



Plan de Trabajo de Ciberseguridad Fase II

 INFORME TÉCNICO Y GERENCIAL

MARZO 2026

Superintendencia de Transporte de Colombia

Convenio Marco con la Agencia Nacional Digital

El presente informe técnico y gerencial constituye el instrumento de gestión para la ejecución ordenada, controlada y trazable de las actividades definidas en el cronograma del convenio, orientadas al fortalecimiento integral de la ciberseguridad institucional de la Superintendencia de Transporte.

Control de Versiones

El presente documento ha sido elaborado y controlado conforme a los estándares de gestión documental institucional. A continuación se presenta el registro oficial de versiones:

Versión	Editado por	Descripción	Firma
1.0	Virgilio Salgado	Creación de documento	✓



Este documento es de carácter institucional y está destinado a la Superintendencia de Transporte, supervisores del convenio y funcionarios públicos con responsabilidades en ciberseguridad.

Tabla de Contenido

El presente plan de trabajo se estructura en los siguientes componentes principales:

01	02	03
Generalidades del Proyecto	Objetivo del Plan	Alcance y Duración
Objeto, alcance del objeto y contexto institucional del convenio.	Propósito estratégico y técnico del plan de trabajo.	Límites del plan, actividades cubiertas y período de ejecución.
04	05	
Fases del Proyecto	Riesgos y Cronograma	
Descripción detallada de cada fase: Planeación, Línea Base y Ejecución (11 subfases).	Identificación de riesgos y cronograma oficial de actividades.	



1. Generalidades del Proyecto

1.1 Objeto del Proyecto

Aunar esfuerzos técnicos, administrativos y financieros en atención al componente de fortalecimiento de la infraestructura de ciberseguridad prevista en el convenio marco suscrito entre la **Agencia Nacional Digital** y la **Superintendencia de Transporte**, que permita robustecer las capacidades de inspección, vigilancia y control de la entidad a nivel nacional.

📄 **Marco institucional:** Este proyecto se enmarca en el Convenio Marco suscrito entre la Agencia Nacional Digital y la Superintendencia de Transporte, con el propósito de garantizar la protección de la información institucional y la continuidad operativa.

1.2 Alcance del Objeto

De acuerdo con el objeto del convenio y con el cronograma establecido, el alcance comprende la planeación, ejecución, seguimiento y cierre de un conjunto de actividades orientadas al **fortalecimiento integral de la infraestructura, capacidades y procesos de ciberseguridad** de la Superintendencia de Transporte, con el propósito de garantizar la protección de la información institucional, la continuidad operativa y el soporte seguro de las funciones misionales de Inspección, Vigilancia y Control a nivel nacional.

Para tal fin, el alcance del convenio incluye, sin limitarse a, el desarrollo de las siguientes actividades, organizadas conforme a las fases definidas en el cronograma anexo:

Componentes del Alcance (1/2)

Planeación y definición de línea base en ciberseguridad

Comprende la elaboración del plan de trabajo, diagnóstico del nivel de madurez institucional, identificación y clasificación de activos de información, definición de indicadores de gestión (KPIs y KRIs) y la caracterización del estado actual de la infraestructura tecnológica y de seguridad de la entidad.

Gestión de riesgos y fortalecimiento de controles de ciberseguridad

Mediante la identificación, análisis y valoración de riesgos cibernéticos, la formulación de la matriz de riesgos, la definición e implementación de controles técnicos y administrativos, así como la ejecución de actividades de hardening sobre los activos críticos de la Superintendencia de Transporte; lo anterior, con el fin de prevenir, mitigar y gestionar de manera oportuna posibles incidentes de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los activos institucionales, así como la continuidad de los servicios misionales de la entidad.

Implementación de capacidades técnicas de monitoreo y detección

Esto incluye la adopción y operación de mecanismos de monitoreo de seguridad, detección y respuesta a incidentes, gestión de vulnerabilidades y análisis de eventos de seguridad, orientados a fortalecer la capacidad institucional de prevención, detección temprana y respuesta frente a amenazas cibernéticas en la entidad.

Desarrollo e implementación de procesos de respuesta a incidentes y continuidad operativa

Este comprende la formulación, adopción e implementación de planes de respuesta a incidentes de seguridad de la información, planes de continuidad del negocio (BCP) y planes de recuperación ante desastres (DRP), así como la ejecución de ejercicios, pruebas técnicas y simulacros controlados orientados a validar su eficacia, nivel de madurez y capacidad de respuesta institucional, garantizando la continuidad de los servicios misionales y la mitigación de impactos operativos ante eventos extraordinarios.

Componentes del Alcance (2/2)

Fortalecimiento de la transformación digital segura

Aquí se incorpora mecanismos de protección, control, monitoreo y gestión de la seguridad de la información en los procesos digitales asociados a las funciones de Inspección, Vigilancia y Control, garantizando el cumplimiento de buenas prácticas, estándares de seguridad y lineamientos de protección de datos.

Transferencia de conocimiento y fortalecimiento de capacidades del talento humano

Mediante la ejecución de actividades estructuradas de capacitación, sensibilización y formación en ciberseguridad dirigidas al personal técnico y administrativo de la Superintendencia de Transporte, orientadas a fortalecer las competencias institucionales, promover el uso adecuado y la correcta operación de las soluciones tecnológicas implementadas.

Análisis comparativo y adopción de buenas prácticas

Este se dará a través de la revisión y análisis de modelos, tecnologías y esquemas de ciberseguridad implementados en entidades nacionales e internacionales, con el fin de seleccionar e incorporar las prácticas más efectivas y acordes con el ecosistema digital de la entidad.

Seguimiento, control y cierre del convenio

Mediante la elaboración, presentación y socialización de informes técnicos, administrativos y ejecutivos de avance, resultados y cierre, el seguimiento al cumplimiento de las actividades e hitos definidos en el cronograma aprobado, la verificación de entregables y la evaluación integral del convenio, incorporando recomendaciones orientadas a la mejora continua y al fortalecimiento sostenible de la postura de ciberseguridad institucional.

2. Objetivo del Plan de Trabajo

El presente plan de trabajo constituye el instrumento de gestión de corto y mediano plazo para la ejecución ordenada y controlada de las actividades definidas en el cronograma del convenio, orientadas al **fortalecimiento integral de la ciberseguridad institucional** de la Superintendencia de Transporte.

