FICHA TÉCNICA INTEGRAL PARA DESCRIPCIÓN DE NECESIDADES CONTRACTUALES

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.
ALCANCE:	El presente convenio interadministrativo tendrá como alcance la planeación, ejecución, seguimiento y cierre de las actividades previstas para la implementación de la Fase II del proyecto institucional de ciberseguridad de la Superintendencia de Transporte, de conformidad con la propuesta presentada y con base en los resultados, hallazgos y recomendaciones derivados de la Fase I, bajo un enfoque de mejora continua de la gestión de la seguridad digital. En desarrollo de lo anterior, el alcance del convenio comprende, de manera enunciativa y sin perjuicio de las demás actividades previstas en la propuesta, las siguientes: 1. Realización de diagnósticos periódicos y establecimiento de línea base en ciberseguridad, orientados a identificar el estado actual de la infraestructura tecnológica, los sistemas de información, los servicios digitales y los controles de seguridad existentes, así como las brechas, riesgos y vulnerabilidades emergentes, reconociendo el carácter dinámico de las amenazas cibernéticas. 2. Ejecución de evaluaciones técnicas especializadas, incluyendo pruebas de penetración internas y externas (pentest), análisis de vulnerabilidades y revisiones de seguridad sobre los activos tecnológicos definidos en el alcance técnico del proyecto, con el fin de identificar debilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información institucional. 3. Análisis, priorización y documentación de hallazgos, mediante la elaboración de informes técnicos y ejecutivos que permitan soportar la toma de decisiones, el seguimiento a riesgos identificados y la definición de acciones de mejora en materia de seguridad digital. 4. Implementación y fortalecimiento de controles de ciberseguridad, a partir de los resultados de los diagnósticos y evaluaciones realizadas, incluyendo actividades de ajuste, endurecimiento (hardening),

configuración, adopción de buenas prácticas y recomendaciones técnicas, en coherencia con los lineamientos, políticas y marcos de referencia definidos para el proyecto.

5. Seguimiento y verificación de la aplicación de las medidas implementadas, orientados a evaluar su efectividad y contribución al fortalecimiento de la resiliencia tecnológica institucional, así como a la prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital.
6. Transferencia de conocimiento y fortalecimiento de capacidades institucionales, mediante actividades de capacitación, sensibilización y concientización dirigidas a los servidores y colaboradores de la Superintendencia de Transporte, con el propósito de consolidar una cultura organizacional de seguridad de la información y reducir riesgos asociados al factor humano.
7. Articulación técnica y administrativa entre las partes, garantizando la adecuada coordinación para la ejecución del proyecto, el cumplimiento del cronograma, la trazabilidad de las actividades desarrolladas y la sostenibilidad de las acciones implementadas en el marco de la Fase II.

El alcance del convenio se circunscribe a las actividades previstas en la Fase II del proyecto institucional de ciberseguridad y no implica la delegación de funciones misionales, decisorias o de control propias de la Superintendencia de Transporte, ni sustituye las responsabilidades que corresponden a la Entidad en materia de dirección, administración y gestión de sus sistemas de información y recursos tecnológicos.

CLASIFICADOR DE BIENES Y SERVICIOS:

Código	***Segmento***	***Familia***	***Clase***	***Producto***
80101507	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	Servicios de asesoría de gestión	Servicios de consultoría de negocios y administración corporativa	Servicios de asesoramiento sobre tecnologías de la información
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	servicios de	Administración	Servicios de

		políticos y de asuntos cívicos	administración y financiación pública	pública	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

NOTA 1. No se podrán celebrar contratos con recursos de inversión que tengan por objeto obligaciones propias del funcionamiento de la Entidad.

NOTA 2. Este objeto debe ser igual al Plan Anual de Adquisiciones (PAA) de la respectiva vigencia.

NOTA 3. El objeto contractual se debe clasificar de acuerdo con los códigos UNSPSC, los cuales se encuentran en la página de la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente. Para tal efecto, se recomienda tenerse en cuenta las guías diseñadas por Colombia Compra Eficiente, las cuales pueden ser consultadas a través de la siguiente fuente: https://www.colombiacompra.gov.co/clasificador-de-bienes-y-servicios.

Conforme a lo establecido en el Decreto 1082 de 2015 (artículo 2.2.1.1.1.4.1), los servicios adquiridos por la Superintendencia de Transporte- en adelante SUPERTRANSPORTE, se encuentran enmarcados en las clasificaciones UNSPSC, conforme el Plan Anual de Adquisiciones.

1. COMPETENCIA, DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN Y JUSTIFICACIÓN TÉCNICA

1.1 COMPETENCIA:

Según lo dispuesto en el artículo 2 de la Constitución Política, son fines esenciales del Estado, entre otros, servir a la comunidad, garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución, asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares.
De acuerdo con lo establecido en el numeral 12 del artículo 25 de la Ley 80 de 1993, modificado por el artículo 87 de la Ley 1474 de 2011 y, conforme lo dispuesto en el artículo 2 de la Ley 1150 de 2007, así como, en el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, modificado por el artículo 1 de Decreto 399 de 2021 (Estudios y documentos previos) y el Manual de Contratación de la Superintendencia de Transporte, la Oficina de Tecnología de la Información y las Comunicaciones, procede a efectuar el presente estudio previo con el propósito de suscribir un Convenio Específico Derivado, en función de las necesidades que se buscan satisfacer, de acuerdo con las condiciones que a continuación se detallan.

La Superintendencia de Transporte, es un organismo de naturaleza pública creada por la Ley 1ª de 1991, modificada por la Ley 1753 del 2015, y Ley 1955 de 2019 normas que dotaron a la entidad de personería jurídica y otorgaron un régimen presupuestal y administrativamente autónomo bajo delegación otorgada por el Presidente de la República. conforme lo previsto en el Decreto 2409 de 2018, la Superintendencia de Transporte es un organismo descentralizado del orden nacional, de carácter técnico, con personería jurídica, autonomía administrativa, financiera y presupuestal, adscrita al Ministerio de Transporte que tiene por objeto, ejercer las funciones de vigilancia, inspección, y control que le corresponden al Presidente de la República como suprema autoridad administrativa en materia de tránsito, transporte y su infraestructura de conformidad con la ley y la delegación establecida en el citado decreto.

