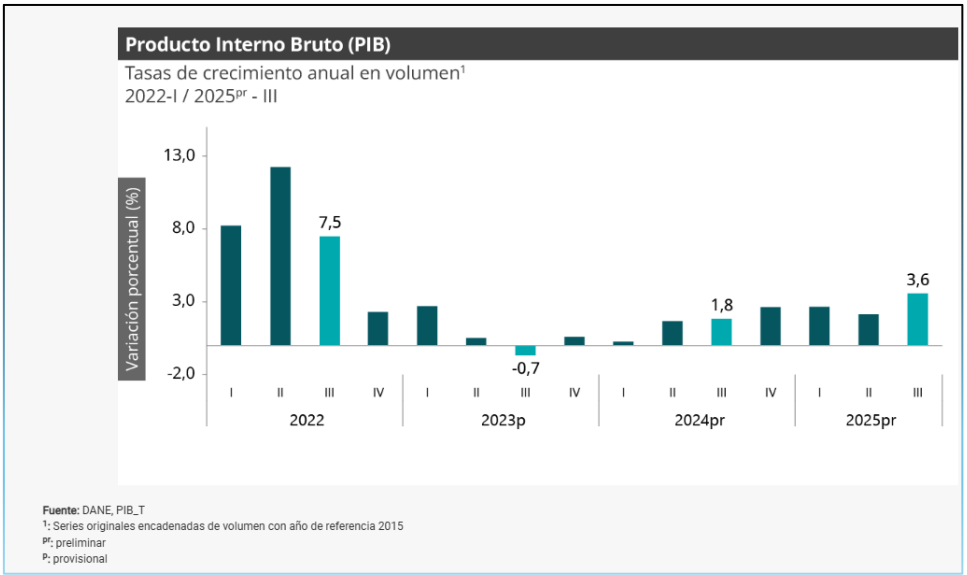
De acuerdo con el Informe de Política Monetaria del Banco de la República, durante el tercer trimestre de 2025 la inflación presentó un aumento superior al esperado, explicado principalmente por mayores ajustes en los precios de los alimentos —especialmente los perecederos— y de algunos bienes, en un contexto de fuerte consumo, presiones de costos laborales y restricciones en la oferta. No obstante, el Emisor mantiene la expectativa de que la inflación continúe reduciéndose gradualmente y se ubique dentro del rango meta entre 2% y 4% en 2026, acercándose al 3% a un ritmo más lento de lo previsto anteriormente.

El informe señala que la economía colombiana ha mantenido una senda de crecimiento, impulsada por el consumo de los hogares, la recuperación de la inversión y un desempeño favorable del mercado laboral, con tasas de desempleo en niveles históricamente bajos. En este contexto, la Junta Directiva ha mantenido una postura cautelosa de la política monetaria, conservando inalterada la tasa de interés de referencia en 9,25%, con el fin de asegurar la convergencia de la inflación hacia la meta y preservar un crecimiento económico sostenible.

[2] https://www.banrep.gov.co/es/serie-publicaciones/informe-politica-monetaria

El contexto descrito incide principalmente en las condiciones de financiamiento, los costos operativos y la planeación presupuestal para el tipo de servicio que requiere la Entidad. La estabilidad relativa de la tasa de interés de referencia y lo que se espera de que la inflación baje gradualmente y se acerque al nivel que el Banco de la República considera normal o saludable (entre 2% y 4%), favorecen escenarios de previsibilidad en los costos asociados al talento humano y al soporte tecnológico, lo cual permite estructurar la contratación bajo criterios de eficiencia, sostenibilidad financiera y razonabilidad del gasto, sin que se evidencien presiones macroeconómicas que afecten de manera significativa la ejecución del objeto contractual.

Por su parte, el **comportamiento del crecimiento económico (PIB),** incide de manera directa en los niveles de inversión pública y en la priorización de proyectos estratégicos, dentro de los cuales la ciberseguridad y la seguridad digital ocupan un lugar central.



Fuente: DANE[3]

De acuerdo con la información publicada por el DANE, el comportamiento del Producto Interno Bruto (PIB) en el periodo comprendido entre el primer trimestre de 2022 y el tercer trimestre de 2025 evidencia una fase de desaceleración posterior a los altos niveles de crecimiento observados en 2022, seguida de una recuperación gradual de la actividad económica.

Durante el año 2022, la economía colombiana registró tasas de crecimiento elevadas, alcanzando variaciones anuales cercanas al 8,0% en el primer trimestre y superiores al 12,0% en el segundo trimestre, reflejando un fuerte dinamismo de la demanda interna. No obstante, hacia el segundo semestre de ese año se observa una moderación del crecimiento, con una variación aproximada

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

del 7,5% en el tercer trimestre y niveles inferiores al 3,0% en el cuarto trimestre, lo que marcó el inicio de un proceso de desaceleración económica.

En 2023, el crecimiento económico continuó perdiendo impulso, registrándose tasas cercanas al 3,0% en los primeros trimestres y una contracción del -0,7% en el tercer trimestre, lo que evidenció un enfriamiento significativo de la actividad productiva. Posteriormente, hacia el cierre del año, el crecimiento se mantuvo en niveles bajos, reflejando un entorno de menor dinamismo económico.

Para 2024, la información preliminar muestra una recuperación gradual del crecimiento, con variaciones positivas que se ubican entre 1,5% y 3,0%, destacándose un crecimiento cercano al 1,8% en el tercer trimestre, lo que sugiere una mejora progresiva en la actividad económica, aunque aún por debajo de los niveles observados en 2022.

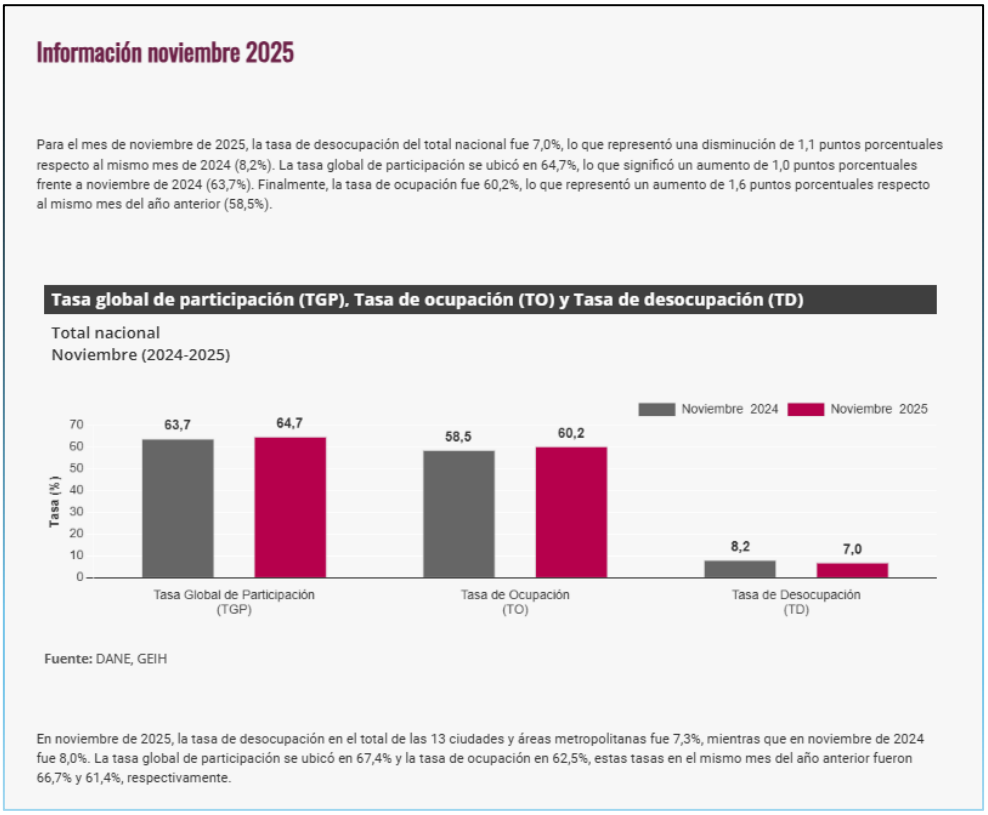
Finalmente, en 2025 (cifras preliminares), el PIB continúa mostrando una tendencia de recuperación, con un crecimiento aproximado del 3,6% en el tercer trimestre, lo que indica un fortalecimiento paulatino de la economía colombiana, soportado por la reactivación del consumo y algunos componentes de la inversión.

