PROPUESTA TÉCNICA

Fase II del proyecto institucional de ciberseguridad

AGENCIA NACIONAL DIGITAL - AND

DIRIGIDO A: SUPERINTENDENCIA DE TRANSPORTE

BOGOTÁ D.C., ENERO DE 2026

CONTENIDO

Control de aprobaciones 3
1. NOMBRE DEL PROYECTO 4
2. PARTICIPANTES 4
3. INTERLOCUCIÓN PARA LA FORMULACIÓN DEL PROYECTO 4
4. CONFIDENCIALIDAD 4
5. OBJETIVOS 5
5.1 Objetivo general 5
5.2 Objetivos Específicos 5
6. JUSTIFICACIÓN 6
6.1 Fundamentación Constitucional y Legal 6
6.2 Vulnerabilidad de la Infraestructura de Información 6
6.3 Necesidad de una Cultura de Seguridad Digital 6
6.4 Alineación con Políticas de Gobierno Digital 6
6.5 Continuidad Operativa y Gestión de Crisis 7
6.6 Eficiencia en la Contratación Pública 7
7. ALCANCE 8
8. FASES 9
9. METODOLOGÍA DE EJECUCIÓN 12
Metodología de Gestión de Proyectos 12
Metodología de Seguridad 13
13. FORMA DE PAGO 19
14. RIESGOS TECNICOS 21
15. Condiciones para el Desarrollo del Proyecto 24
16. Cierre del Proyecto 24

Control de aprobaciones

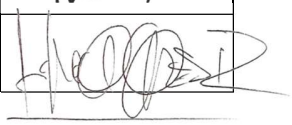
Aprobación	Responsable	Subdirección	Fecha	Firma
Comercial	Victor Botero	Soluciones y Servicios	29/01/2026	
Técnica	Julio Echavarría	Desarrollo y SCD	29/01/2026	
Financiera	Johanna Acero	Financiera y Administrativa	29/01/2026	
Jurídica	Paula Ricaurte	Jurídica	29/01/2026	
Dirección	Adriana Garcés	N/A	29/01/2026	

Tabla 1 Control de aprobaciones

1. NOMBRE DEL PROYECTO

Fase II del proyecto institucional de ciberseguridad

2. PARTICIPANTES

- **Área responsable del Proyecto en la Entidad:** Superintendencia de Transporte.
- **Área responsable del Proyecto Agencia Nacional Digital:** Subdirección de Soluciones y Servicios.

3. INTERLOCUCIÓN PARA LA FORMULACIÓN DEL PROYECTO

- Superintendencia de Transporte
- Subdirección de Soluciones y Servicios

4. CONFIDENCIALIDAD

Toda la información proporcionada en esta propuesta se considera información confidencial de la Corporación Agencia Nacional de Gobierno Digital en adelante AND y está dirigida exclusivamente a la Superintendencia de Transporte– Oficina de Tecnologías de la Información y las Comunicaciones.

La Superintendencia de Transporte podrá revelar la información confidencial contenida en la propuesta a los trabajadores, contratistas, asesores o funcionarios de la entidad, que tengan necesidad de conocerla en cumplimiento de sus obligaciones contractuales, si ello resulta necesario. Para cualquier uso distinto o suministro a terceros, la entidad destinataria deberá solicitar aprobación previa y escrita a la AND.

Se entenderá por "Información Confidencial" toda la información que la AND suministre verbalmente, en documentos físicos o en medios magnéticos al Superintendencia de Transporte, o a la que esta pueda tener acceso en virtud de la discusión de la propuesta. Tal información comprende, pero no está limitada a,

información comercial, estratégica, contractual, operativa, planes de negocio, de desarrollo, información técnica, tecnológica, financiera, contable, legal, información sobre recursos humanos, planes de servicio, análisis y proyecciones, especificaciones, componentes de propiedad intelectual e industria, know how, diseños, modelos, procesos, equipos, software, proyectos e investigaciones de ciencia, tecnología e investigación, datos personales semiprivados, privados y/o sensibles, bases de datos personales y cualquier otro aspecto que concierne a las actividades desarrolladas por la AND, aun cuando no estén marcadas o identificadas como confidenciales.