Por su naturaleza pública, esta Superintendencia está sometida a los principios de la función administrativa y como consecuencia de ello, debe aplicar los postulados de la buena fe, igualdad, moralidad, celeridad, economía, imparcialidad, eficacia, eficiencia, participación, publicidad, responsabilidad y transparencia, cumpliendo a satisfacción la función de vigilancia, inspección y control que se le ha encomendado.

De igual manera, respecto de las funciones de la Superintendencia, estas se encuentran contenidas en el artículo 5 del Decreto 2409 de 2018:

> *"(…) 1. Asesorar al Gobierno Nacional y participar en la formulación de las políticas en los temas de competencia de la superintendencia, en las cuales siempre se debe privilegiar la*

protección de los derechos de los usuarios establecidos en la Constitución y en la normativa vigente.

2. Adoptar las políticas, metodologías y procedimientos para ejercer la supervisión de las entidades sometidas a la vigilancia, inspección y control de la Superintendencia.

3. Vigilar, inspeccionar y controlar el cumplimiento de las disposiciones que regulan la debida prestación del servicio público de transporte, puertos, concesiones e infraestructura, servicios conexos, y la protección de los usuarios del sector transporte, salvo norma especial en la materia.

4. Vigilar, inspeccionar y controlar las condiciones subjetivas de las empresas de servicio público de transporte, puertos, concesiones e infraestructura y servicios conexos.

5. Realizar visitas de inspección, interrogar, tomar declaraciones y, en general, decretar y practicar pruebas, con el fin de verificar el cumplimiento de las disposiciones de la normativa cuyo control es de competencia de la Superintendencia.

6. Solicitar a las autoridades públicas y particulares, el suministro y entrega de documentos públicos, privados, reservados, garantizando la cadena de custodia, y cualquier otra información que se requiera para el correcto ejercicio de sus funciones.

7. Ordenar planes de mejoramiento, mediante acto administrativo de carácter particular, y cuando así se considere necesario, con la finalidad de subsanar las dificultades identificadas a partir del análisis del estado jurídico, contable, económico y/o administrativo interno de todos aquellos quienes presten el servicio de transporte, los puertos, las concesiones o infraestructura, servicios conexos y los demás sujetos previstos en la normativa vigente.

8. Adelantar y decidir las investigaciones administrativas a que haya lugar por las fallas en la debida prestación del servicio público de transporte, puertos, concesiones e infraestructura, servicios conexos, y o en la protección de los usuarios del sector transporte, de acuerdo con la normativa vigente.

9. Imponer las medidas y sanciones que correspondan de acuerdo con la normativa vigente, como consecuencia de la infracción de las normas relacionadas con la debida prestación del servicio público de transporte, puertos, concesiones e infraestructura, servicios conexos, y la protección de los usuarios del sector transporte,

10. Imponer las medidas y sanciones que correspondan por la inobservancia de órdenes e instrucciones impartidas por la Superintendencia o por la obstrucción de su actuación administrativa.

11. Ordenar, mediante acto administrativo de carácter particular y cuando así proceda, los correctivos necesarios para subsanar una situación crítica de los prestadores del servicio de transporte, los puertos, las concesiones o infraestructura, servicios conexos, y los demás sujetos previstos en la ley.

12. Decretar medidas especiales o provisionales en busca de garantizar la debida prestación del servicio público de transporte, así como la correcta operación de los servicios conexos en puertos, concesiones e infraestructura, siempre privilegiando la protección de los derechos de los usuarios en los términos señalados en la normativa vigente.

13. Impartir instrucciones para la debida prestación del servicio público de transporte, puertos, concesiones e infraestructura, servicios conexos, y la protección de los usuarios del sector transporte, así como en las demás áreas propias de sus funciones; fijar criterios que faciliten su cumplimiento y señalar los trámites para su cabal aplicación.

14. Divulgar, promocionar y capacitar a los vigilados y público en general, en las materias de competencia de la Superintendencia.

15. Emitir los conceptos relacionados con la debida prestación del servicio público de transporte, puertos, concesiones e infraestructura, servicios conexos, y la protección de los usuarios del sector transporte.

16. Fijar las tarifas de las contribuciones y cobrar las multas que deban pagar las entidades vigiladas y controladas, de conformidad con la ley.

17. Administrar y llevar las bases de datos y registros asignados a la entidad y que resulten de competencia de la Superintendencia.

18. Todas las demás que se le atribuyan de conformidad con la ley."

A su vez el artículo 6 del citado decreto, establece la estructura de la entidad, en el cual señala en el numeral primero la existencia del Despacho del Superintendente de Transporte, dicho lo anterior se evidencia que el artículo 7 del referido Decreto, señala que son funciones del Despacho del Superintendente, entre otras, las siguientes:

"(…)

2. Adoptar las políticas, metodologías y procedimientos para ejercer la supervisión de las entidades sometidas a la vigilancia, inspección y control de la Superintendencia.

3. Adoptar las políticas, objetivos y estrategias relacionadas con la administración de la Superintendencia.

4. Dirigir y adoptar la acción administrativa de la Superintendencia y el cumplimiento de las funciones que a esta corresponden.
5. Dirigir, supervisar y coordinar el desarrollo de la labor de inspección, vigilancia y control en el cumplimiento de las normas relativas a la debida prestación del servicio público de transporte, puertos, concesiones e infraestructura, servicios conexos, y la protección de los usuarios del sector transporte.

6. Impartir instrucciones en materia de la prestación del servicio de transporte, la protección de sus usuarios, concesiones e infraestructura, servicios conexos; así como en las demás áreas propias de sus funciones; fijar criterios que faciliten su cumplimiento y señalar los procedimientos para su cabal aplicación.

(…)

17. Actuar como representante legal de la Superintendencia de Transporte.

18. Velar por el eficiente desempeño de las funciones de la entidad.

(…)

23. Dirigir la implementación y mantenimiento de las Políticas de Gestión y Desempeño Institucional, y del Modelo Integrado de Planeación y Gestión.

(…)

25. Expedir los actos y celebrar los convenios y contratos que se requieran para el normal funcionamiento de la Superintendencia.