En este sentido, el plan tiene como objetivo planear, ejecutar y hacer seguimiento a las acciones técnicas, administrativas y operativas necesarias para la realización de:

Pruebas de Penetración

Pentest interno y externo sobre sistemas críticos

Evaluación de Vulnerabilidades

Análisis y gestión de riesgos cibernéticos

Controles de Seguridad

Implementación de medidas de mitigación

Monitoreo y Detección

Fortalecimiento de capacidades de respuesta a incidentes

Transferencia de Conocimiento

Capacitación al talento humano de la entidad

Objetivo Estratégico del Plan

El plan de trabajo contempla el desarrollo de actividades estructuradas que permiten:



Identificar debilidades

En la infraestructura tecnológica y en los procesos de seguridad de la información.



Evaluar riesgos asociados

A las amenazas cibernéticas y definir e implementar medidas de mitigación acordes con las mejores prácticas y estándares de ciberseguridad.



Incrementar la protección

Resiliencia y continuidad operativa de los sistemas de información de la Superintendencia de Transporte.

De manera transversal, el plan busca contribuir a la mejora de los procesos misionales de Inspección, Vigilancia y Control, asegurando que estos se soporten en entornos digitales confiables, seguros y controlados, y que se alineen con los lineamientos del Convenio Marco suscrito con la Agencia Nacional Digital y con los objetivos de transformación digital segura de la entidad.

3. Alcance del Plan de Trabajo

El presente plan de trabajo 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.

Pruebas de Penetración

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.

Fortalecimiento de Controles

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.

Alcance: Análisis, Documentación y Soporte Misional

1

Análisis y Reporte de Hallazgos

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.

2

Soporte a Funciones Misionales

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.

4. Duración del Plan

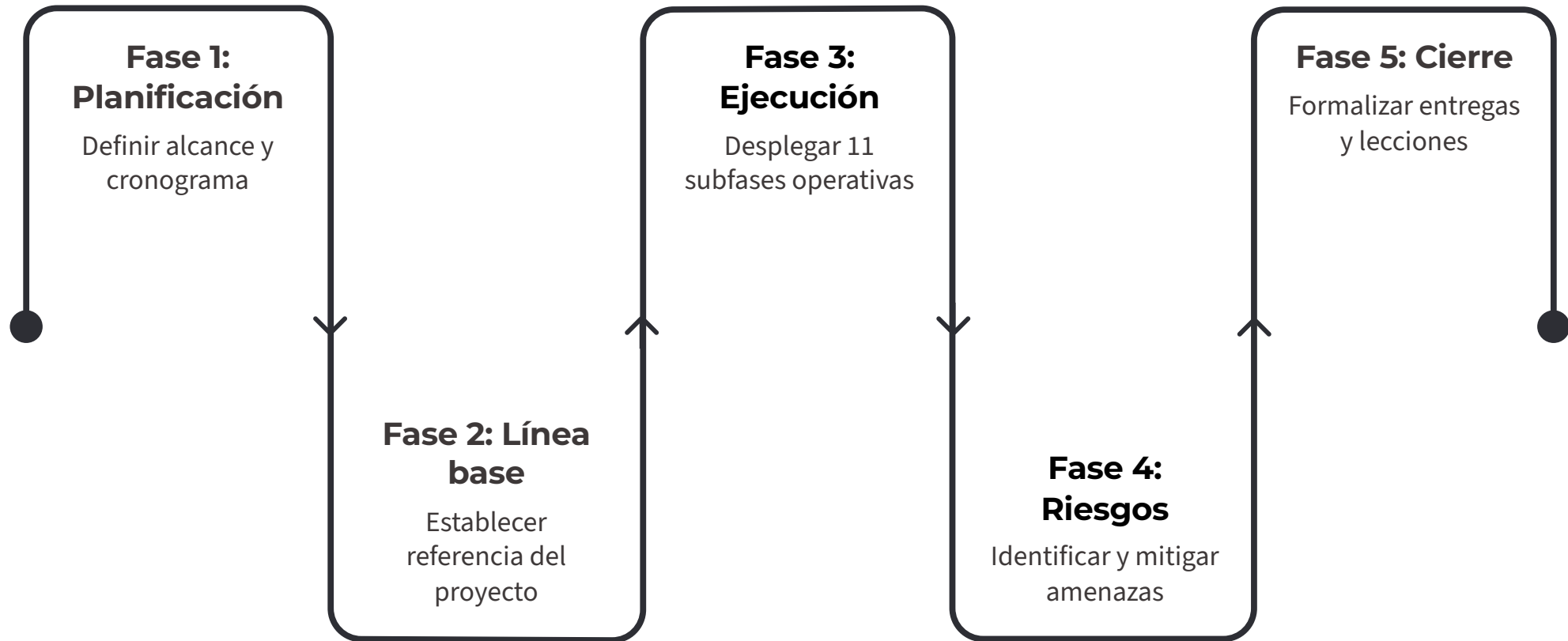
La duración del presente plan de trabajo comprende el período necesario para la planeación, ejecución, seguimiento y cierre de las actividades definidas en el cronograma del convenio, orientadas a la ejecución de pruebas de penetración (pentest), evaluaciones de seguridad, análisis de vulnerabilidades, fortalecimiento de controles técnicos y procedimentales, capacitación y transferencia de conocimiento, así como a la elaboración y entrega de informes técnicos y ejecutivos.

 **Fecha límite de culminación:** Las actividades se desarrollarán de manera progresiva y conforme a las fases establecidas en el cronograma, dentro del marco del convenio suscrito, y deberán ejecutarse en su totalidad hasta el **treinta (30) de diciembre de 2026**, fecha límite para la culminación del plan y la entrega de los productos y resultados correspondientes.

2026	12	30/12
Año de ejecución	Fases de ejecución	Fecha de cierre
Inicio: Marzo 2026	Planeación + Línea Base + 10 Ejecuciones	Max. Diciembre 2026

5. Fases del Proyecto: Visión General

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



El proyecto se estructura en fases progresivas que garantizan una ejecución ordenada, desde la planeación inicial hasta el cierre formal del convenio, pasando por la definición de la línea base y once subfases de ejecución técnica.

5.1 Fase 1: Planeación

La Fase 1 constituye el punto de partida formal del proyecto. Su propósito es establecer las bases contractuales, administrativas y técnicas que permitan una ejecución ordenada y controlada de todas las actividades previstas en el convenio.