De acuerdo con la información del Producto Interno Bruto (PIB), la economía colombiana evidencia un comportamiento de recuperación gradual del crecimiento económico luego de la desaceleración registrada en 2023, con tasas de variación positivas durante 2024 y un crecimiento preliminar del 3,6 % en el tercer trimestre de 2025, lo cual refleja una dinámica económica más favorable y una mayor estabilidad en la actividad productiva.

Con relación a las condiciones del **mercado laboral**, los niveles de empleo, informalidad y disponibilidad de talento humano inciden de manera directa en el sector de tecnologías de la información y las comunicaciones (TIC) y, de forma específica, en los servicios de ciberseguridad y seguridad digital, en la medida en que la ejecución de este tipo de proyectos depende principalmente de perfiles técnicos y profesionales altamente calificados.

Para el análisis del mercado laboral se tiene en cuenta la información más reciente publicada por el DANE correspondiente al mes de noviembre, la cual resulta representativa del comportamiento del empleo durante el año analizado y permite identificar las tendencias del mercado laboral que inciden en la disponibilidad de talento, la estabilidad de los costos laborales y la sostenibilidad en la prestación de los servicios tecnológicos objeto de contratación.

En el sector público, estas condiciones adquieren una relevancia adicional, dado que la gestión de la seguridad digital exige no solo conocimientos técnicos, sino también comprensión del entorno normativo, los procesos administrativos y la arquitectura institucional. En este contexto, un Convenio Interadministrativo permite mitigar los riesgos derivados de la rotación del talento y la escasez de perfiles especializados.



Fuente: DANE[4]

De acuerdo con la información publicada por el DANE, para el mes de noviembre de 2025 el mercado laboral a nivel nacional presentó un comportamiento favorable en comparación con el mismo periodo del año anterior. La tasa de desocupación se ubicó en 7,0%, lo que representó una disminución de 1,1 puntos porcentuales frente a noviembre de 2024, cuando fue del 8,2%, evidenciando una mejora en las condiciones de empleo del país.

De manera complementaria, la tasa global de participación (TGP) alcanzó el 64,7%, registrando un incremento de 1,0 punto porcentual frente a noviembre de 2024 (63,7%), lo cual indica una mayor incorporación de personas en edad de trabajar al mercado laboral. Este comportamiento sugiere un fortalecimiento de la oferta laboral y una mayor disposición de la población para participar activamente en la economía.

Por su parte, la tasa de ocupación (TO) se situó en 60,2%, lo que significó un aumento de 1,6 puntos porcentuales frente al mismo mes del año anterior (58,5%), reflejando una expansión en el número de personas efectivamente ocupadas. Este resultado es consistente con el crecimiento del empleo observado en los últimos meses, especialmente en las principales áreas urbanas.

[4] https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-y-desempleo

En conjunto, la reducción de la tasa de desocupación, junto con el aumento en la participación y en la ocupación, evidencia una dinámica positiva del mercado laboral durante el año 2025.

Finalmente, desde la perspectiva de la **política fiscal**, el Estado enfrenta el reto de garantizar la sostenibilidad de las finanzas públicas, lo cual implica fortalecer la eficiencia en la asignación y ejecución del gasto público, así como optimizar el uso de los recursos disponibles. En este contexto, los lineamientos establecidos en el Marco Fiscal de Mediano Plazo[5], resaltan la importancia de priorizar inversiones que generen eficiencia operativa, fortalezcan los mecanismos de control institucional y contribuyan a una gestión pública moderna, preventiva y orientada a resultados.

En relación con el objeto de la contratación, el fortalecimiento de la ciberseguridad institucional contribuye de manera directa a dichos objetivos fiscales, en la medida en que permite prevenir pérdidas económicas derivadas de incidentes de seguridad digital, interrupciones en la operación de los servicios tecnológicos, afectaciones a la integridad de la información y posibles responsabilidades administrativas o legales. Así mismo, fortalece los mecanismos de control sobre los activos de información y los sistemas críticos, reduciendo riesgos que podrían generar costos adicionales para la Entidad.

Análisis Microeconómico
Desde el punto de vista microeconómico, la prestación de servicios especializados en ciberseguridad y seguridad digital se caracteriza por ser una actividad altamente intensiva en talento humano calificado, cuya ejecución depende principalmente de perfiles técnicos, profesionales y operativos especializados en seguridad de la información, gestión del riesgo tecnológico, análisis y gestión de vulnerabilidades, pruebas de penetración, arquitectura de seguridad, monitoreo y respuesta a incidentes.

En este contexto, la estructura de costos de este tipo de servicios se encuentra determinada, en gran medida, por los costos laborales asociados al talento humano especializado, dado que las actividades de ciberseguridad no corresponden a servicios estandarizados ni automatizables en su totalidad, sino a procesos técnicos que requieren conocimiento experto, experiencia certificada y comprensión del entorno tecnológico e institucional en el cual se implementan. Así mismo, la ejecución de estas actividades exige dedicación continua, coordinación técnica, seguimiento permanente y transferencia de conocimiento a los equipos internos de la Entidad.

Los costos laborales constituyen, por tanto, un componente relevante dentro de la estructura de costos del servicio, siendo el salario mínimo legal vigente, los ajustes salariales del mercado y la disponibilidad de talento especializado referentes para la estimación de los valores asociados a los perfiles requeridos. Las variaciones en dichos costos inciden directamente en los recursos necesarios para la ejecución del proyecto, junto con otros factores como el nivel de especialización requerido, la complejidad técnica de la infraestructura a proteger, la duración de

[5] Marco Fiscal de Mediano Plazo – Ministerio de Hacienda y Crédito Público

las actividades, la continuidad operativa, el soporte técnico especializado y las actividades de documentación y reporte.

Adicionalmente, la naturaleza del servicio implica costos asociados a la gestión técnica del proyecto, la utilización de metodologías especializadas, la coordinación entre equipos multidisciplinarios y la adopción de buenas prácticas y estándares de seguridad reconocidos. En consecuencia, la valoración económica de este tipo de servicios no se basa en la comparación de precios unitarios de mercado, sino en la razonabilidad de los recursos requeridos para garantizar una implementación efectiva, sostenible y alineada con las necesidades institucionales.

En el marco de un convenio interadministrativo, el análisis microeconómico se orienta a la optimización del uso de los recursos públicos, priorizando la eficiencia, la reducción de costos de transacción y el aprovechamiento de capacidades institucionales existentes, más que a la formación de precios bajo criterios de competencia de mercado. Este enfoque resulta consistente con la naturaleza especializada del servicio y con el objetivo de fortalecer de manera estructural las capacidades de ciberseguridad de la Entidad.