(…)"

Por su parte, el artículo 6 del Decreto 2409 de 2018 en el numeral 1.3 establece que la Oficina de Tecnologías de la Información y las comunicaciones hace parte del Despacho del Superintendente, y es la oficina que actúa como articuladora de la gestión estratégica de tecnologías de la información (TI), ejecutando las políticas, planes, objetivos y metas en gestión de tecnologías que faciliten el cumplimiento de la misión institucional y el apoyo a las demás dependencias de la entidad en la implementación de soluciones que permitan el fortalecimiento de la gestión institucional, encaminando los proyectos de TI al cumplimiento de los lineamientos del Gobierno Nacional y definidos por el MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC). A su vez el artículo 11 del decreto establece como funciones de Oficina de Tecnologías de la Información y las Comunicaciones, entre otras, las siguientes:

"1. Liderar la gestión estratégica de tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado.

2. Liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad y/o sector en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información y las Comunicaciones (TIC) del Estado, la estrategia GEL y según la visión estratégica, las necesidades de transformación y marco legal específicos de su entidad o sector.

3. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia.

(…)

6. Identificar oportunidades para adoptar nuevas tendencias tecnológicas que generen impacto en el desarrollo del sector y del país.

(…)

9. Liderar los procesos de adquisición de bienes y servicios de tecnología, mediante la definición de criterios de optimización y métodos que direccionen la toma de decisiones de inversión en tecnologías de la información buscando el beneficio económico y de los servicios de la entidad.

10. Adelantar acciones que faciliten la coordinación y articulación entre entidades del sector y del Estado en materia de integración e interoperabilidad de información y servicios, creando sinergias y optimizando los recursos para coadyuvar en la prestación de mejores servicios al ciudadano.

11. Generar espacios de articulación con otros actores institucionales, la academia, el sector privado y la sociedad civil para contribuir en aspectos inherentes a la formulación y ejecución de planes, programas y proyectos que incorporen tecnologías y sistemas de la información y las comunicaciones (TIC).

(…)

14. Proponer e implementar acciones para impulsar la estrategia de gobierno abierto mediante la habilitación de mecanismos de interoperabilidad y apertura de datos que faciliten la participación, transparencia y colaboración en el Estado.

(…)".

Ahora bien, de acuerdo con las bases que soportan el Plan Nacional de Desarrollo 2023- 2026: "Colombia, potencia mundial de la vida", materializado a través de la Ley 2294 de 2023, que busca establecer la importancia de las tecnologías de la información y comunicaciones como pilar fundamental para una sociedad del conocimiento y el desarrollo de las regiones de Colombia, es así como se cita literalmente: "Democratización de las TIC para desarrollar una sociedad del conocimiento y la tecnología, conectada con el saber y los circuitos globales"., el sector transporte actúa como catalizador en procura de la garantía de derechos fundamentales y la accesibilidad a bienes y servicios como fundamentos de la dignidad humana y condiciones para el bienestar y la calidad de vida. Asimismo, busca el fortalecimiento del sector transporte como motor de cambio para recuperar la confianza de la ciudadanía y para el fortalecimiento del vínculo Estado – Ciudadanía, teniendo entre otros enfoques que el transporte sea un servicio público accesible a la población, garantizando una infraestructura resiliente con vocación social, procurando por una movilidad segura y sostenible en el territorio colombiano y fortaleciendo las instituciones al servicio de las regiones.

Según lo estipulado en el artículo 113 de la Constitución Política de Colombia, los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus fines.

Así mismo, el artículo 209° constitucional dispone que *"(…) La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. (…)".*

La Ley 80 de 1993 establece que las entidades en ejercicio de la autonomía de la voluntad podrán celebrar los contratos y acuerdos que se requieran para el cumplimiento de los fines estatales.

El artículo 4° de la Ley 489 de 1998 prevé que*: "(…) La función administrativa del Estado busca la satisfacción de las necesidades generales de todos los habitantes, de conformidad con los principios, finalidades y cometidos consagrados en la Constitución Política. Los organismos, entidades y personas encargadas, de manera permanente o transitoria, del ejercicio de funciones administrativas, deben ejercerlas consultando el interés general (…)".*

De igual manera, el artículo 6° de Ley 489 de 1998 establece el principio de coordinación, de la siguiente manera *"(…) las autoridades administrativas deben garantizar la armonía en el ejercicio de sus respectivas funciones con el fin de lograr los fines y cometidos estatales (…)".*

El artículo 95 de la Ley 489 de 1998 faculta a las entidades públicas para asociarse con el fin de cooperar en el cumplimiento de sus funciones administrativas o de prestar conjuntamente servicios que se hallen a su cargo, mediante la celebración de convenios interadministrativos, garantizando el eficiente y eficaz ejercicio de las funciones públicas.

En el mismo sentido, el literal c) numeral 4 del artículo 2° de la Ley 1150 de 2007 dispone que las entidades podrán celebrar directamente contratos o convenios interadministrativos. Como complemento a lo anterior, el Decreto 1082 de 2015 establece en su artículo 2.2.1.2.1.4.4 que: *"(…) Convenios o contratos interadministrativos. La modalidad de selección para la contratación entre Entidades Estatales es la contratación directa; y en consecuencia, le es aplicable lo establecido en el artículo 2.2.1.2.1.4.1 del presente decreto (…)".*

Bajo este marco normativo, la SUPERINTENDENCIA DE TRANSPORTE Y CORPORACION AGENCIA NACIONAL DE GOBIERNO DIGITAL, suscribieron Convenio Marco No. 630 de 2025, con el objeto de *"798_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 marco de la política de Gobierno Digital."*

El referido Convenio Marco de Transformación Digital se constituye en un instrumento estratégico que articula la gestión tecnológica con el cumplimiento del mandato institucional, fortaleciendo las capacidades de supervisión inteligente, la eficiencia administrativa, la transparencia en la gestión y la confianza de la ciudadanía en la labor de la Entidad. Sobre el particular se precisa que como alcance al convenio se establecieron una series de actividades bajo las cuales se cobija la necesidad que se presenta en el siguiente numeral, entre las que se destacan el fortalecimiento del ecosistema digital de información pública y la transformación digital, mediante la realización de actividades, planes y proyectos que respondan a la estrategia, acompañamiento, transferencia de conocimiento, desarrollo e implementación de seguridad de la información.