La entrega de información sea confidencial o no, no concede, ni expresa ni implícitamente, autorización, permiso o licencia de uso de marcas, patentes, derechos de autor o de cualquier otro derecho de propiedad industrial o intelectual propiedad de la AND.

5. OBJETIVOS

5.1 Objetivo general

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.

5.2 Objetivos Específicos

- Establecer la Línea Base: Diagnosticar y documentar el estado actual de la infraestructura de ciberseguridad para identificar brechas y priorizar las intervenciones técnicas.
- Fortalecer la Infraestructura Técnica: Implementar controles y herramientas tecnológicas que aseguren la protección de los activos críticos de información de la entidad.
- Gestionar Vulnerabilidades y Riesgos: Ejecutar pruebas de intrusión (Pentesting) y escaneos de vulnerabilidades para remediar fallos de seguridad de manera proactiva.
- Promover la Cultura de Ciberseguridad: Capacitar y concientizar al personal de la Superintendencia a través de cursos de phishing y charlas de seguridad digital para

reducir riesgos por error humano.

- Asegurar el Cumplimiento Normativo: Alinear la gestión de la entidad con las directrices de seguridad y privacidad de la información dictadas por el Ministerio TIC.

6. JUSTIFICACIÓN

6.1 Fundamentación Constitucional y Legal

El proyecto se basa en los fines esenciales del Estado (Artículo 2 de la Constitución Política), que exigen a las autoridades proteger a los residentes y asegurar el cumplimiento de los deberes sociales. Bajo este mandato, la **Superintendencia de Transporte**, como organismo encargado de la inspección, vigilancia y control, tiene la responsabilidad de garantizar que los servicios de transporte operen bajo principios de legalidad y seguridad, lo cual depende hoy directamente de la integridad de su infraestructura digital.

6.2 Vulnerabilidad de la Infraestructura de Información

La entidad gestiona activos de información críticos que soportan la supervisión del transporte a nivel nacional. La ausencia de un esquema robusto de ciberseguridad Fase II expondría a la Superintendencia a riesgos de interrupción del servicio, pérdida de datos sensibles y ataques de terceros que podrían comprometer la soberanía de la información estatal. La justificación técnica radica en que la infraestructura actual requiere un fortalecimiento para enfrentar amenazas avanzadas que los controles básicos no pueden mitigar.

6.3 Necesidad de una Cultura de Seguridad Digital

Se identifica que el factor humano representa una de las mayores vulnerabilidades en la cadena de custodia de la información. El proyecto se justifica en la necesidad de implementar estrategias de concientización, como simulacros de *phishing* y capacitaciones especializadas, para transformar el comportamiento de los funcionarios y contratistas frente a los riesgos digitales, reduciendo así la probabilidad de incidentes causados por errores involuntarios o ingeniería social.

6.4 Alineación con Políticas de Gobierno Digital

El Estado Colombiano, a través del Ministerio TIC, ha establecido directrices estrictas en el Modelo de Seguridad y Privacidad de la Información (MSPI). La ejecución de este proyecto es necesaria para que la Superintendencia cumpla con el marco normativo vigente y se integre de manera segura a los servicios ciudadanos digitales, garantizando que el tratamiento de datos personales y estratégicos se realice bajo estándares

internacionales de seguridad.

6.5 Continuidad Operativa y Gestión de Crisis

La justificación operativa se centra en la capacidad de respuesta. El proyecto no solo busca prevenir ataques, sino asegurar que, en caso de un incidente, la entidad posea la capacidad técnica y procedimental para recuperar sus servicios en tiempos mínimos (RTO y RPO definidos), evitando impactos económicos y sociales derivados de la parálisis de las actividades de vigilancia y control en el sector transporte.