Actividades

- **Acta de Inicio.**
- **Validación contractual, administrativa y técnica.**
- **Consolidación del inventario de sistemas a evaluar.**
- **Recolección de listados del personal con acceso autorizado a documentos confidenciales.**

Entregables

- **Plan de Trabajo aprobado.**
- **Cronograma oficial.**

Hitos

- **Firma del contrato.**
- **Aprobación de la planeación.**

5.2 Fase 2: Línea Base

La Fase 2 establece el diagnóstico inicial del estado de madurez en ciberseguridad de la Superintendencia de Transporte, identificando activos críticos y definiendo los indicadores de gestión que guiarán el seguimiento del proyecto.

Actividades

- Elaboración de Evaluación de madurez en ciberseguridad.
- Elaboración de Documento de Informe de Seguimiento.
- Elaboración de Catálogo de activos.
- Elaboración de Matriz KPIs/KRIs.

Entregables

- Documento de Madurez de ciberseguridad
- Documento de Informe de Seguimiento
- Documento de Catálogos Activos
- Documento de Matriz KPIs/KRIs

Importancia de la Línea Base en Ciberseguridad

La definición de la línea base es un componente estratégico fundamental del proyecto. Permite establecer el punto de partida medible desde el cual se evaluará el progreso y el impacto de todas las intervenciones técnicas posteriores.



Evaluación de Madurez

Diagnóstico del nivel actual de madurez institucional en ciberseguridad, identificando brechas y oportunidades de mejora.



Catálogo de Activos

Identificación y clasificación de todos los activos de información críticos de la entidad, base para la gestión de riesgos.



Matriz KPIs/KRIs

Definición de indicadores clave de rendimiento y riesgo que permitirán medir el avance y la efectividad de los controles implementados.

5.3 Fase 3 – Ejecución 1

La primera subfase de ejecución combina la actualización del diagnóstico de madurez con el lanzamiento de la plataforma educativa y la definición del roadmap estratégico de ciberseguridad.

Actividades

- Elaboración de Evaluación de madurez en ciberseguridad.
- Elaboración de plataforma educativa para la concientización y certificación de ciberseguridad.
- Elaboración de Informe de seguimiento sobre la ciberseguridad.
- Elaboración de cursos y contenido inicial para la plataforma educativa.
- Elaboración de Documento de roadmap sobre Ciberseguridad.

Entregables

- Documento de Madurez de ciberseguridad
- Plataforma Educativa en producción
- Documento informe de seguimiento
- Documento evidencia de los cursos
- Documento Road Map sobre Ciberseguridad

5.3 Fase 3 – Ejecución 2

La segunda subfase de ejecución se enfoca en la formulación de políticas de ciberseguridad, el monitoreo de credenciales expuestas en la Dark Web, el escaneo de vulnerabilidades y la primera charla de hacking ético.

Actividades

- Elaboración de borrador de política de ciberseguridad.
- Elaboración de informe técnico y ejecutivo mensual de credenciales expuestas.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.
- Elaboración de Escaneo mensual de vulnerabilidades en activos tecnológicos.
- Elaboración de Charla de Ciberseguridad Hacking #1.

Entregables

- Documento de borrador de política de ciberseguridad
- Documento técnico de credenciales expuestas
- Documento de seguimiento de control de cumplimiento de ciberseguridad
- Documento de escaneo mensual de vulnerabilidades
- Documento de evidencia de Charla de hacking

5.3 Fase 3 – Ejecución 3

La tercera subfase de ejecución marca un hito técnico fundamental: la implementación del SOC/EDR básico y la ejecución de actividades de hardening sobre endpoints y servidores críticos de la entidad.

Actividades

- Implementación de SOC/EDR básico.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.
- Elaboración de Reporte Hardening endpoints / Servidores.

Entregables

- Documento de evidencia de implementación de SOC/EDR
- Documento de seguimiento de control y cumplimiento
- Documento de Reporte de Hardening

❏ **Hito técnico clave:** La implementación del SOC/EDR básico representa el inicio de las capacidades de monitoreo continuo y detección de amenazas en tiempo real para la Superintendencia de Transporte.



5.3 Fase 3 – Ejecución 4

La cuarta subfase de ejecución se centra en la formulación del Manual de Respuesta a Incidentes (IRP) y el Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR), instrumentos fundamentales para la resiliencia operativa institucional.

Actividades

- Elaboración de Manual IRP.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.
- Elaboración de documento sobre PLAN BC/DR.

Entregables

- Documento de manual de IRP
- Documento de control y seguimiento de Ciberseguridad
- Documento de plan de BC/DR

Importancia del IRP y el Plan BC/DR

La formulación del Manual de Respuesta a Incidentes y el Plan de Continuidad del Negocio son pilares estratégicos para garantizar la resiliencia operativa de la Superintendencia de Transporte ante eventos de ciberseguridad.



Manual IRP

Instrumento que define los procedimientos, roles y responsabilidades para la detección, contención, erradicación y recuperación ante incidentes de seguridad de la información.



Plan BC/DR

Planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) que garantizan la continuidad de los servicios misionales ante eventos extraordinarios.



Resiliencia Operativa

La combinación de ambos instrumentos fortalece la capacidad institucional de respuesta y minimiza el impacto operativo de posibles incidentes cibernéticos.

5.3 Fase 3 – Ejecución 5

La quinta subfase de ejecución incluye la realización de simulacros de incidentes de seguridad y la generación de reportes de vulnerabilidades, actividades orientadas a validar la eficacia de los controles implementados y la capacidad de respuesta institucional.

Actividades

- Elaboración de informe de simulacro.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.
- Elaboración de Reporte de vulnerabilidades.

Entregables

- Documento de informe de simulacro
- Documento de control y seguimiento de Ciberseguridad
- Documento de Reporte de Vulnerabilidades

5.3 Fase 3 – Ejecución 6

La sexta subfase de ejecución eleva las capacidades de monitoreo con la generación del Reporte de SOC e introduce el modelo de seguridad Zero Trust como marco de referencia para la protección avanzada de los activos institucionales.

Actividades

- Elaboración de Reporte de SOC.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.
- Elaboración de Documento de Zero Trust.