De otra parte, y con ocasión del convenio marco referido, la SUPERINTENDENCIA DE TRANSPORTE Y CORPORACION AGENCIA NACIONAL DE GOBIERNO DIGITAL, suscribieron Convenio interadministrativo derivado No. 654-2025, con el objeto de *"799_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."*., orientado a evaluar y comprender el estado real de su gestión de seguridad digital, lo cual implicó el desarrollo de la Fase I de desarrollo e implementación de esta estrategia de ciberseguridad para la Entidad.

En este contexto, y con el fin de avanzar en el fortalecimiento institucional previsto en el convenio principal, se hace necesario suscribir un convenio específico derivado para el desarrollo e implementación de la Fase II de seguridad digital en la Superintendencia de Transporte. Este modelo tiene como propósito garantizar la confidencialidad, integridad y disponibilidad de la información de la Entidad, promoviendo la articulación de esfuerzos entre instituciones y el cumplimiento de los objetivos institucionales.

1.2 DESCRIPCIÓN DE LA NECESIDAD

La Superintendencia de Transporte enfrenta una serie de desafíos, incluyendo la necesidad de agilizar los procesos de vigilancia, inspección y control, mejorar la gestión de la información y datos, y adaptarse a las nuevas regulaciones y estándares tecnológicos. Estos desafíos destacan la importancia de emprender iniciativas de transformación digital que permitan a la entidad mantenerse actualizada y responder eficazmente a las demandas generadas en un entorno caracterizado por cambios rápidos y constantes.

En particular, el contexto actual exige fortalecer la infraestructura tecnológica institucional para garantizar la disponibilidad, integridad y confidencialidad de la información, así como la resiliencia de los servicios digitales frente a riesgos cibernéticos. La creciente digitalización de los procedimientos de supervisión, sanción y atención al ciudadano requiere de mecanismos avanzados de protección de datos y continuidad operativa.

En suma a lo anterior, es preciso indicar que en cumplimiento de lo dispuesto en la Ley 2294 del 19 de mayo de 2023, mediante la cual se expidió el Plan Nacional de Desarrollo 2022–2026 “Colombia Potencia Mundial de la Vida”, el Gobierno Nacional establece en su artículo 1 los objetivos orientados a la construcción de un nuevo contrato social, el fortalecimiento de la justicia social y ambiental, y la transformación productiva sustentada en el conocimiento y la tecnología. Dicho Plan reconoce la transformación digital como un eje transversal para alcanzar la equidad, la eficiencia institucional y la consolidación de una gestión pública moderna al servicio del ciudadano.

Dentro de esa estrategia nacional, el fortalecimiento de la ciberseguridad es un pilar esencial para garantizar la confianza digital y la protección de la información estatal. En consecuencia, las entidades públicas deben desarrollar capacidades institucionales en gestión del riesgo tecnológico, protección de infraestructuras críticas y adopción de marcos internacionales de seguridad como ISO 27001, NIST CSF y las Guías de Seguridad Digital del MinTIC.

De manera específica, el artículo 143 de la ley 2294 de 2023, dispone que el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC diseñará e implementará una estrategia integral para democratizar las tecnologías de la información y las comunicaciones (TIC) y desarrollar la sociedad del conocimiento y la tecnología en el país, promoviendo la inclusión digital y la generación de oportunidades en todos los sectores del Estado. En este marco, las entidades públicas deben avanzar en la implementación de herramientas tecnológicas que

fortalezcan sus capacidades institucionales y garanticen el acceso efectivo de la ciudadanía a los servicios públicos a través de medios digitales.

En el caso de la Superintendencia de Transporte, este mandato se traduce en la necesidad de contar con sistemas robustos, resilientes y auditables que soporten de manera segura la operación de los servicios misionales, el intercambio de información con otras entidades del sector transporte y el funcionamiento de los sistemas críticos que gestionan datos sensibles.

En concordancia con este mandato, la Oficina de Tecnologías de la Información y las Comunicaciones de la Superintendencia de Transporte, en desarrollo de los proyectos definidos en el Plan Estratégico de Tecnologías de la Información (PETI), el cual fue aprobado mediante sesión del Comité Institucional de Gestión y Desempeño del 17 de septiembre de 2024, ha incorporado iniciativas orientadas a la adopción de nuevas tecnologías y a la implementación de los lineamientos establecidos por el MinTIC en materia de Gobierno Digital. Estas acciones buscan consolidar un conjunto de soluciones tecnológicas y procedimientos que fortalezcan la capacidad institucional para su transformación digital, garantizando la interacción eficiente, transparente y segura con los ciudadanos, en cumplimiento del derecho al acceso a la administración pública a través de medios electrónicos ante la administración pública.

Entre los ejes del PETI se prioriza la gestión integral de la ciberseguridad, mediante la actualización de controles perimetrales, la segmentación de redes, la gestión de identidades, la protección de entornos en la nube y la implementación de mecanismos de monitoreo, respuesta y remediación frente a incidentes de seguridad. Dichas acciones se articulan con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano.

En coherencia con el Plan Estratégico de Tecnologías de la Información (PETI) 2023-2026 de la Superintendencia de Transporte, la Entidad prioriza el fortalecimiento de la seguridad y privacidad de la información como componente esencial de su arquitectura tecnológica. Dicho plan establece, dentro del dominio de “Administración de la Seguridad y Privacidad de la Información”, acciones orientadas al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), la actualización de las políticas de seguridad, el desarrollo de una cultura institucional de seguridad digital, la ejecución de pruebas de vulnerabilidad, la gestión de incidentes y la configuración de los equipos de seguridad informática.

Estas líneas de acción, recogidas en el numeral 4.7 del PETI, se desarrollan conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Política de Gobierno Digital, la Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020) y las buenas prácticas de ciberseguridad del Estado colombiano. Por tanto, el presente convenio específico derivado con la Agencia Nacional Digital materializa los objetivos definidos en el PETI, orientados a fortalecer el Sistema de Gestión de Seguridad de la Información, garantizar la confidencialidad, integridad y disponibilidad de los datos institucionales y asegurar la continuidad operativa de los servicios tecnológicos misionales de la Entidad.