Serie ▼	Salario mínimo mensual, sector urbano alto	Salario mínimo mensual, sector rural	Salario mínimo mensual	Auxilio de transporte mensual
Fecha ▼				
31/12/2026	.	.	1.750.905,00	249.095,00
31/12/2025	.	.	1.423.500,00	200.000,00
31/12/2024	.	.	1.300.000,00	162.000,00
31/12/2023	.	.	1.160.000,00	140.606,00
31/12/2022	.	.	1.000.000,00	117.172,00
31/12/2021	.	.	908.526,00	106.454,00
31/12/2020	.	.	877.803,00	102.854,00
31/12/2019	.	.	828.116,00	97.032,00
31/12/2018	.	.	781.242,00	88.211,00
31/12/2017	.	.	737.717,00	83.140,00
31/12/2016	.	.	689.455,00	77.700,00

Fuente: Banco de la República[6]

De acuerdo con la información disponible sobre la evolución del salario mínimo legal mensual vigente (SMLMV) en Colombia, se evidencia una tendencia creciente y sostenida durante el periodo comprendido entre 2016 y 2026. En particular, el salario mínimo pasó de $689.455 en 2016 a $1.423.500 en 2025, y se proyecta en $1.750.905 para 2026, lo que refleja incrementos significativos en los costos laborales a lo largo del tiempo.

De manera complementaria, el auxilio de transporte mensual también ha presentado un aumento progresivo, pasando de $77.700 en 2016 a $200.000 en 2025, y alcanzando $249.095 en 2026,

[6] https://uba.banrep.gov.co/htmlcommons/SeriesHistoricas/mercado-laboral.html

lo cual incrementa el costo total asociado a la vinculación de personal que devenga hasta dos salarios mínimos.

En este contexto, el salario mínimo legal vigente se constituye en un referente fundamental para el análisis microeconómico del sector, dado que permite comprender la evolución de los costos asociados a la prestación del servicio y su incidencia en la estructura de precios, sin que ello implique necesariamente una variación proporcional en la calidad o el alcance del servicio contratado.

Conclusión del análisis económico

El análisis económico evidencia que la contratación orientada al fortalecimiento de la ciberseguridad institucional resulta económicamente viable, pertinente y sostenible, en la medida en que se apoya en un entorno macroeconómico estable y en un enfoque microeconómico que privilegia la eficiencia, la gestión del riesgo y el aprovechamiento de capacidades institucionales del Estado, garantizando la adecuada utilización de los recursos públicos y la sostenibilidad de las capacidades implementadas en el mediano y largo plazo.

b. **Aspectos de Tipo Técnico**

La necesidad para satisfacer implica la planeación, ejecución, seguimiento y cierre de las actividades orientadas al fortalecimiento integral de la ciberseguridad institucional de la Superintendencia de Transporte, conforme a las fases y actividades definidas en el cronograma del convenio.

En consecuencia, se deberá realizar la ejecución de pruebas de penetración internas y externas (pentest) sobre los sistemas, plataformas, aplicaciones, servicios tecnológicos e infraestructura crítica de la entidad, así como la realización de evaluaciones de seguridad, análisis y gestión de vulnerabilidades, con el fin de identificar debilidades técnicas, operativas y procedimentales que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

De igual manera, se deben implementar controles técnicos y procedimentales, mediante la definición e implementación de medidas de mitigación, actividades de hardening, ajustes de configuración, recomendaciones de mejora y adopción de buenas prácticas de seguridad de la información y ciberseguridad, alineadas con estándares y marcos de referencia reconocidos.

De otra parte, la ejecución de las actividades contempla el análisis, validación, documentación y reporte de los hallazgos identificados durante las pruebas y evaluaciones, así como la elaboración de informes técnicos y ejecutivos que permitan a la Superintendencia de Transporte contar con información clara, oportuna y trazable para la toma de decisiones y el seguimiento a la implementación de las recomendaciones.

Finalmente, la ejecución de las actividades busca apoyar el adecuado desarrollo de las funciones misionales de Inspección, Vigilancia y Control, garantizando que los procesos institucionales, tanto a nivel central como en las regiones, se soporten en entornos digitales más seguros, resilientes y confiables, contribuyendo al fortalecimiento institucional y a la consolidación de una transformación digital segura.

Las actividades anteriormente descritas se presentan de manera general desde una perspectiva técnica, mientras que los aspectos técnicos, funcionales y operativos específicos, incluyendo el alcance detallado, metodologías, entregables y criterios de ejecución, se encuentran desarrollados en el Anexo Técnico, el cual hace parte integral del presente proceso.

c. **Aspectos de Tipo Ambiental**

El objeto de la presente contratación, orientado al fortalecimiento de la ciberseguridad institucional de la Superintendencia de Transporte, no genera impactos ambientales directos, no obstante, desde una perspectiva ambiental indirecta, el proyecto contribuye de manera positiva a los objetivos de sostenibilidad ambiental, en la medida en que promueve el uso de entornos digitales seguros, la optimización de los sistemas de información y la modernización de los procesos institucionales. Estas acciones favorecen la reducción del consumo de papel, la disminución de desplazamientos físicos asociados a trámites presenciales y la optimización del uso de recursos tecnológicos, lo cual se traduce en una menor huella ambiental de la operación institucional.

Adicionalmente, el fortalecimiento de la seguridad digital permite mejorar la eficiencia en el uso de la infraestructura tecnológica existente, contribuyendo a prácticas de gestión más responsables, tales como la racionalización del uso de equipos, la mejora en los esquemas de operación de los centros de datos y la adopción de buenas prácticas orientadas a la sostenibilidad tecnológica.

En este sentido, si bien la contratación no se encuentra sujeta a requerimientos ambientales específicos, se alinea con los principios de gestión ambiental responsable, eficiencia en el uso de recursos públicos y sostenibilidad, en concordancia con los objetivos de modernización y transformación digital del Estado.

d. **Licencias y permisos**

El objeto de la presente contratación no requiere la obtención de licencias, permisos o autorizaciones administrativas especiales para su ejecución, en tanto no involucra la prestación de servicios sujetos a regulación sectorial específica, ni la realización de actividades que demanden habilitaciones previas por parte de autoridades competentes.

No obstante, la ejecución de las actividades previstas exige el cumplimiento de los lineamientos normativos y técnicos aplicables en materia de seguridad de la información, protección de datos personales y gestión del riesgo digital, así como la observancia de las políticas, procedimientos y controles internos de la Entidad.

De manera particular, las actividades técnicas que impliquen acceso a sistemas de información, plataformas tecnológicas, infraestructura crítica y ejecución de pruebas de seguridad, deberán realizarse previa autorización institucional, bajo esquemas controlados, documentados y trazables, garantizando la confidencialidad, integridad y disponibilidad de la información, de conformidad con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI).

En consecuencia, no se identifican requerimientos de licencias o permisos externos para la ejecución del contrato, más allá del cumplimiento del marco normativo vigente y de las autorizaciones internas necesarias para el desarrollo de las actividades técnicas previstas.

3. ANÁLISIS DE LA OFERTA

a. Reseña del Sector

El sector objeto del presente estudio corresponde al sector de ciberseguridad y seguridad digital en el ámbito del Estado colombiano, entendido como el conjunto de políticas públicas, capacidades institucionales, marcos normativos, procesos técnicos y mecanismos de articulación interadministrativa orientados a garantizar la protección de los activos de información, la continuidad de los servicios digitales y la resiliencia tecnológica de las entidades públicas frente a riesgos y amenazas cibernéticas.

Este sector ha adquirido una relevancia estratégica creciente como resultado de la transformación digital del Estado, la ampliación del uso de medios electrónicos para la prestación de servicios públicos y la interoperabilidad entre sistemas de información institucionales. En este contexto, la ciberseguridad se configura como un componente transversal y habilitador de la gestión pública moderna, en la medida en que permite asegurar la confidencialidad, integridad y disponibilidad de la información, así como la confianza de la ciudadanía en los servicios digitales.