Entregables

- Documento de Reporte de SOC
- Documento de Informe de Seguimiento y Control de Cumplimientos de Ciberseguridad
- Documento de Zero Trust



Zero Trust: La adopción del modelo Zero Trust representa un avance estratégico en la postura de seguridad institucional, basado en el principio de "nunca confiar, siempre verificar".

5.3 Fase 3 – Ejecución 7

La séptima subfase de ejecución se enfoca en la evaluación de riesgos asociados a terceros y proveedores, un componente crítico para garantizar la seguridad de la cadena de suministro tecnológico de la Superintendencia de Transporte.

Actividades

- Elaboración de Reporte de vulnerabilidades a terceros.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.

Entregables

- Documento de reporte de vulnerabilidades de terceros
- Documento de Seguimiento y Control de Cumplimientos de Ciberseguridad

5.3 Fase 3 – Ejecución 8

La octava subfase de ejecución combina la segunda charla de hacking ético con la realización de simulaciones de phishing, actividades orientadas a fortalecer la cultura de ciberseguridad del personal de la entidad.

Actividades

- Elaboración de Charla de Ciberseguridad Hacking #2.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.
- Elaboración de Reporte de Phishing.

Entregables

- Documento de Charla de Ciberseguridad
- Documento de informe de Seguimiento y Control de Cumplimiento en Ciberseguridad
- Documento de reporte de Phishing

5.3 Fase 3 – Ejecución 9

La novena subfase de ejecución contempla la realización de la Auditoría Interna de Ciberseguridad, un proceso de evaluación independiente que permite verificar el cumplimiento de los controles implementados y la efectividad de las medidas adoptadas.

Actividades

- Elaboración de Informe de Auditoría Interna.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.

Entregables

- Documento de Auditoría Interna
- Documento de Seguimiento y Control de Cumplimiento en Ciberseguridad

5.3 Fase 3 – Ejecución 10

La décima subfase de ejecución culmina con la elaboración del Informe Final Ejecutivo del CISO, documento de alto nivel que consolida los resultados, hallazgos y recomendaciones estratégicas del proyecto para la toma de decisiones directivas.

Actividades

- Elaboración de informe Final ejecutivo de CISO.
- Elaboración de Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad.

Entregables

- Documento de informe Final Ejecutivo de CISO
- Documento de Seguimiento y Control de Cumplimiento en Ciberseguridad



5.3 Fase 3 – Ejecución 11: Cierre

La undécima y última subfase de ejecución corresponde al cierre formal del convenio, con la generación del informe de cierre con recomendaciones y la firma del acta de cierre/liquidación.

Actividades

- Generación del informe de cierre con recomendaciones.
- Firma de acta de cierre/liquidación.

Entregables

- Documentación de cierre con recomendaciones
- Documento de Cierre



Cierre formal: La firma del acta de cierre/liquidación constituye el hito final del convenio, certificando el cumplimiento de todas las actividades y entregables comprometidos.

Resumen de Fases y Entregables del Proyecto

El siguiente cuadro consolida todas las fases del proyecto con sus respectivos entregables principales:

Fase	Nombre	Entregables Principales
Fase 1	Planeación	Plan de Trabajo aprobado, Cronograma oficial
Fase 2	Línea Base	Madurez ciberseguridad, Catálogo activos, Matriz KPIs/KRIs
Ejec. 1	Plataforma Educativa y Roadmap	Plataforma Educativa en producción, Road Map Ciberseguridad
Ejec. 2	Políticas y Vulnerabilidades	Borrador política, Escaneo vulnerabilidades, Charla Hacking #1
Ejec. 3	SOC/EDR y Hardening	Implementación SOC/EDR, Reporte Hardening
Ejec. 4	IRP y BC/DR	Manual IRP, Plan BC/DR
Ejec. 5	Simulacro y Vulnerabilidades	Informe simulacro, Reporte vulnerabilidades
Ejec. 6	SOC Avanzado y Zero Trust	Reporte SOC, Documento Zero Trust
Ejec. 7	Vulnerabilidades Terceros	Reporte vulnerabilidades terceros
Ejec. 8	Hacking #2 y Phishing	Charla Hacking #2, Reporte Phishing
Ejec. 9	Auditoría Interna	Informe Auditoría Interna
Ejec. 10	Informe Final CISO	Informe Final Ejecutivo CISO
Ejec. 11	Cierre	Documentación de cierre, Acta de cierre/liquidación

Arquitectura de Capacidades de Ciberseguridad

El proyecto construye de manera progresiva un conjunto de capacidades institucionales de ciberseguridad, organizadas en capas que se complementan y refuerzan mutuamente:



6. Gestión de Riesgos del Proyecto

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:



Metodología: El proceso de gestión de riesgos sigue las mejores prácticas de identificación, análisis, valoración y tratamiento de riesgos, alineado con los estándares internacionales de gestión de riesgos en proyectos de ciberseguridad.

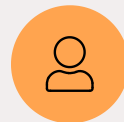
Categorías de Riesgos Identificados

Los riesgos del proyecto han sido clasificados en las siguientes categorías principales, cada una con sus respectivas medidas de mitigación:



Riesgos de Cronograma

Retrasos en la entrega de inventarios, documentos o accesos por parte de la entidad que puedan afectar el inicio o desarrollo de actividades dependientes.



Riesgos de Recursos Humanos

Disponibilidad limitada del personal técnico y administrativo de la Superintendencia para participar en las actividades del proyecto.



Riesgos Técnicos

Complejidad o indisponibilidad de los sistemas a evaluar, restricciones de acceso a infraestructura crítica o incompatibilidades tecnológicas.



Riesgos Contractuales

Cambios en el alcance, modificaciones contractuales o situaciones administrativas que puedan afectar la ejecución del convenio.