La Superintendencia de Transporte, atendiendo a diversos informes recibidos por parte de autoridades competentes, ha identificado la necesidad de fortalecer su seguridad informática, sustentando en:

- Recuperar la gobernanza y soberanía digital de los recursos tecnológicos y sistemas de información.
- Capacitar adecuadamente a los responsables de la seguridad de la información con el fin de determinar su pertinencia y/o identificar si cuenta con las competencias técnicas requeridas para salvaguardar la integridad de la información.
- Identificar si la Entidad cuenta con las protecciones perimetrales y optimizadores de recursos de red como lo pueden ser Balanceadores, WAF, CON, IPS, IDS, Firewalls, etc., teniendo cuenta que son una tecnología ampliamente necesaria para mitigar los riesgos.
- Atender con buenas prácticas y metodologías de desarrollo seguro y a su vez sostener en el tiempo la evaluación periódica de vulnerabilidades para su debida remediación y de esta manera obtener una protección integral.
- Identificar la necesidad de evaluar la posibilidad de alcanzar los servicios de tipo backend, desarrollo, pruebas, gestión, intranet, mesas de ayuda y soporte etc., a través de conexiones seguras por VPN web o portales que una vez se surta el proceso de multifactor de autenticación le provea los servicios necesarios. Así mismo, es importante contemplar el uso de captcha, dobles factores de autenticación y validación de datos en formulario
- Desarrollo de actividades de análisis de vulnerabilidades y penetración con el fin de identificar posibles brechas de seguridad que deban ser subsanadas y de esta manera fortalecer la postura de seguridad.
- Validar en lo que corresponda, las actividades requeridas para minimizar la cantidad de servicios y sistemas de información expuestos en internet; buscando dejar estrictamente los necesarios para la operación de la Entidad y servicios de la ciudadanía.
- Identificar si se cuenta o requieren la efectividad de los procesos de copias de seguridad, plan de continuidad de la operación de la Entidad y plan de recuperación de servicios y sistemas de información.
- Identificar los vectores o la interrelación entre los diferentes proveedores de servicios de telecomunicaciones, aplicaciones y servicios tercerizados con el fin de detectar efectos colaterales que pueda llegar a resultar de un ataque de cadena de suministro.
- Diseñar estrategias que protejan temporalmente servicios legacy o en obsolescencia en caso de ser necesario.
- Es importante considerar el fortalecimiento en la cultura de la seguridad de la información y evaluar el comportamiento que pueden llegar a tener los servidores públicos y/o contratistas frente las amenazas cibernéticas. Por ejemplo, a través de la simulación de ataques de Spear Phishing (Suplantación dirigida).

Estas líneas de acción constituyen la base técnica para la implementación de una estrategia de ciberseguridad institucional que cubra todos los niveles de la arquitectura tecnológica —

infraestructura, aplicaciones, servicios en la nube y usuarios finales—. El enfoque integral propuesto busca pasar de un modelo reactivo a un modelo preventivo y resiliente, que combine la gestión de riesgos, la respuesta a incidentes y la concienciación de los funcionarios.

Con base en lo anterior, y en atención al convenio marco suscrito se ha precisado que la Entidad ha identificado la necesidad de fortalecer la seguridad de la información que posee, dado que la Superintendencia de Transporte, en cumplimiento de su función misional de inspección, vigilancia y control del sector transporte, administra sistemas de información que procesan datos sensibles, documentos electrónicos oficiales, expedientes sancionatorios y registros de entidades vigiladas.

La complejidad y criticidad de estos sistemas demandan la adopción de medidas técnicas avanzadas y el acompañamiento de una entidad estatal experta en tecnología, capaz de ejecutar proyectos de fortalecimiento digital de alta complejidad, garantizando cumplimiento normativo y eficiencia en la inversión pública.

Esta infraestructura tecnológica constituye un activo estratégico institucional, cuya disponibilidad, integridad y confidencialidad son esenciales para garantizar la transparencia, la eficiencia administrativa y la confianza digital ante la ciudadanía.

La Superintendencia de Transporte, en el marco de sus funciones misionales y de su responsabilidad institucional en la protección de los activos de información, adelantó previamente un proceso estructurado orientado a evaluar y comprender el estado real de su gestión de seguridad digital. Dicho proceso se materializó en la Fase I del proyecto de ciberseguridad, la cual fue desarrollada a partir de un estudio previo que permitió identificar el nivel de madurez institucional, las brechas existentes, los riesgos relevantes asociados a la infraestructura tecnológica y a la información administrada por la Entidad, así como la necesidad de adoptar medidas técnicas, organizacionales y procedimentales para fortalecer su postura de ciberseguridad.

Como resultado de esa Fase I, la Entidad no solo obtuvo un diagnóstico técnico, sino un conjunto de conclusiones y un plan de mejoramiento, en los que se evidenció que la gestión de la seguridad digital no podía agotarse en ejercicios de evaluación, caracterización o análisis, sino que requería avanzar hacia una fase de implementación progresiva y controlada, orientada a convertir los hallazgos y recomendaciones en capacidades institucionales efectivas.

En ese sentido, la Fase II del proyecto de ciberseguridad surge como una consecuencia directa y necesaria de los resultados obtenidos en la Fase I. No se trata de una iniciativa autónoma ni desconectada, sino de una etapa posterior que tiene como finalidad materializar, consolidar y poner en operación los lineamientos, controles, procedimientos y capacidades identificadas como prioritarias. La ausencia de esta fase de implementación 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.

Adicionalmente, la necesidad de ejecutar esta Fase II se encuentra alineada con los instrumentos de planeación institucional de la Superintendencia de Transporte, en particular con el Plan Estratégico de Tecnologías de la Información – PETI 2023–2026, el cual contempla el fortalecimiento de la seguridad de la información y de la seguridad digital como componentes esenciales para la sostenibilidad de los servicios tecnológicos, la protección de la información y la continuidad de la operación institucional. En este marco, la implementación de políticas, planes, mecanismos de verificación técnica, actividades de fortalecimiento de capacidades y acciones de gestión del riesgo constituye un habilitador indispensable para el cumplimiento de los objetivos estratégicos definidos por la Entidad.

La necesidad que se pretende satisfacer mediante el presente convenio interadministrativo no corresponde, entonces, a la contratación de servicios aislados o a la ejecución de actividades rutinarias, sino a la continuación lógica y técnicamente justificada de un proceso previamente iniciado, orientado a fortalecer de manera integral la gestión de la seguridad digital de la Superintendencia de Transporte. Esta continuidad exige coherencia metodológica, articulación con los resultados ya obtenidos y una ejecución que permita garantizar que el conocimiento generado, los controles definidos y las capacidades desarrolladas sean efectivamente incorporados a la gestión institucional.