6.6 Eficiencia en la Contratación Pública

Finalmente, el uso de la figura del **Convenio Interadministrativo** con la **Agencia Nacional Digital (AND)** se justifica en la optimización de recursos y la transferencia de conocimiento. La AND, como entidad especializada del Estado, ofrece la idoneidad técnica requerida para la ejecución de proyectos de alta complejidad tecnológica, asegurando que el fortalecimiento de la ciberseguridad se realice con el mayor nivel de experiencia y bajo principios de economía y transparencia.

Este proyecto permitirá a la entidad:

- Robustecer sus capacidades de supervisión: Fortalecer las funciones de inspección, vigilancia y control a nivel nacional mediante una infraestructura digital más segura y confiable.

- Garantizar la continuidad operativa: Asegurar que los servicios y procesos misionales de la entidad no se vean interrumpidos por incidentes o ataques cibernéticos.

- Proteger la información institucional: Resguardar la confidencialidad, integridad y disponibilidad de los datos sensibles manejados por la Superintendencia.

- Identificar y mitigar vulnerabilidades: Detectar fallos de seguridad de forma proactiva a través de pruebas de intrusión (Pentesting) y escaneos técnicos antes de que sean explotados.

- Reducir el riesgo del factor humano: Elevar el nivel de conciencia y preparación de los funcionarios y contratistas frente a amenazas como el phishing y la ingeniería social.

- Cumplir con estándares nacionales: Alinear la gestión de la entidad con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI) del

Ministerio TIC.

- Establecer una línea base técnica: Contar con un diagnóstico claro y documentado de su estado de seguridad para la toma de decisiones estratégicas en tecnología.

7. ALCANCE

La presente propuesta tiene como alcance 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 este marco, el alcance comprende 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.

Adicionalmente, el alcance incluye el **fortalecimiento de 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.

El plan 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, el alcance del plan 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.

8. FASES

A continuación, se describen las actividades que se realizarán en cada fase.

Fase	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	líticas de ciberseguridad orradores)	Desarrollo políticas institucionales

Fase	Actividad	Descripción
	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	lan de Respuesta a Incidentes (IRP)	Desarrollo plan de reacción

Fase	Actividad	Descripción
	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

Fase	Actividad	Descripción
	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
	Transferencia de Conocimiento y Cierre Ejecutivo CISO Etapa II	Documentación de resultados
1 2	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.
	edición de madurez final y roadmap futuro	Comparativo estado inicial/final

Nota aclaratoria del numeral 2 de la tabla anterior:

Las actividades podrán adquirirse en el mercado, de conformidad con el Manual de Contratación de la AND, y que la Agencia actuará en calidad de articuladora y supervisora.

9. METODOLOGÍA DE EJECUCIÓN

Para la ejecución del proyecto de Ciberseguridad Fase II, se emplea una combinación de metodologías ágiles, marcos de referencia internacionales y estándares técnicos de seguridad digital. Esta estructura híbrida garantiza que el proyecto sea flexible pero rigurosamente técnico

Metodología de Gestión de Proyectos

Se utiliza un enfoque basado en Scrum adaptado a la administración pública, lo que permite:

- Iteraciones por Hitos: El proyecto no se entrega en bloque al final, sino que se divide en 4 entregables (hitos) que permiten revisiones constantes.
- Seguimiento Semanal: Reuniones de control entre la Agencia Nacional Digital y la OTIC de la Superintendencia para ajustar el cronograma ante cualquier riesgo.

Metodología de Seguridad

- El proyecto se alinea con estándares globales para asegurar que la infraestructura sea robusta:
- NIST Cybersecurity Framework (CSF): Se utiliza para las fases de Identificar, Proteger, Detectar, Responder y Recuperar.
- ISO/IEC 27001: Es el marco utilizado para la Fase 1 (Línea Base), evaluando el cumplimiento de controles de seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información (MSPI): Metodología obligatoria del Ministerio TIC de Colombia para entidades del Estado.