Matriz de Riesgos: Probabilidad e Impacto

La siguiente matriz ilustra la distribución de los riesgos identificados según su probabilidad de ocurrencia e impacto potencial sobre el proyecto:

GESTIÓN DE RIESGOS - PROYECTO CIBERSEGURIDAD					
ID	RIESGO	PROBABILIDAD	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.	• Reprogramar pruebas dependientes.
				• Validar responsables por cada sistema.	• Ajustar el cronograma según disponibilidad.
				• Establecer fechas límite para entrega de credenciales.	• Escalar a supervisión del contrato para priorización.
				• Realizar seguimiento diario a pendientes.	
R2	Indisponibilidad de personal técnico de la entidad para validaciones, pruebas o revisiones	Media	Alto	• Asegurar agenda con los técnicos responsables.	• Realizar validaciones parciales con personal disponible.
				• Coordinar reuniones con anticipación.	• Ajustar actividades que no dependan del recurso faltante.
				• Establecer suplencias por área.	
R3	Cambios no previstos en la infraestructura o configuraciones de los sistemas evaluados durante el pentest	Baja	Alto	• Establecer <i>freeze period</i> durante la ejecución de pruebas.	• Reprogramar configuraciones y repetir pruebas afectadas.
				• Validar versiones y configuraciones antes de iniciar.	• Aplicar rollback a versiones estables.
				• Documentar arquitectura inicial.	
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.	• Reprogramar sesiones.
				• Acordar horarios con anticipación.	• Dividir la capacitación en grupos más pequeños.
				• Validar la disponibilidad del espacio físico y plataforma.	• 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.	• Revocar accesos de manera inmediata.
				• Entregar archivos con control de acceso y trazabilidad.	• Notificar a la supervisión del contrato.
				• Marcar todos los documentos como confidenciales.	• 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.	• Reintentar capacitación en ventana alternativa.
				• Validación anticipada de credenciales.	• Habilitar plataforma de respaldo.
				• Soporte técnico asignado durante el módulo.	
R7	Retrasos en aprobación de informes o actas que afectan los hitos de facturación	Media	Medio	• Alinear fechas de entrega desde el inicio.	• Ajustar fechas internas sin afectar la final del proyecto.
				• Mantener comunicación continua con supervisión del contrato.	• Escalar a las instancias administrativas correspondientes.
				• Enviar borradores para revisión anticipada.	
ASPECTOS CLAVES					
El tiempo es un factor de riesgo en cadena: El retraso en la entrega de accesos (R1) o la demora en aprobar informes (R7) no solo retrasa el cronograma técnico, sino que afecta directamente los hitos de facturación. Es un llamado a la agilidad administrativa. La escalabilidad como vía de escape: En las acciones de contingencia (R1, R5, R7) aparece frecuentemente "Escalar a supervisión del contrato". Esto deja claro que el equipo técnico no se quedará de brazos cruzados si hay bloqueos; se involucrará a la gerencia rápidamente para destrabar el proceso. Planes B técnicos y logísticos ya establecidos: Se tienen contempladas alternativas si algo falla. Por ejemplo, si falla la plataforma de phishing (R6), hay ventanas alternativas; o si la gente no va a la charla (R4), se dividirá en grupos más pequeños. Estabilidad en la Infraestructura (Freeze Period): Requerimos congelar cambios y actualizaciones no planificadas durante la ejecución del pentest para garantizar resultados precisos y evitar falsos positivos. Tiempos de Respuesta Ágiles: La entrega oportuna de credenciales de acceso y la aprobación de informes son el motor que mantiene nuestro cronograma e hitos al día. Compromiso en las Capacitaciones: El éxito de las pruebas de phishing y las charlas depende de la asistencia de su equipo. Contamos con flexibilidad, pero necesitamos su priorización. Comunicación y Escalabilidad: Ante cualquier bloqueo técnico o administrativo, escalaremos de inmediato a la supervisión del contrato para no perder impulso. Máxima Confidencialidad: Toda la información y hallazgos descubiertos serán manejados bajo el más estricto control de acceso y trazabilidad.					

Estrategias de Mitigación de Riesgos

Para cada categoría de riesgo identificada, se han definido estrategias de mitigación orientadas a reducir la probabilidad de ocurrencia y/o el impacto potencial sobre el proyecto:

→ **Gestión proactiva de dependencias**

Identificación temprana de todas las dependencias del proyecto con la entidad (inventarios, accesos, documentos) y establecimiento de fechas comprometidas con los responsables institucionales.

→ **Plan de comunicación estructurado**

Establecimiento de canales formales de comunicación, reuniones periódicas de seguimiento y escalamiento oportuno de bloqueos o impedimentos.

→ **Flexibilidad en la planificación**

Incorporación de holguras en el cronograma para actividades con dependencias externas, permitiendo absorber retrasos sin afectar los hitos críticos del proyecto.

→ **Protocolos de pruebas controladas**

Definición de ventanas de mantenimiento, ambientes de prueba y procedimientos de rollback para minimizar el impacto de las actividades técnicas sobre los sistemas en producción.

7. Cronograma del Proyecto

Fase 1 y 2

Las siguientes actividades corresponden a las fases iniciales del proyecto, con sus fechas tentativas de inicio, duración en días y fecha tentativa de finalización:

#	Actividad	Fecha Inicio	Días	Fecha Final
1	Plan de trabajo	3/03/26	7	10/03/26
1	Cronograma	3/03/26	7	10/03/26
1	Evaluación de madurez en ciberseguridad	3/03/26	21	24/03/26
1	Seguimiento y Control de Cumplimiento en Ciberseguridad	3/03/26	28	31/03/26
1	Identificación de activos críticos (depende de la entrega de inventario T.I)	Dependiente	14	Dependiente
1	Definición de KPIs y KRIs	3/03/26	7	10/03/26

Cronograma del Proyecto

Fase 3 (Parte 1)

#	Actividad	Fecha Inicio	Días	Fecha Final
2	Evaluación de riesgos (Risk Assessment)	3/03/26	28	31/03/26
2	Plataforma Educativa periódica y certificación de cumplimiento en conocimientos de phishing	12/03/26	84	4/06/26
2	Seguimiento y Control de Cumplimiento en Ciberseguridad	10/03/26	28	7/04/26
2	Desarrollo y Suscripción de Contenidos y Mantenimiento a la plataforma educativa	3/03/26	90	1/06/26
2	Roadmap de seguridad	10/03/26	14	24/03/26
3	Políticas de ciberseguridad (borradores) (depende de la entrega de los documentos)	25/03/26	28	Dependiente
3	Monitoreo mensual de credenciales expuestas en Dark Web + Sistema de Alertas	4/03/26	90	Dependiente
3	Seguimiento y Control de Cumplimiento en Ciberseguridad	10/04/26	28	8/05/26
3	Escaneo mensual de vulnerabilidades en activos tecnológicos. Volumen: más de 50 IPs/Activos	4/03/26	90	Dependiente
3	Charla ciberseguridad – Hacking #1	15/04/26	1	16/04/26