A diferencia de otros sectores económicos, la ciberseguridad en el ámbito público no se limita a la provisión de bienes o servicios tecnológicos estandarizados, sino que involucra la gestión integral del riesgo digital, la adopción de estándares técnicos, la gobernanza de la seguridad de la información y el fortalecimiento de capacidades institucionales. Su desarrollo se encuentra

determinado principalmente por decisiones de política pública, lineamientos normativos y planes estratégicos institucionales, más que por dinámicas de oferta y demanda propias del mercado.

En Colombia, el sector de la seguridad digital se encuentra estructurado a partir de los lineamientos definidos por el Gobierno Nacional en materia de Gobierno Digital, Confianza y Seguridad Digital, así como por la adopción de modelos de referencia como el Modelo de Seguridad y Privacidad de la Información (MSPI), los cuales orientan a las entidades públicas en la implementación de controles, procedimientos y mecanismos de gestión del riesgo tecnológico.

En este marco, la ejecución de proyectos de ciberseguridad en el sector público se desarrolla de manera predominante a través de convenios interadministrativos, que permiten aunar esfuerzos técnicos, administrativos y financieros entre entidades del Estado, aprovechar capacidades institucionales existentes y garantizar la alineación con las políticas nacionales y los objetivos estratégicos de la administración pública

b. **Posibles Proveedores**

Teniendo en cuenta la naturaleza del objeto contractual, orientado a la implementación de la Fase II del proyecto institucional de ciberseguridad, y considerando que se ejecutará mediante la figura de convenio interadministrativo.

En este contexto, la Agencia Nacional de Gobierno Digital se identifica como el actor institucional idóneo para la ejecución del proyecto, en tanto es una entidad pública especializada en transformación digital, seguridad de la información y ciberseguridad, creada con el propósito de articular, desarrollar y ejecutar proyectos de ciencia, tecnología e innovación orientados al fortalecimiento de las capacidades digitales del Estado colombiano.

La Agencia Nacional Digital cuenta con capacidades técnicas, operativas y metodológicas para la ejecución de proyectos complejos de ciberseguridad en entidades públicas, así como con experiencia en la implementación de controles de seguridad, gestión de vulnerabilidades, pruebas de penetración, fortalecimiento de infraestructuras tecnológicas, gestión de incidentes y transferencia de conocimiento, en concordancia con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Modelo de Seguridad y Privacidad de la Información (MSPI).

Adicionalmente, la AND ha presentado a la Superintendencia de Transporte una propuesta técnica integral para la ejecución de la Fase II del proyecto de ciberseguridad, en la cual se definen de manera detallada el alcance, las fases, la metodología de ejecución, los entregables, el cronograma, los riesgos técnicos y la estructura de costos del proyecto, lo cual evidencia su idoneidad técnica y funcional para atender las necesidades identificadas por la Entidad.

En consecuencia, no resulta procedente realizar un análisis comparativo de proveedores, en la medida en que el objeto del contrato se enmarca en un convenio interadministrativa, orientado a aunar esfuerzos técnicos, administrativos y financieros entre entidades del Estado, aprovechar las capacidades institucionales existentes y garantizar la alineación del proyecto con las políticas nacionales de Gobierno Digital, Confianza y Seguridad Digital.

c. **Análisis del Modelo de Abastecimiento Estratégico MAE- Colombia Compra Eficiente**

Agencia Nacional de Contratación Pública Colombia Compra Eficiente

ANÁLISIS DE LA OFERTA



Fuente: Analítica de datos Colombia Compra Eficiente

El presente análisis se realiza con base en la información disponible en SECOP II y en los reportes consolidados del MAE administrado por Colombia Compra Eficiente, con un enfoque descriptivo del comportamiento de la oferta, sin evaluación de proveedores específicos, es

importante precisar que el código UNSPSC 81 agrupa una multiplicidad de servicios profesionales y empresariales de naturaleza muy diversa, que incluyen, entre otros, servicios jurídicos, financieros, administrativos, de consultoría general, soporte operativo y servicios tecnológicos.

Año	2022			2023			2024			2025		
Clasificador de Bienes y Servicios - Familia	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	P
8110 - Servicios profesionales de ingeniería	13645	$6.194.134.606.310	13,88%	13609	$6.327.774.361.706	14,18%	10953	$4.345.522.214.573	9,74%	11118	$5.714.229.103.068	
8111 - Servicios informáticos	16024	$2.443.396.816.794	5,48%	11759	$3.778.457.650.118	8,47%	11302	$3.977.442.937.765	8,91%	10541	$3.467.718.219.218	
8112 - Economía	397	$30.513.936.335	0,07%	556	$31.596.716.925	0,07%	436	$30.457.248.066	0,07%	243	$26.476.036.896	
8113 - Estadística	552	$121.690.586.662	0,27%	530	$160.559.147.952	0,36%	501	$206.683.347.283	0,46%	351	$176.502.458.577	
8114 - Tecnologías de fabricación	3285	$2.673.858.398.024	5,99%	2806	$627.774.387.474	1,41%	3704	$618.622.835.490	1,39%	2933	$617.512.982.377	
8115 - Servicios de pedología	975	$268.683.729.462	0,60%	1966	$214.963.779.401	0,48%	953	$197.557.232.642	0,44%	956	$394.858.656.959	
8116 - Entrega de servicios de tecnología de información	1338	$800.022.541.432	1,79%	789	$369.814.291.162	0,83%	1047	$490.794.226.737	1,10%	1044	$310.199.859.435	
Total	36216	$12.532.300.615.019	28,09%	32015	$11.510.940.334.738	25,80%	28896	$9.867.080.042.556	22,11%	27186	$10.707.497.316.530	

Fuente: Analítica de datos Colombia Compra Eficiente

d. **Información Financiera posibles proveedores**

Desde una perspectiva sectorial, los servicios objeto del presente análisis, se caracterizan por una estructura financiera basada principalmente en costos de operación y talento humano, los proveedores deben contar, de manera general, con capacidad administrativa y financiera suficiente para gestionar recursos públicos, garantizar la continuidad de las actividades, atender compromisos operativos y soportar procesos de articulación institucional de mediano y largo plazo.

4. ANALISIS DE LA DEMANDA

a. **Adquisiciones Propias de la Entidad**

En el marco del análisis de adquisiciones propias de la Entidad, y de conformidad con la Guía para la Elaboración de Estudios de Sector – GEES, resulta pertinente identificar los procesos contractuales adelantados previamente por la Superintendencia de Transporte que guardan relación directa con el objeto del presente proceso, con el fin de analizar antecedentes, prácticas contractuales y resultados relevantes.

En este contexto, se destacan los convenios interadministrativos suscritos con la Agencia Nacional de Gobierno Digital, mediante uno de ellos, se ejecutó la Fase I del proyecto institucional de ciberseguridad, orientada a la realización del diagnóstico del nivel de madurez en seguridad digital, la identificación de brechas, riesgos y vulnerabilidades, así como la formulación de un plan de mejoramiento para el fortalecimiento de la postura de ciberseguridad de la Entidad.

La información que se presenta a continuación corresponde a dicho antecedente contractual, el cual constituye un insumo técnico fundamental para la estructuración del presente proceso, en tanto permite evidenciar la continuidad técnica, metodológica y funcional del proyecto de ciberseguridad, y soporta la necesidad de avanzar hacia una fase de implementación, en coherencia con los resultados obtenidos en la etapa diagnóstica.