En consecuencia, se configura una necesidad clara, objetiva y actual de aunar esfuerzos con una entidad pública especializada, que permita llevar a cabo la Fase II del proyecto de ciberseguridad, asegurando la implementación de las medidas identificadas, la reducción progresiva de los riesgos, la apropiación institucional de los resultados y la sostenibilidad de la gestión de la seguridad digital en el mediano y largo plazo.

La materialización de un convenio específico derivado con la Agencia Nacional Digital permitirá canalizar recursos para la ejecución de proyectos de ciberseguridad y seguridad de la información, bajo un esquema de cooperación técnica, garantizando la trazabilidad en el uso de los recursos y la implementación de soluciones ajustadas a las normas nacionales e internacionales aplicables.

El propósito final de esta contratación es fortalecer la postura de seguridad digital de la Superintendencia de Transporte, garantizando la protección de la información institucional, la continuidad de los servicios misionales y la resiliencia tecnológica frente a amenazas cibernéticas.

La Superintendencia de Transporte identifica la necesidad imperativa de abordar los desafíos emergentes y las demandas crecientes del entorno mediante la adopción de estrategias de transformación digital. La complejidad inherente a la vigilancia, inspección y control del sector del transporte requiere una modernización efectiva de los sistemas y procesos y herramientas tecnológicas existentes para mejorar la eficiencia operativa, la transparencia y la capacidad de respuesta institucional.

En este sentido la colaboración de un aliado estratégico se erige como un como un catalizador significativo, aprovechando su experiencia y capacidades en investigación y desarrollo tecnológico para impulsar la implementación exitosa del Sistema de Supervisión Inteligente. Este proyecto, enmarcado en las políticas gubernamentales de ciencia, tecnología e innovación, representa un compromiso decidido con la excelencia y la vanguardia en el ámbito de la gobernanza digital, alineado con los objetivos estratégicos de la Superintendencia y contribuyendo a cumplir con los procesos misionales de la entidad como un actor clave en el panorama nacional.

Desde el punto de vista jurídico, la suscripción de un convenio interadministrativo con la Agencia Nacional de Gobierno Digital (AND) encuentra pleno respaldo en el literal c) numeral 4 del artículo 2 de la Ley 1150 de 2007, que autoriza la contratación directa entre entidades estatales cuando el objeto del acuerdo sea el cumplimiento de funciones públicas o la cooperación tecnológica. De igual modo, el artículo 2.2.1.2.1.4.4 del Decreto 1082 de 2015 confirma que esta modalidad se ajusta a los principios de planeación, transparencia y economía previstos en la Ley 80 de 1993 (arts. 23, 24 y 25).

Financieramente, la suscripción del convenio resulta más eficiente que una contratación directa con terceros privados, pues:

1. Permite aprovechar las capacidades instaladas y conocimiento especializado de la AND, evitando gastos de estructuración, licencias y consultorías externas.
2. Elimina los costos de transacción y los riesgos derivados de la contratación de proveedores privados, optimizando el uso de los recursos públicos conforme a los artículos 25 y 26 de la Ley 80 de 1993.
3. Facilita la cofinanciación o gestión conjunta de recursos de cooperación técnica o de innovación pública, de acuerdo con lo previsto en los artículos 94 y 95 de la Ley 489 de 1998, que promueven la colaboración interinstitucional para el fortalecimiento de capacidades estatales.
4. Garantiza la sostenibilidad tecnológica, dado que la AND cuenta con infraestructura propia y modelos escalables de desarrollo digital que reducen los costos de mantenimiento y actualización en el mediano plazo.

Por tanto, el convenio no solo resulta jurídicamente viable y técnicamente pertinente, sino que además es financieramente racional, al potenciar la eficiencia del gasto público, la interoperabilidad de los sistemas institucionales y la capacidad de respuesta de la Superintendencia ante los retos tecnológicos del sector transporte.

Dicho lo anterior y en aras de aunar esfuerzos en el marco del principio constitucional de colaboración existente entre las entidades estatales, se evidencia que desde el 29 de diciembre de 2017 mediante Documento Privado de Constitución de Corporación sin Ánimo de Lucro, el Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública, constituyeron la Corporación Agencia Nacional de Gobierno

Digital - AND, la cual tiene como objeto articular los Servicios Ciudadanos Digitales de que trata el título 17 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, acorde con la evolución de los modelos de servicios digitales ciudadanos y del sistema de planeación y gestión pública, y desarrollar las actividades de ciencia, tecnología e innovación asociadas a la creación de un ecosistema de información pública, incorporando la debida gestión de riesgos asociada a la información, que permita apoyar proyectos de ciencia, tecnología e innovación, así como identificar planes programas y proyectos que ofrezcan soluciones a problemáticas o cuellos de botella en el sector público colombiano, introduciendo con ello mejoras significativas en los procesos estatales, mediante el uso y desarrollo de soluciones de software, analítica de datos, entre otras.

Los estatutos de la Corporación Agencia Nacional de Gobierno Digital - AND establece que el objeto de la corporación es:

> *(…) a. Facilitar a los ciudadanos el acceso a la administración pública a través de medios electrónicos, por virtud de lo dispuesto en el Decreto 1078 de 2015, diseñando y ejecutando el Modelo de Servicios ciudadanos digitales básicos y especiales.*
>
> *c) Formular, apoyar, proponer y ejecutar proyectos de ciencia, tecnología e innovación que incorporen tecnologías emergentes para generar capacidades de analítica de datos.*
>
> *e) Mejorar la calidad de los servicios ofrecidos por las diversas entidades públicas a través de la tecnología y velar por la optimización de trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos, siguiendo los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública. (…)*

Desde su creación, la Corporación Agencia Nacional de Gobierno Digital - AND se ha consolidado como un organismo referente en el desarrollo de infraestructura tecnológica, especialmente en el ámbito del sector público, promoviendo la investigación científica y el desarrollo tecnológico. Así mismo, impulsa la creación de nuevos productos, procesos y servicios basados en las Tecnologías de la Información y las Comunicaciones (TIC), participando activamente en proyectos de innovación que incorporan tecnología destinada a mejorar la calidad de los servicios públicos ofrecidos por diversas entidades gubernamentales. Además, la Corporación Agencia Nacional de Gobierno Digital - AND actúa como un puente entre la tecnología nacional e internacional, facilitando el acceso a nuevas soluciones tecnológicas que optimicen los procesos y servicios públicos. La entidad también proporciona consultorías especializadas de alta calidad para identificar las necesidades específicas de las entidades públicas, y articula proyectos de TIC utilizando metodologías de diseño basadas en prácticas ágiles. Estas metodologías permiten que la ejecución de proyectos en el sector público se realice con mayor celeridad y eficiencia, garantizando resultados rápidos y efectivos en beneficio de la ciudadanía.