Cronograma del Proyecto

Fase 3 (Parte 2)

#	Actividad	Fecha Inicio	Días	Fecha Final
4	Implementación SOC/EDR básico	23/03/26	42	4/05/26
4	Seguimiento y Control de Cumplimiento en Ciberseguridad	15/03/26	28	12/04/26
4	Hardening endpoints/servidores (depende de la entrega de los códigos)	8/04/26	21	Dependiente
5	Implementación IAM (depende de la entrega de los documentos)	12/03/26	35	Dependiente
5	Seguimiento y Control de Cumplimiento en Ciberseguridad	12/03/26	28	9/04/26
5	Segmentación de red básica (depende de la entrega de los documentos)	12/03/26	21	Dependiente
6	Plan de Respuesta a Incidentes (IRP)	5/05/26	28	2/06/26
6	Seguimiento y Control de Cumplimiento en Ciberseguridad	5/05/26	28	2/06/26
6	Respaldo y recuperación de datos	5/05/26	21	26/05/26

Cronograma del Proyecto

Fase 3 (Parte 3)

#	Actividad	Fecha Inicio	Días	Fecha Final
7	Simulacro de incidente (depende de la fecha)	17/05/26	2	Dependiente
7	Seguimiento y Control de Cumplimiento en Ciberseguridad	17/05/26	28	14/06/26
7	Gestión de vulnerabilidades continua	17/05/26	28	14/06/26
8	SOC avanzado & alertas 24/7	23/05/26	28	20/06/26
8	Seguimiento y Control de Cumplimiento en Ciberseguridad	23/05/26	28	20/06/26
8	Zero Trust (fase inicial)	27/05/26	28	24/06/26
9	Evaluación de riesgo proveedores (depende de la entrega de documentos)	8/04/26	21	Dependiente
9	Seguimiento y Control de Cumplimiento en Ciberseguridad	12/04/26	28	10/05/26

Cronograma del Proyecto

Fase 3 (Parte 4) y Cierre

#	Actividad	Fecha Inicio	Días	Fecha Final
10	Charla ciberseguridad – Hacking #2	10/04/26	1	11/04/26
10	Seguimiento y Control de Cumplimiento en Ciberseguridad	12/04/26	28	10/05/26
10	Simulación phishing y cultura	20/04/26	21	11/05/26
11	Auditoría interna de ciberseguridad (depende de la entrega de documentos)	8/04/26	21	Dependiente
11	Seguimiento y Control de Cumplimiento en Ciberseguridad	12/04/26	28	10/05/26
11	Re-test controles críticos	24/04/26	14	8/05/26
12	Transferencia de Conocimiento y Cierre Ejecutivo CISO Etapa II	10/07/26	14	24/07/26
12	Seguimiento y Control de Cumplimiento en Ciberseguridad	10/07/26	28	7/08/26
12	Medición de madurez final y roadmap futuro	10/07/26	21	31/07/26

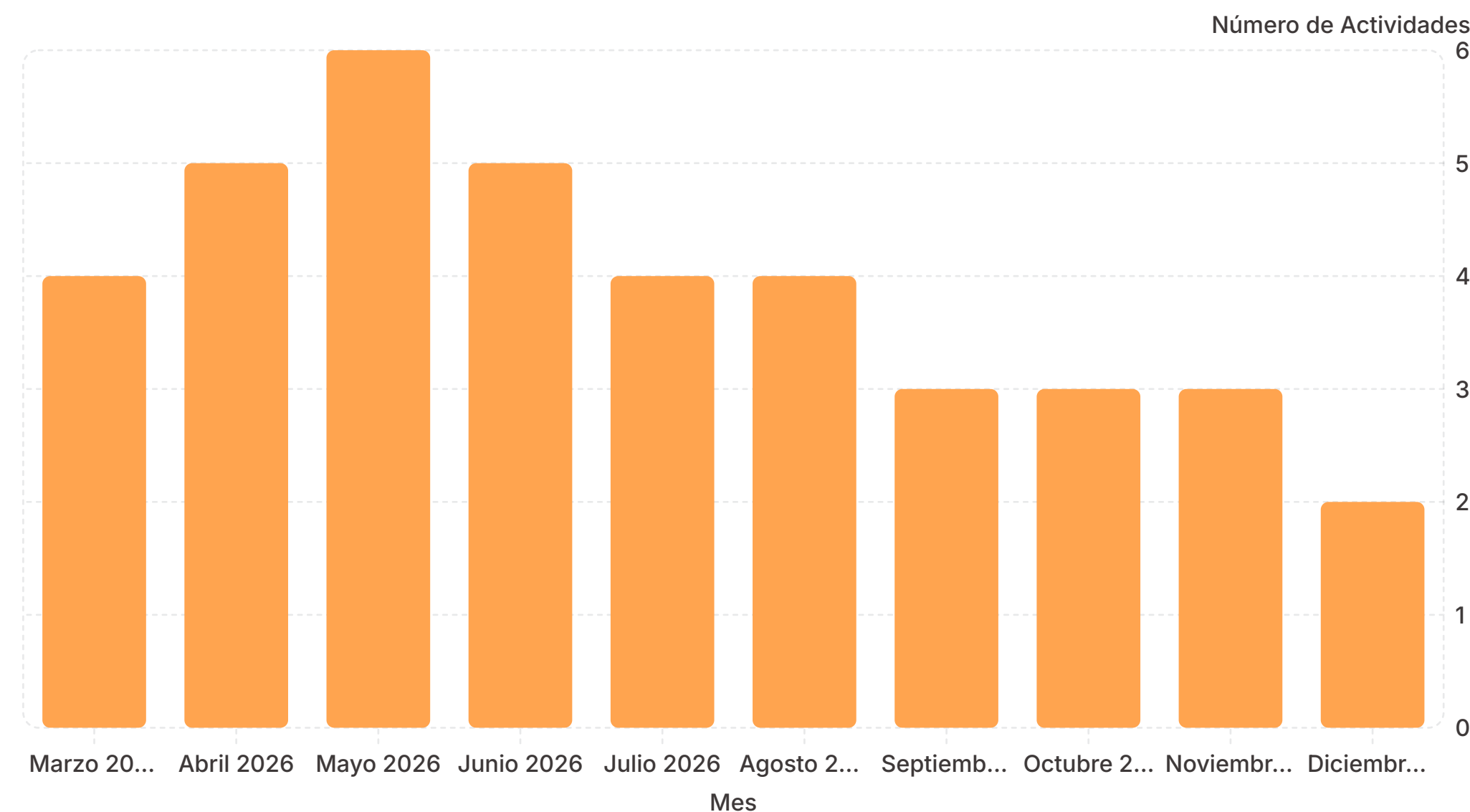
Timeline del Proyecto: Visión Ejecutiva

El siguiente diagrama presenta la línea de tiempo ejecutiva del proyecto, mostrando los hitos principales desde el inicio en marzo de 2026 hasta el cierre en diciembre de 2026:



Distribución de Actividades por Período

El siguiente gráfico muestra la distribución de actividades planificadas por mes durante el período de ejecución del proyecto:



Source:

Como se observa en el gráfico, la mayor concentración de actividades se produce entre marzo y junio de 2026, con un pico en mayo con 6 actividades. Este período inicial es crucial para las fases técnicas más intensivas del proyecto, incluyendo la implementación del SOC/EDR, el hardening, los planes IRP y BC/DR, y las actividades de formación. A partir de julio, el número de actividades disminuye progresivamente hacia el cierre del proyecto en diciembre.

Actividades con Dependencias Externas

Varias actividades del cronograma presentan dependencias de entregas por parte de la Superintendencia de Transporte. Su gestión oportuna es crítica para el cumplimiento del cronograma:

1

Identificación de activos críticos

Depende de la entrega del inventario de T.I. por parte de la entidad. Duración estimada: 14 días desde la fecha de entrega.

2

Políticas de ciberseguridad

Depende de la entrega de documentos base. Fecha tentativa de inicio: 25/03/2026. Duración: 28 días.

3

Hardening endpoints/servidores

Depende de la entrega de los códigos de acceso. Fecha tentativa: 08/04/2026. Duración: 21 días.

4

Implementación IAM y Segmentación de red

Dependen de la entrega de documentos técnicos. Fecha tentativa: 12/03/2026. Duraciones: 35 y 21 días respectivamente.

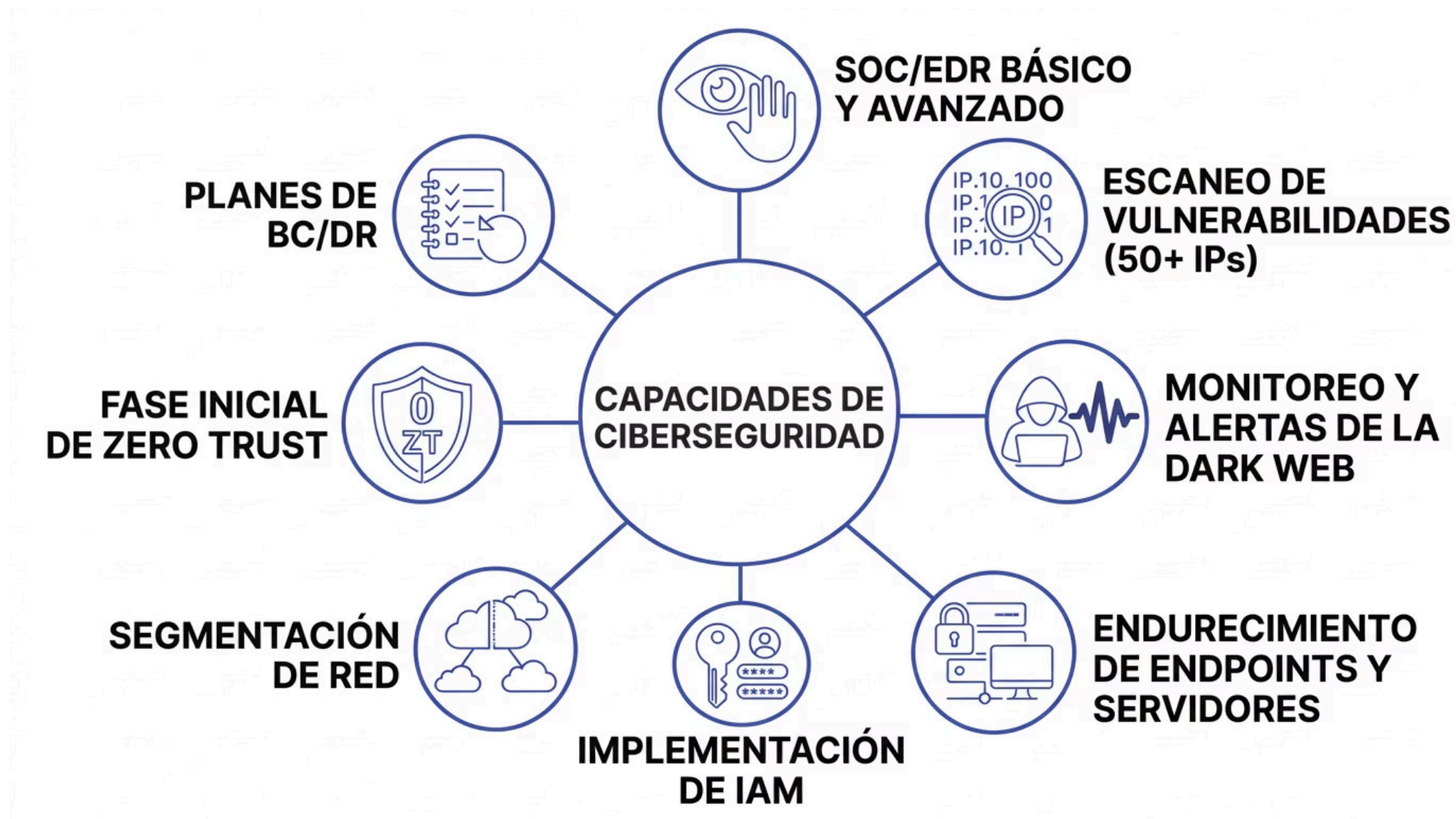
5

Evaluación de riesgo proveedores y Auditoría interna

Dependen de la entrega de documentos. Fecha tentativa: 08/04/2026. Duración: 21 días cada una.