Metodología de Pruebas Técnicas (Pentesting)

- (Fortalecimiento e Infraestructura), se aplican metodologías de hacking ético reconocidas:
- OWASP (Open Web Application Security Project): Específicamente para la revisión de aplicaciones web y servicios ciudadanos de la entidad.
- OSSTMM (Open Source Security Testing Methodology Manual): Para las pruebas de intrusión en la infraestructura de red y comunicaciones.

Metodología para el Factor Humano

- Para los Simulacros de Phishing y capacitaciones, se sigue un ciclo de mejora continua:
- Línea Base de Engaño: Se lanza un primer simulacro sin aviso para medir la vulnerabilidad real.
- Micro-learning: Tras el simulacro, se entregan cápsulas de aprendizaje inmediato a quienes "cayeron" en la prueba.
- Evaluación Final: Medición del cambio de comportamiento tras las charlas de sensibilización.

Metodología de Implementación de IA

- Se utiliza una metodología de despliegue de modelos basada en: CRISP-DM (Cross-Industry Standard Process for Data Mining): Para asegurar que los agentes de IA comprendan el negocio (supervisión de transporte) antes de analizar los datos y detectar anomalías.

10. ENTREGABLES

Fase	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
3	Políticas de ciberseguridad (borradores)	Manual de políticas
	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

Fase	Actividad	Entregable
	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

11. CRONOGRAMA DEL PROYECTO

Fase	Actividad	Duración
1	Plan de trabajo	1 semana
	Cronograma	1 semana
	Evaluación de madurez en ciberseguridad	3 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Identificación de activos críticos	2 semanas
	Definición de KPIs y KRIs	1 semana
2	Evaluación de riesgos (Risk Assessment)	4 semanas
	Desarrollo e Implementación Plataforma Educativa periódica y certificación de cumplimiento en conocimientos de phishing al personal de la superintendencia	12 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Desarrollo y Suscripción de Contenidos y Mantenimiento a la plataforma educativa.	10 meses
	Roadmap de seguridad	2 semanas
	Políticas de ciberseguridad (borradores)	4 semanas
	Monitoreo mensual de credenciales expuestas en Dark Web + Sistema de Alertas.	9 meses con ejecución y reporte mensual.”
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas

3	Escaneo mensual de vulnerabilidades en activos tecnológicos. Volumen de Activos: más de 50 IPs/Activos.	9 meses Con ejecución y reporte mensual.”
	Charla ciberseguridad – Hacking #1	1 día
4	Implementación SOC/EDR básico	6 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Hardening endpoints/servidores	3 semanas
5	Implementación IAM	5 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Segmentación de red básica	3 semanas
6	Plan de Respuesta a Incidentes (IRP)	4 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Respaldo y recuperación de datos	3 semanas
7	Simulacro de incidente	2 días
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Gestión de vulnerabilidades continua	4 semanas
8	SOC avanzado & alertas 24/7	4 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Zero Trust (fase inicial)	4 semanas
9	Evaluación de riesgo proveedores	3 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
10	Charla ciberseguridad – Hacking #2	1 día
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Simulación phishing y cultura	3 semanas
11	Auditoría interna de ciberseguridad	3 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas

	Re-test controles críticos	2 semanas
12	Transferencia de Conocimiento y Cierre Ejecutivo CISO Etapa II	2 semanas
	Seguimiento y Control de Cumplimiento en Ciberseguridad	4 Semanas
	Medición de madurez final y roadmap futuro	3 semanas

12. COSTOS DEL PROYECTO

Teniendo en cuenta los costos aportes de las entidades el valor del convenio corresponde a MIL TRESCIENTOS TREINTA MILLONES CUATROCIENTOS DOCE MIL DOSCIENTOS SETENTA Y CINCO PESOS M/CTE., discriminado así:

VALOR APORTE SUPERTRANSPORTE	$1.308.983.200
CONTRAPARTIDA AND	$ 21.429.075
VALOR TOTAL DEL CONVENIO	$ 1.330.412.275

La contrapartida ofrecida por la AND se materializa en el aporte de personal por parte de la Agencia Nacional Digital, así:

Durante la ejecución del proyecto se dispondrá de un (1) Profesional de Tecnologías de la Información, con una dedicación del 35% de su tiempo, por un valor total de veintiún millones cuatrocientos veintinueve mil setenta y cinco pesos ($21.429.075 M/CTE).

Con base en lo anterior, se precisa que el valor correspondiente a la administración cobrada por la AND equivale al 5%.

En consecuencia, para efectos de la facturación establecida en la forma de pago, la AND deberá presentar una cuenta de cobro y una factura, siendo esta última la correspondiente al porcentaje de administración de la Agencia. Lo anterior, teniendo en cuenta que, al tratarse de un convenio interadministrativo, la AND debe legalizar cada uno de los pagos realizados con cargo a dicho convenio.

Finalmente, se aclara que la factura asociada al valor de administración corresponde a recursos propios de la Agencia.

13. FORMA DE PAGO

Se propone la siguiente forma de pago

Fases	Entregable	VALOR	VALOR TOTAL
1	Informe de plan de trabajo	$ 64.022.000	**$ 238.297.500**
	Cronograma	$ 59.500.000	
	Informe de madurez	$ 57.715.000	
	Informe de seguimiento	$ 11.900.000	
	Catálogo activos	$ 30.464.000	
	Matriz KPIs/KRIs	$ 14.696.500	
2	Matriz de riesgos	$ 29.800.000	**$ 180.100.000**
	Aplicativo funcional	$ 78.900.000	
	Informe de seguimiento	$ 11.900.000	
	Contenido inicial	$ 36.850.000	

	Documento roadmap	$ 22.650.000	
3	Manual de políticas	$ 35.521.500	**$ 142.090.200**
	Informe mensual técnico y ejecutivo	$ 31.808.700	
	Informe de seguimiento	$ 11.900.000	
	Informe mensual técnico y ejecutivo	$ 53.010.000	
	Sesión y material	$ 9.850.000	
4	SOC operativo	$ 143.250.000	**$ 178.600.000**
	Informe de seguimiento	$ 11.900.000	
	Reporte hardening	$ 23.450.000	
5	IAM configurado	$ 47.850.000	**$ 87.350.000**
	Informe de seguimiento	$ 11.900.000	
	Topología segura	$ 27.600.000	
6	Manual IRP	$ 29.450.000	**$ 80.144.000**
	Informe de seguimiento	$ 11.900.000	
	Plan BC/DR	$ 38.794.000	
7	Informe de simulacro	$ 12.350.000	**$ 61.050.000**
	Informe de seguimiento	$ 11.900.000	
	Reporte de vulnerabilidades	$ 36.800.000	
8	Reportes SOC	$ 96.750.000	**$ 123.150.000**
	Informe de seguimiento	$ 11.900.000	
	Documento Zero Trust	$ 14.500.000	
9	Reportes terceros	$ 20.400.000	**$ 32.300.000**
	Informe de seguimiento	$ 11.900.000	
10	Sesión y grabación	$ 9.850.000	**$ 40.450.000**
	Informe de seguimiento	$ 11.900.000	
	Reporte phishing	$ 18.700.000	
11	Informe auditoría	$ 36.850.000	**$ 78.100.000**
	Informe de seguimiento	$ 11.900.000	
	Reporte re-test	$ 29.350.000	

12	Informe final	$ 23.500.000	**$ 67.351.500**
	Informe de seguimiento	$ 11.900.000	
	Roadmap 2027	$ 31.951.500	
			$ 1.308.983.200

14. RIESGOS TECNICOS

Dada la naturaleza del proyecto y en atención a las actividades descritas anteriormente, se llevó a cabo el proceso de identificación, análisis y valoración de riesgos, a partir del cual se determinaron los principales riesgos asociados al desarrollo y ejecución del proyecto de ciberseguridad, que se relacionan a continuación.