Las actividades de la Corporación Agencia Nacional de Gobierno Digital - AND se enmarcan en la promoción y desarrollo de transformación digital del estado como mecanismo para potenciar el valor social y económico del país, a través del uso de las tecnologías digitales en el sector público y sector privado, para impulsar la productividad y favorecer el bienestar de la ciudadanía. Esto en el marco de la política digital del Estado, especialmente el CONPES 3975 del 2019 y el CONPES 4144 del 2025, de manera que, se hace necesario, bajo el principio de coordinación, articular esfuerzos con las entidades estatales para la implementación de tecnologías TIC que permitan la transformación digital.

De acuerdo con todo lo anterior, se hace necesario suscribir el presente convenio como manifestación de las actividades y compromisos adquiridos por las partes de acuerdo con el Convenio Marco suscrito, buscando que la Superintendencia de Transporte fortalezca su seguridad informática.

La contratación de un servicio especializado en ciberseguridad permitirá a la Superintendencia de Transporte fortalecer su postura de seguridad digital, cumplir con los lineamientos normativos vigentes y proteger la información institucional frente a los riesgos cibernéticos. Con ello, la entidad avanza hacia una gestión tecnológica más segura, transparente y resiliente, alineada con la Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020) y la Resolución 500 de 2021 del MinTIC.

2. ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO A CONTRATAR

La necesidad a 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.

- **ACTIVIDADES A DESARROLLAR**

Mes	Actividad	Descripción
1	Plan de trabajo	Documento en el cual se describe de manera detallada el trabajo a desarrollar dentro de la Superintendencia de Transporte, incluyendo las actividades planificadas, los alcances definidos y el análisis del estado actual de la ciberseguridad de la entidad.
	Cronograma	Documento en el cual se establecen las actividades a desarrollar dentro de la Superintendencia de Transporte, definiendo los tiempos de ejecución, la secuencia de las tareas y los hitos del proyecto.
	Evaluación de madurez en ciberseguridad	Diagnóstico estructural según NIST/ISO
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Identificación de activos críticos	Clasificación de sistemas y datos
	Definición de KPIs y KRIs	Desarrollo tablero indicadores
2	Evaluación de riesgos (Risk Assessment)	Evaluación amenazas y riesgos
	Desarrollo e Implementación Plataforma Educativa periódica y certificación de cumplimiento en conocimientos de phishing al personal de la superintendencia	Plataforma de concientización en ciberseguridad que automatiza la capacitación, evalúa el aprendizaje y emite certificados de cumplimiento auditorables para cada funcionario
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.

	Desarrollo y Suscripción de Contenidos y Mantenimiento a la plataforma educativa.	Carga inicial de 3 cursos, integración LDAP y soporte técnico plataforma x 10 meses.
	Roadmap de seguridad	Plan estratégico 24 meses
3	Políticas de ciberseguridad (borradores)	Desarrollo políticas institucionales
	Monitoreo mensual de credenciales expuestas en Dark Web + Sistema de Alertas.	Servicio mensual para identificar y validar credenciales potencialmente expuestas asociadas a la organización mediante herramientas especializadas de Threat Intelligence y monitoreo de fuentes abiertas, filtraciones conocidas y repositorios criminales.
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Escaneo mensual de vulnerabilidades en activos tecnológicos. Volumen de Activos: más de 50 IPs/Activos.	Servicio mensual de gestión de vulnerabilidades mediante la ejecución de escaneos controlados con Nessus, orientados a identificar vulnerabilidades conocidas, configuraciones inseguras, servicios expuestos y debilidades técnicas en los activos tecnológicos de la organización (servidores, aplicaciones, equipos de red y servicios publicados).
	Charla ciberseguridad – Hacking #1	Sensibilización técnica
4	Implementación SOC/EDR básico	Configuración SOC/EDR 50 dispositivos
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Hardening endpoints/servidores	Refuerzo de controles técnicos
5	Implementación IAM	Sistema de gestión de accesos
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Segmentación de red básica	Separación lógicas y controles

6	Plan de Respuesta a Incidentes (IRP)	Desarrollo plan de reacción
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Respaldo y recuperación de datos	Estrategia de backups y restauración
7	Simulacro de incidente	Prueba de IRP con escenarios
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Gestión de vulnerabilidades continua	Escaneo y priorización
8	SOC avanzado & alertas 24/7	Madurez de SOC con casos de uso
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Zero Trust (fase inicial)	Reforzamiento Zero Trust
9	Evaluación de riesgo proveedores	Evaluación ciber riesgo terceros
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
10	Charla ciberseguridad – Hacking #2	Formación avanzada
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Simulación phishing y cultura	Simulaciones internas
11	Auditoría interna de ciberseguridad	Revisión de todo lo realizado

	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Re-test controles críticos	Validación técnica post auditoría
12	Transferencia de Conocimiento y Cierre Ejecutivo CISO Etapa II	Documentación de resultados
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Actividad orientada a verificar y monitorear el cumplimiento de los lineamientos, controles, políticas y requerimientos de ciberseguridad definidos en el proyecto, asegurando su correcta ejecución conforme a normas, buenas prácticas y cronograma establecido.
	Medición de madurez final y roadmap futuro	Comparativo estado inicial/final

- **ENTREGABLES**

Mes	Actividad	Entregable
1	Plan de trabajo	Informe de plan de trabajo
	Cronograma	Cronograma
	Evaluación de madurez en ciberseguridad	Informe de madurez
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Identificación de activos críticos	Catálogo activos
	Definición de KPIs y KRIs	Matriz KPIs/KRIs
2	Evaluación de riesgos (Risk Assessment)	Matriz de riesgos
	Desarrollo e Implementación Plataforma Educativa periódica y certificación de cumplimiento en conocimientos de phishing al personal de la superintendencia	Aplicativo funcional
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Desarrollo y Suscripción de Contenidos y Mantenimiento a la plataforma educativa.	Contenido inicial
	Roadmap de seguridad	Documento roadmap
	Políticas de ciberseguridad (borradores)	Manual de políticas