NUMERO DEL PROCESO	OBJETO	ENTIDAD	VALOR	MODALIDAD
653-2025	Aunar esfuerzos técnicos, administrativos y financieros en atención al componente de mejoramiento de la infraestructura tecnológica prevista en el Convenio Marco suscrito entre la Agencia Nacional Digital y la Supertransporte, que permita el fortalecimiento de la función de Inspección, Vigilancia y Control de la Superintendencia en las regiones	CORPORACION AGENCIA NACIONAL DE GOBIERNO DIGITAL	$ 1.050.000.000	Convenio Interadministrativo
654-2025	Aunar esfuerzos técnicos, administrativos y financieros para modernizar y desarrollar una estrategia integral de mejora que permita fortalecer la ciberseguridad en la Superintendencia de Transporte, con el fin de protegerla información institucional, garantizando su accesibilidad, confidencialidad, integridad y disponibilidad.	CORPORACION AGENCIA NACIONAL DE GOBIERNO DIGITAL	$ 397.425.500	Convenio Interadministrativo
630-2025	Aunar esfuerzos técnicos, administrativos, jurídicos y financieros, para adelantar el fortalecimiento de la transformación digital, respondiendo a la estrategia de formulación, planificación, acompañamiento, capacitación en el marzo de la política de Gobierno Digital	CORPORACION AGENCIA NACIONAL DE GOBIERNO DIGITAL	$ -	Convenio Interadministrativo

Fuente: datos abiertos del SECOP II

b. **Adquisiciones Otras Entidades**

En cumplimiento de lo dispuesto en la Guía de Elaboración de Estudios de Sector – GEES, Versión 03 del 19 de agosto de 2025, resulta pertinente identificar y analizar los procesos de contratación adelantados por otras Entidades Estatales que hayan adquirido bienes o servicios iguales o comparables al objeto del presente estudio.

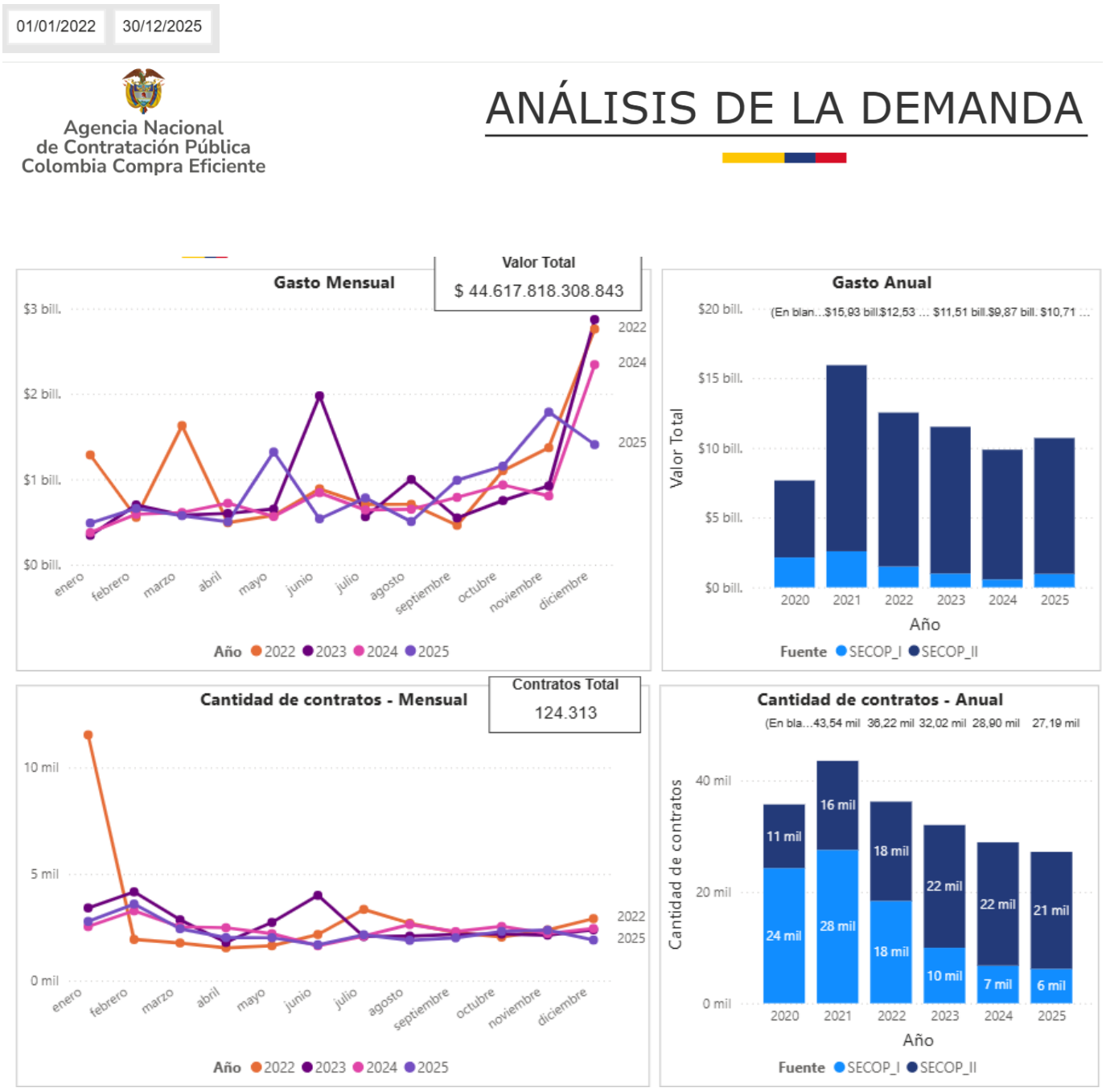
En este sentido, a continuación, se relaciona en la tabla siguiente, la información correspondiente a procesos contractuales adelantados por otras entidades públicas, la cual se incorpora como un referente de análisis, con el propósito de identificar prácticas contractuales, condiciones generales y elementos relevantes que aporten insumos para la estructuración del presente proceso.