	RIESGO		IMPACTO	ACCIONES DE MITIGACIÓN	ACCIONES DE CONTINGENCIA
R1	Retraso en la entrega de credenciales internas, accesos o permisos necesarios para ejecutar el pentest	Media	Alto	Solicitar accesos desde la fase de planeación. Validar responsables por cada sistema. Establecer fechas límite para entrega de credenciales. Realizar seguimiento diario a pendientes.	Reprogramar pruebas dependientes. Ajustar el cronograma según disponibilidad. Escalara supervisión del contrato para priorización.
R2	Indisponibilidad de personal técnico de la entidad para validaciones, pruebas o	Media	Alto	• Asegurar agenda con los	• Realizar

	revisiones			técnicos responsables. Coordinar reuniones con anticipación. ablecer suplencias por área.	validaciones parciales con personal disponible. • Ajustar actividades que no dependan del recurso faltante.
R3	Cambios no previstos en la infraestructura o configuraciones de los sistemas evaluados durante el pentest	Baja	Alto	Establecer *freeze period* durante la ejecución de pruebas. Validar versiones y configuraciones antes de iniciar. Documentar arquitectura inicial.	Reprogramar configuraciones y repetir pruebas afectadas. Aplicar rollback a versiones estables.
R4	No disponibilidad del personal para el curso de phishing o para asistir a la charla de ciberseguridad	Media	Medio	• Solicitar listado oficial desde la fase de planeación. • Acordar horarios con anticipación. • Validar la disponibilidad del espacio físico y plataforma.	Reprogramar sesiones. • Dividir la capacitación en grupos más pequeños. • Solicitar designación de reemplazos.

R5	Riesgo de filtración o mal manejo de documentos confidenciales entregados durante el proyecto	Baja	Alto	• Solicitar listado autorizado de personas que recibirán documentos. • Entregar archivos con control de acceso y trazabilidad. • Marcar todos los documentos como confidenciales.	• Revocar accesos de manera inmediata. • Notificar a la supervisión del contrato. • Emitir versión controlada de documentos afectados.
R6	Fallos en la plataforma de entrenamiento para el curso de phishing (accesos, disponibilidad, carga)	Baja	Medio	• Pruebas preliminares de acceso. • Validación anticipada de credenciales. • Soporte técnico asignado durante el módulo.	• Reintentar capacitación en ventana alternativa. • Habilitar plataforma de respaldo.
R7	Retrasos en aprobación de informes o actas que afectan los hitos de facturación	Media	Medio	• Alinear fechas de entrega desde el inicio. • Mantener comunicación continua con supervisión del contrato.	• Ajustar fechas internas sin afectar la final del proyecto. • Escalar a las instancias administrativas correspondientes.

				• Enviar borradores para revisión anticipada.	

15. **Condiciones para el Desarrollo del Proyecto**

Para garantizar la correcta ejecución del proyecto, el cumplimiento del cronograma y la calidad de los entregables, se establecen las siguientes condiciones:

a. La Superintendencia de Transporte será responsable de realizar todas las configuraciones, ajustes y validaciones en su infraestructura de seguridad perimetral (firewall, políticas, NAT, segmentación y reglas de acceso) necesarias para la correcta operación de los Access Points y la integración del canal de Internet adicional, actividades que no forman parte del alcance de la presente propuesta.

16. **Cierre del Proyecto**

La fase de cierre incluirá la validación final de los servicios entregados, la aceptación de entregables y la firma del acta de cierre. Se presentará un informe final con los logros alcanzados.