3	Monitoreo mensual de credenciales expuestas en Dark Web + Sistema de Alertas.	Informe mensual técnico y ejecutivo
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Escaneo mensual de vulnerabilidades en activos tecnológicos. Volumen de Activos: más de 50 IPs/Activos.	Informe mensual técnico y ejecutivo
	Charla ciberseguridad – Hacking #1	Sesión y material
4	Implementación SOC/EDR básico	SOC operativo
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Hardening endpoints/servidores	Reporte hardening
5	Implementación IAM	IAM configurado
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Segmentación de red básica	Topología segura
6	Plan de Respuesta a Incidentes (IRP)	Manual IRP
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Respaldo y recuperación de datos	Plan BC/DR
7	Simulacro de incidente	Informe de simulacro
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Gestión de vulnerabilidades continua	Reporte de vulnerabilidades
8	SOC avanzado & alertas 24/7	Reportes SOC
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Zero Trust (fase inicial)	Documento Zero Trust
9	Evaluación de riesgo proveedores	Reporte terceros
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
10	Charla ciberseguridad – Hacking #2	Sesión y grabación
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Simulación phishing y cultura	Reporte phishing

11	Auditoría interna de ciberseguridad	Informe auditoría
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Re-test controles críticos	Reporte re-test
12	Transferencia de Conocimiento y Cierre Ejecutivo CISO Etapa II	Informe final
	Seguimiento y Control de Cumplimiento en Ciberseguridad	Informe de seguimiento
	Medición de madurez final y roadmap futuro	Roadmap 2027

3. INFORMACIÓN PRESUPUESTAL

La dependencia debe establecer cuál es la fuente de recurso, indicando si es de funcionamiento o inversión (en este último caso debe incluir el Código BPIN, el nombre del proyecto y el nombre del producto), haciendo además mención del Número PAA y CDP (Adjuntar este último, de existir)

4. PLAZO

El plazo de ejecución del contrato será hasta el día treinta y uno (31) de diciembre de 2026, contado a partir de la suscripción del acta de inicio, la cual no podrá ser anterior al cumplimiento de los requisitos de ejecución y perfeccionamiento del contrato.

5. FORMA DE PAGO

La superintendencia realizara desembolsos conforme a porcentajes de avance en las actividades contempladas.

6. LUGAR DE EJECUCIÓN

El negocio jurídico por medio del cual se pretende satisfacer la necesidad identificada se ejecutará en la ciudad de Bogotá D.C.

7. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

1. Elaborar y ejecutar el plan de trabajo y de implementación de la Fase II, en estricta coherencia con la propuesta técnica presentada, el cronograma aprobado, las fases definidas y los resultados, hallazgos y recomendaciones derivados de la Fase I del proyecto institucional de ciberseguridad.
2. Entregar los productos y entregables previstos en el cronograma y en la propuesta, dentro de los plazos establecidos y cumpliendo los criterios de calidad, trazabilidad y

aceptabilidad definidos, incluyendo informes técnicos, informes ejecutivos, documentos de línea base, evaluaciones, reportes y entregables de cierre.

3. Desarrollar las actividades de transferencia de conocimiento, capacitación y sensibilización, conforme a lo previsto en el plan de trabajo y en la propuesta técnica, incluyendo la entrega de materiales, soportes, evidencias de asistencia y resultados de las actividades realizadas.
4. Ejecutar las actividades técnicas previstas para la Fase II, tales como diagnósticos periódicos, evaluaciones de madurez, pruebas de penetración internas y externas, escaneos de vulnerabilidades, fortalecimiento de controles, hardening, monitoreo y demás acciones definidas en la propuesta, de conformidad con los estándares, marcos de referencia y buenas prácticas allí establecidos.
5. Presentar informes de avance, seguimiento y control, así como reportes técnicos y ejecutivos periódicos y finales, que permitan a la Superintendencia de Transporte conocer el estado del proyecto, los riesgos identificados, los hallazgos relevantes, las acciones de mejora y los próximos pasos.
6. Garantizar que la ejecución del convenio se realice con personal idóneo y calificado, aplicando prácticas de seguridad de la información y ciberseguridad, y adoptando las medidas necesarias para evitar la exposición, uso indebido o filtración de información sensible.
7. Custodiar y proteger la información a la que tenga acceso, aplicando controles de confidencialidad, integridad y uso limitado, y asegurando que dicha información sea utilizada exclusivamente para el cumplimiento del objeto y alcance del convenio.
8. Entregar a la Superintendencia de Transporte los documentos, procedimientos, políticas, matrices, reportes, materiales y demás entregables definidos, en los formatos establecidos, incluyendo versiones editables y reutilizables, que permitan la sostenibilidad y apropiación institucional de los resultados de la Fase II.

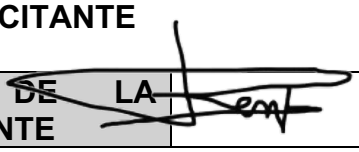
8. ANÁLISIS DE RIESGOS Y FORMAS DE MITIGARLOS

La superintendencia a través de documento anexo elaborado por el Grupo Interno de Gestión contractual, realizó la elaboración de la matriz de riesgos.

9. SUPERVISIÓN

De acuerdo con la carga operativa e idoneidad técnica, se sugiere al ordenador del gasto que el funcionario Daniela Peñaloza Mejía – Asesora código 1020, grado 11, asignada al despacho del Superintendente se designe como Supervisor del futuro contrato.

10. DEPENDENCIA SOLICITANTE

FIRMA DEL JEFE DE LA DEPENDENCIA SOLICITANTE	

NOMBRE COMPLETO DEL JEFE DE LA DEPENDENCIA SOLICITANTE	Rafael Enrique Niebles Fuenmayor
CARGO Y DEPENDENCIA	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (E)
NOMBRE COMPELTO ENLACE RESPONSABLE DE LA ADQUISICIÓN, DEL ÁREA TÉCNICA – ENLACE CONTRACTUAL	Nicolás Andrés Guzmán Padilla

Proyectó: Nicolás Andrés Guzmán Padilla – Contratista Dirección Administrativa