NOMBRE DE LA ENTIDAD	OBJETO	VALOR	MODALIDAD	PLAZO	LINK SECOP
SUPERINTENDENCIA DE NOTARIADO Y REGISTRO	Establecer los lineamientos generales mediante los cuales la corporación Agencia Nacional Digital prestará a favor de la Superintendencia de Notariado y Registro los servicios y/o bienes necesarios para la operación tecnológica y demás actividades requeridas para la gestión operativa y misional de la Superintendencia de Notariado y Registro.	$ -	Contratos o convenios Interadministrativos	3 AÑOS	https://community.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.4711060&isFromPublicArea=True&isModal=true&asPopupView=true
FONDO ÚNICO DE TIC	Adelantar un ejercicio de Arquitectura Empresarial que aborde el proceso de direccionamiento estratégico del Ministerio de Tecnologías de la Información y las Comunicaciones acorde a la priorización de la hoja de ruta, cumpliendo con los lineamientos actuales del marco de referencia de	$ 1.713.600.000,00	Contratos o convenios Interadministrativos	5 MESES	ommunity.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.3100479&isFromPublicArea=True&isModal=true&asPopupView=true
UNIDAD DE GESTION PENSIONAL Y PARAFISCALES - UGPP	Aunar esfuerzos para el fortalecimiento de los procesos de la Unidad en materia de tecnologías de la información, seguridad, transformación digital, calidad y comunicación, así como para desarrollar la implementación de las políticas de gobierno de seguridad digital y de la estrategia de gobierno	$ -	Contratos o convenios Interadministrativos	de inicio yel	https://community.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.6347922&isFromPublicArea=True&isModal=true&asPopupView=true
DEPARTAMENTO DE CUNDINAMARCA-SECRETARIA DE TICS	Aunar esfuerzos técnicos, administrativos, jurídicos y financieros, para adelantar el fortalecimiento de la transformación digital, respondiendo a la estrategia de formulación, planificación, acompañamiento, capacitación, desarrollo de sistemas de inteligencia artificial, conectividad, infraestructura tecnológica,	$ -	Contratos o convenios Interadministrativos	2 AÑOS	https://community.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.6220237&isFromPublicArea=True&isModal=true&asPopupView=true
ANI	AUNAR ESFUERZOS TÉCNICOS, ADMINISTRATIVOS, OPERATIVOS, JURÍDICOS, TECNOLÓGICOS Y FINANCIEROS ENTRE LAS PARTES EN EL MARCO DE SUS MISIONALIDADES, PARA LA CONSULTORÍA Y ASESORÍA EN LA IMPLEMENTACIÓN DE SOLUCIONES QUE APOYEN LA GESTIÓN INTEGRAL DE LA	$ 3.239.725.000,00	Contratos o convenios Interadministrativos	12 AÑOS	munity.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.5368491&isFromPublicArea=True&isModal=true&asPopupView=true
FONDO ÚNICO DE TIC	Aunar esfuerzos técnicos, administrativos y financieros para implementar un modelo de Servicios Ciudadanos Digitales que brinde al Estado capacidad y eficiencia para su transformación digital y aumentar las herramientas tecnológicas para la prestación de los servicios de las entidades públicas	$ 7.918.967.781,00	Contratos o convenios Interadministrativos	5 MESES	https://community.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.1373738&isFromPublicArea=True&isModal=true&asPopupView=true
FONDO ÚNICO DE TIC	Aunar esfuerzos técnicos, administrativos y financieros para implementar un modelo de Servicios Ciudadanos Digitales que brinde al Estado capacidad y eficiencia para su transformación digital y aumentar las herramientas tecnológicas para la prestación de los servicios de las entidades públicas.	$ 15.670.708.494,00	Contratos o convenios Interadministrativos	352 DIAS	https://community.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.1652193&isFromPublicArea=True&isModal=true&asPopupView=true
SUPERINTENDENCIA NACIONAL DE SALUD	Contratar los servicios de asesoría especializada para diagnosticar el estado actual de las Políticas de Gobierno y Seguridad Digital en la Supersalud, que permita definir, formular y priorizar estrategias para avanzar en la implementación de dichas políticas, e incentivar su uso y apropiación, dando cumplimiento	$ 2.439.500.000,00	Contratos o convenios Interadministrativos	4 MESES	ommunity.secop.gov.co/Public/TEndering/OpportunityDetail/Index?noticeUID=CO1.NTC.4855609&isFromPublicArea=True&isModal=true&asPopupView=true
FUENTE: MAE- SECOP					

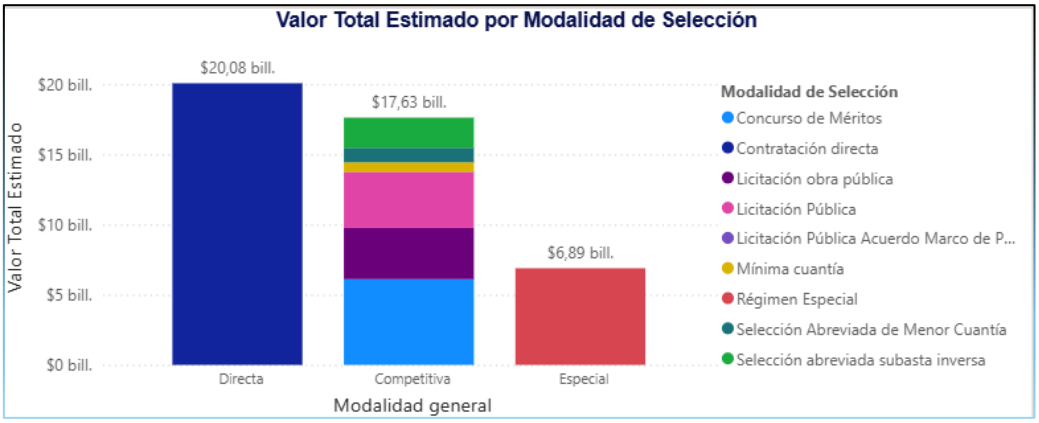
Fuente: datos abiertos del SECOP II

La Agencia Nacional Digital ha suscrito una considerable cantidad de convenios y contratos interadministrativos con entidades del orden nacional y territorial, para coadyuvar en provisión de la solución integral de las necesidades que demanden las entidades. Por tal razón se han llevado a cabo diferentes tipos de contratos y proyectos orientados a cubrir las necesidades de la política digital, desarrollo social y tecnológico, nuevas tecnologías y procesos de transformación digital. Adicionalmente, ha ejecutado interventorías, consultorías, asesorías, educación, mediante la ejecución proyectos con entidades a nivel nacional.

c. **Análisis del Modelo de Abastecimiento Estratégico MAE- Colombia Compra Eficiente**



Fuente: Modelo de abastecimiento Estratégico Colombia Compra Eficiente



Fuente: Modelo de abastecimiento Estratégico Colombia Compra Eficiente

Año	2022			2023			2024			2025	
Clasificador de Bienes y Servicios - Familia	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor
8110 - Servicios profesionales de ingeniería	13645	$6.194.134.606.310	13,88%	13609	$6.327.774.361.706	14,18%	10953	$4.345.522.214.573	9,74%	11118	$5.714.229.103.068
8111 - Servicios informáticos	16024	$2.443.396.816.794	5,48%	11759	$3.778.457.650.118	8,47%	11302	$3.977.442.937.765	8,91%	10541	$3.467.718.219.218
8114 - Tecnologías de fabricación	3285	$2.673.858.398.024	5,99%	2806	$627.774.387.474	1,41%	3704	$618.622.835.490	1,39%	2933	$617.512.982.377
8116 - Entrega de servicios de tecnología de información	1338	$800.022.541.432	1,79%	789	$369.814.291.162	0,83%	1047	$490.794.226.737	1,10%	1044	$310.199.859.435
8115 - Servicios de pedología	975	$268.683.729.462	0,60%	1966	$214.963.779.401	0,48%	953	$197.557.232.642	0,44%	956	$394.858.656.959
8113 - Estadística	552	$121.690.586.662	0,27%	530	$160.559.147.952	0,36%	501	$206.683.347.283	0,46%	351	$176.502.458.577
8112 - Economía	397	$30.513.936.335	0,07%	556	$31.596.716.925	0,07%	436	$30.457.248.066	0,07%	243	$26.476.036.896
Total	**36216**	**$12.532.300.615.019**	**28,09%**	**32015**	**$11.510.940.334.738**	**25,80%**	**28896**	**$9.867.080.042.556**	**22,11%**	**27186**	**$10.707.497.316.530**

Fuente: Modelo de abastecimiento Estratégico Colombia Compra Eficiente

5. ANÁLISIS DEL SECTOR PARA DETERMINAR OTROS CRITERIOS DIFERENCIALES Y APLICACIÓN DE NORMATIVIDAD.

Del análisis del sector correspondiente se establece que por la naturaleza del objeto contractual se condiciona la aplicabilidad de criterios diferenciales en el proceso de contratación.

En este sentido, no resultan aplicables criterios diferenciales asociados a condiciones poblacionales, enfoques de inclusión, promoción de MIPYME, emprendimientos o economía popular, en la medida en que la ejecución del objeto requiere capacidades técnicas, administrativas y tecnológicas especializadas.

Por otra parte, el sector se encuentra regulado por un marco normativo transversal, principalmente en materia transformación digital, el cual orienta y condiciona la estructuración

técnica del objeto contractual, sin imponer requisitos diferenciales adicionales distintos a los previstos en la normativa general de contratación estatal.

6. FUNDAMENTO TEÓRICO Y METODOLOGIA UTILIZADA PARA ANÁLISIS DE PRECIOS.

El análisis de precios para la presente contratación se fundamenta en los principios de eficiencia, economía, planeación y responsabilidad en el uso de los recursos públicos, previstos en la Ley 80 de 1993, así como en los lineamientos establecidos para la contratación directa mediante convenios interadministrativos.

Desde una perspectiva teórica, los servicios especializados en ciberseguridad y seguridad digital corresponden a servicios no estandarizados, intensivos en conocimiento y altamente dependientes del talento humano especializado, cuya valoración económica se determina a partir de la razonabilidad de los costos necesarios para cumplir con el alcance técnico y los resultados esperados.

En este sentido, el análisis económico se sustenta en el enfoque de costo–efectividad, según el cual la inversión en ciberseguridad se concibe como una medida preventiva y estratégica, orientada a mitigar riesgos operativos, financieros, legales y reputacionales asociados a incidentes de seguridad digital, garantizando la continuidad de los servicios misionales y la protección de los activos de información de la Superintendencia de Transporte.

Así mismo, tratándose de un convenio interadministrativo, el análisis económico se orienta a verificar la coherencia y proporcionalidad entre el valor propuesto por la Agencia Nacional Digital, el alcance técnico, la complejidad de las actividades y los beneficios esperados.

La metodología empleada para el análisis de precios se basó en una evaluación de razonabilidad económica, a partir de los siguientes criterios:

Análisis del alcance técnico del proyecto
Se revisó de manera integral la propuesta técnica presentada por la Agencia Nacional de Gobierno Digital, verificando la coherencia entre las actividades planteadas, las fases del proyecto, los entregables, el cronograma y los objetivos definidos para la implementación de la Fase II del proyecto de ciberseguridad.

Identificación de los componentes de costo
Se identificaron los principales componentes que inciden en el valor del proyecto, tales como:

- Talento humano especializado requerido.

- Nivel de complejidad técnica de las actividades (pentesting, análisis de vulnerabilidades, hardening, implementación de controles).
- Dedicación y continuidad operativa del equipo de trabajo.
- Actividades de documentación, reporte y transferencia de conocimiento.
- Gestión técnica y seguimiento del proyecto.

Evaluación de proporcionalidad y coherencia
Se evaluó la proporcionalidad entre el valor económico propuesto y el alcance técnico definido, verificando que los recursos estimados resulten coherentes con la magnitud del proyecto, la criticidad de los activos a proteger y los riesgos identificados en la Fase I.

Análisis de eficiencia del gasto público
Se tuvo en cuenta que la ejecución del proyecto mediante un convenio interadministrativo permite optimizar el uso de los recursos públicos, al reducir costos de transacción, aprovechar capacidades institucionales existentes y evitar la fragmentación de la inversión en soluciones aisladas.

Con base en lo anterior, se concluye que el valor económico propuesto resulta razonable, proporcional y acorde con el alcance técnico, la complejidad de las actividades, los beneficios institucionales esperados y los principios de eficiencia y sostenibilidad del gasto público, sin que se identifiquen elementos que indiquen la existencia de precios artificialmente altos o desalineados frente a los objetivos del proyecto. En este sentido, se contempla un aporte de MIL TRESCIENTOS OCHO MILLONES NOVECIENTOS OCHENTA Y TRES MIL DOSCIENTOS PESOS ($1.308.983.200) por parte de la Superintendencia de Transporte, así como una contrapartida de VEINTIÚN MILLONES CUATROCIENTOS VEINTINUEVE MIL SETENTA Y CINCO PESOS ($21.429.075) por parte de la Agencia Nacional de Gobierno Digital, valores que guardan coherencia con el alcance definido.

7. CONCLUSIONES Y/O RECOMENDACIONES

a. Recomendaciones para requisitos de tipo financiero

De acuerdo con el análisis efectuado el valor del proceso se encuentra previsto en el Plan Anual de Adquisiciones (PAA) de la Superintendencia de Transporte, con un presupuesto de MIL TRESCIENTOS NUEVE MILLONES DE PESOS ($1.309.000.000), el cual guarda correspondencia con el valor de la propuesta presentada por la Agencia Nacional de Gobierno Digital, por valor de MIL TRESCIENTOS OCHO MILLONES NOVECIENTOS OCHENTA Y TRES MIL DOSCIENTOS PESOS ($1.308.983.200), evidenciándose coherencia entre la planeación contractual y la estructuración económica.

80101507 81102702 81111500 81111800 81111808 93151505 93151508 93151512	06 Prestar servicios especializados para la implementación del proyecto de ciberseguridad de la Superintendencia de Transporte, orientada al fortaleci (...)	Enero	Enero	360 Día(s)	Contratación directa	Recursos propios	1.309.000.000 COP

Fuente: plan anual de adquisiciones SECOP II

b. Recomendaciones para requisitos de tipo técnico

En atención a la naturaleza del objeto contractual, orientado a "*Prestar servicios especializados para la implementación del proyecto de ciberseguridad de la Superintendencia de Transporte, orientada al fortalecimiento integral de la gestión de la seguridad digital, mediante la adopción de lineamientos, controles y capacidades institucionales que permitan proteger los activos de información, fortalecer la resiliencia tecnológica de la Entidad y asegurar una adecuada prevención, detección, respuesta y recuperación frente a riesgos y amenazas cibernéticas, en concordancia con los resultados del diagnóstico y plan de mejoramiento definidos por la Entidad",* se requiere la articulación con una entidad pública que cuente con capacidades institucionales, técnicas y administrativas integrales, así como con idoneidad técnica y experiencia demostrable en la ejecución de contratos de ciberseguridad en el sector público. En este sentido, la Agencia Nacional de Gobierno Digital resulta idónea, en la medida en que participó y ejecutó la Fase I del proyecto de Institucional de ciberseguridad, lo que le permitió adquirir un conocimiento directo, específico y detallado del contexto institucional, la arquitectura tecnológica, las brechas identificadas y el plan de mejoramiento definido por la Entidad, garantizando la continuidad técnica, metodológica y operativa necesaria para la adecuada implementación de la Fase II.

En este contexto, La ejecución de la Fase II del proyecto institucional de ciberseguridad genera beneficios estratégicos, técnicos, operativos y financieros para la Superintendencia de Transporte, en la medida en que permite materializar los hallazgos y recomendaciones obtenidos en la Fase I, avanzando de un diagnóstico a una implementación efectiva de capacidades institucionales en seguridad digital.

1. Fortalecimiento integral de la postura de ciberseguridad
La propuesta permite fortalecer de manera progresiva la infraestructura de ciberseguridad de la Entidad, mediante la implementación de controles técnicos, procedimentales y organizacionales alineados con marcos de referencia reconocidos como NIST CSF, ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la Información (MSPI), reduciendo los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información institucional.

2. Gestión proactiva de riesgos y vulnerabilidades

A través de la ejecución de pruebas de penetración, escaneos periódicos de vulnerabilidades, monitoreo de credenciales expuestas en la dark web y auditorías internas, la Entidad fortalece su capacidad para identificar, priorizar y mitigar amenazas cibernéticas antes de que se materialicen, disminuyendo la probabilidad de incidentes que puedan afectar los servicios misionales.

3. Garantía de continuidad operativa de los servicios misionales
La implementación de planes de respuesta a incidentes (IRP), respaldo y recuperación de la información (BC/DR) y la madurez progresiva de un SOC con capacidades de monitoreo y alertas, permiten a la Superintendencia contar con mecanismos efectivos de prevención, detección, respuesta y recuperación, asegurando la continuidad de los procesos de inspección, vigilancia y control a nivel nacional.

4. Fortalecimiento del factor humano y cultura de seguridad digital
La propuesta incorpora componentes específicos de concientización y capacitación, como simulaciones de phishing, charlas técnicas y plataformas educativas con certificación, lo que contribuye a reducir el riesgo asociado al error humano, considerado uno de los principales vectores de ataque en las entidades públicas.

5. Mejora en la toma de decisiones y trazabilidad
La generación de informes técnicos y ejecutivos periódicos, indicadores (KPIs y KRIs), matrices de riesgos y reportes de madurez, proporciona a la Entidad información clara, oportuna y trazable para la toma de decisiones estratégicas en materia de tecnología, seguridad de la información y gestión del riesgo.

6. Continuidad técnica y metodológica del proyecto
Al ser ejecutada por la misma entidad que desarrolló la Fase I, la propuesta garantiza continuidad técnica, coherencia metodológica y aprovechamiento del conocimiento institucional adquirido, evitando reprocesos, duplicidad de diagnósticos y riesgos derivados de la transferencia incompleta de información a terceros.

7. Eficiencia en el uso de los recursos públicos
La ejecución del proyecto mediante un convenio interadministrativo permite optimizar el gasto público, al aprovechar las capacidades especializadas de una entidad pública, reducir costos de transacción y asegurar que los recursos se destinen directamente a la implementación de capacidades de ciberseguridad, sin depender de soluciones aisladas o de corto plazo.

En conjunto, la propuesta permite a la Superintendencia de Transporte avanzar hacia un modelo de gestión de la seguridad digital preventivo, resiliente y sostenible, fortaleciendo la confianza

institucional, la transparencia, la protección de la información estatal y la continuidad de los servicios a la ciudadanía.

CUADRO COMPARATIVO – CONVENIO CON LA AGENCIA NACIONAL DE GOBIERNO DIGITAL (ANGD)

CRITERIO DE ANÁLISIS	**CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL (AND)**	**ALTERNATIVAS (MINISTERIO TIC / UNIVERSIDAD PÚBLICA / ENTIDAD PRIVADA ESPECIALIZADA)**	**VENTAJA COMPARATIVA PARA LA SUPERTRANSPORTE**
Naturaleza jurídica	Entidad pública de carácter nacional, con funciones delegadas del Gobierno Nacional para liderar la Política de Gobierno Digital.	Ministerio TIC: entidad rectora de políticas, no ejecutora directa de proyectos. Universidad: entidad académica con capacidad técnica, pero no con rol normativo. Privada: requiere licitación o proceso contractual.	Al ser entidad pública, la AND permite la suscripción directa de convenios interadministrativos, garantizando legalidad y economía del gasto público.
Competencia técnica	Especializada en interoperabilidad, infraestructura tecnológica, ciberseguridad y servicios digitales del Estado.	Ministerio TIC formula políticas, no ejecuta directamente proyectos. Universidades o privados pueden desarrollar software, pero sin lineamientos oficiales.	La AND garantiza alineación con los estándares nacionales de arquitectura y seguridad digital definidos por el Gobierno.
Alineación con políticas nacionales	Implementa y articula la Política de Gobierno Digital (CONPES 3975 de 2019) y el Decreto 620 de 2020.	Las universidades o privados no son responsables de la aplicación de políticas públicas.	Asegura cumplimiento normativo y coherencia institucional en materia de transformación digital del Estado.
Seguridad y soberanía digital	Maneja infraestructura y protocolos avalados por el Gobierno Nacional; garantiza la confidencialidad, integridad y disponibilidad de la información.	En privados o universidades, el tratamiento de datos debe ser supervisado por la entidad, con mayor riesgo operativo.	La AND ofrece mayor garantía de seguridad digital y continuidad operativa institucional.

Transferencia de conocimiento y sostenibilidad	Aporta asistencia técnica y acompañamiento permanente a las entidades del Estado, fomentando la apropiación tecnológica.	Las universidades pueden capacitar, pero no implementan sistemas de gestión TI del Estado.	La AND permite transferencia directa de capacidades institucionales a la Supertransporte.
Costos y eficiencia administrativa	Optimización de recursos mediante cooperación interinstitucional sin ánimo de lucro.	Las universidades cobran gastos administrativos; los privados buscan margen de utilidad.	Con la AND se asegura eficiencia, economía y transparencia en la inversión pública.
Impacto en la función misional (IVC)	Fortalece la infraestructura tecnológica que soporta las funciones de inspección, vigilancia y control, especialmente en regiones.	Otros aliados podrían apoyar proyectos puntuales, pero sin continuidad ni integración con el ecosistema digital del Estado.	El convenio con la AND potencia la función misional y mejora la trazabilidad y eficiencia del control institucional.
Viabilidad jurídica y contractual	Permite celebrar convenios interadministrativos conforme a la Ley 489 de 1998 (arts. 95 y 96) y el Decreto 092 de 2017.	Con privados o universidades se requeriría proceso contractual o convenio especial sujeto a análisis de selección objetiva.	Facilita la formalización ágil y legalmente sustentada del acuerdo de cooperación.

El convenio con la **Agencia Nacional de Gobierno Digital** representa la opción más idónea y estratégica para la Superintendencia de Transporte, ya que:

- Garantiza el cumplimiento de la Política de Gobierno Digital.
- Optimiza recursos públicos mediante cooperación interinstitucional.
- Asegura la sostenibilidad y seguridad de la infraestructura tecnológica.
- Fortalece la capacidad institucional para el ejercicio efectivo de las funciones de Inspección, Vigilancia y Control en todo el territorio nacional.

En conclusión, la suscripción del convenio Interadministrativo se enmarca en el **ARTÍCULO 95 DE LA LEY 489 DE 1998**, que permite a las entidades públicas celebrar convenios interadministrativos con el fin de aunar esfuerzos, recursos y capacidades para el cumplimiento de sus funciones, e igualmente el **ARTÍCULO 6 de la precitada Ley establece - *Principio de coordinación.*** En virtud del principio de coordinación y colaboración, las autoridades administrativas deben garantizar la armonía en el ejercicio de sus respectivas funciones con el fin de lograr los fines y cometidos estatales

8. FUENTES DE INFORMACIÓN

a. Fuentes de Información Primaria

- La propuesta técnica y económica presentada por la Agencia Nacional de Gobierno Digital.
- Los resultados del diagnóstico y plan de mejoramiento obtenidos en la Fase I del proyecto de ciberseguridad, desarrollada previamente para la Superintendencia de Transporte.
- Los instrumentos de planeación institucional, tales como el Plan Estratégico de Tecnologías de la Información (PETI) y los lineamientos internos en materia de seguridad de la información y gestión del riesgo digital.

b. Fuentes de Información Secundaria

- http://secop.gov.co
- http://www.colombiacompraeficiente.gov.co
- Banco República (informe de política monetaria)
- http://www.dane.com.co
- Formato de anexo técnico del área generadora

9. ANEXOS

a. **Anexo 1:** Cuadro de Tabulación y Análisis de Cotizaciones junto con sus evidencias: Invitaciones a Cotizar y Cotizaciones Obtenidas: N/A

b. **Anexo 2:** Cuadro Comparativo Consumos Entidad Vigencias Anteriores y de Otras Entidades Estatales: N/A

Expedido en la ciudad de Bogotá, a los, veintidos (22) días del mes de enero de 2026.

Rafael Enrique Niebles Fuenmayor
(Nombre y firma)
(jefe / Líder de la dependencia solicitante de la contratación)

Proyección		Revisión	
Firma:		Firma:	DIEGO A. PULIDO A.
Nombre Completo:	Lina Marcela Osorio	Nombre Completo:	Diego Arnulfo Pulido Aguilar
Cargo:	Contratista	Cargo:	Profesional Especializado