Capacidades Técnicas a Implementar

El proyecto contempla la implementación de un conjunto de capacidades técnicas de ciberseguridad que transformarán la postura de seguridad de la Superintendencia de Transporte:



Programa de Formación y Concientización

El proyecto incorpora un robusto programa de transferencia de conocimiento y fortalecimiento de capacidades del talento humano, estructurado en múltiples componentes:



Plataforma Educativa

Elaboración de plataforma educativa para la concientización y certificación de ciberseguridad, con desarrollo y suscripción de contenidos y mantenimiento continuo. Período: 12/03/26 – 4/06/26 (84 días).



Charlas de Hacking Ético

Dos charlas de ciberseguridad sobre hacking ético: Charla #1 el 15/04/26 y Charla #2 el 10/04/26, orientadas a fortalecer la conciencia de seguridad del personal técnico y administrativo.



Simulación de Phishing

Simulación de phishing y cultura de seguridad, con generación de reporte de resultados. Período: 20/04/26 – 11/05/26 (21 días).



Cierre Ejecutivo CISO

Transferencia de Conocimiento y Cierre Ejecutivo CISO Etapa II, con medición de madurez final y roadmap futuro. Período: 10/07/26 – 24/07/26 (14 días).

Indicadores de Gestión: KPIs y KRIs

La Fase 2 (Línea Base) contempla la definición de una Matriz de KPIs y KRIs que permitirá medir el avance y la efectividad del proyecto. A continuación se presentan los tipos de indicadores a definir:

KPIs – Indicadores Clave de Rendimiento

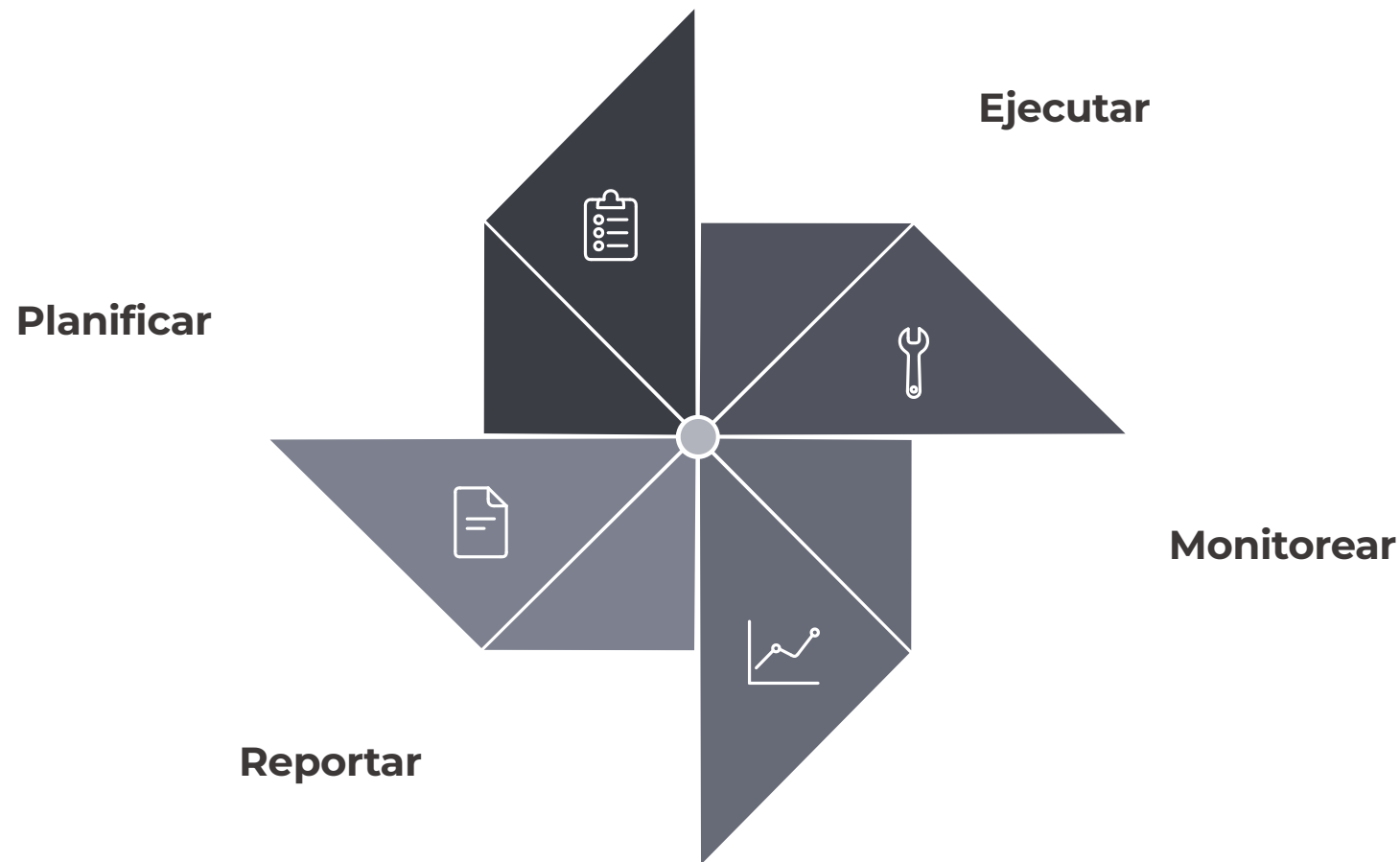
- Porcentaje de actividades ejecutadas vs. planificadas
- Número de entregables entregados en tiempo
- Porcentaje de vulnerabilidades remediadas
- Nivel de madurez en ciberseguridad (inicial vs. final)
- Porcentaje de personal capacitado en ciberseguridad
- Tiempo promedio de detección y respuesta a incidentes

KRIs – Indicadores Clave de Riesgo

- Número de vulnerabilidades críticas identificadas sin remediar
- Número de credenciales expuestas en Dark Web
- Número de incidentes de seguridad detectados
- Porcentaje de activos sin hardening aplicado
- Número de terceros con riesgos de seguridad identificados
- Tiempo de recuperación ante incidentes (RTO/RPO)

Modelo de Seguimiento y Control

El proyecto contempla un modelo de seguimiento y control continuo a lo largo de todas las fases de ejecución, garantizando la trazabilidad, el cumplimiento y la calidad de los entregables:



El Informe de Seguimiento y Control de Cumplimiento en Ciberseguridad es un entregable recurrente en todas las subfases de ejecución, garantizando visibilidad continua sobre el avance del proyecto y el estado de cumplimiento de los controles de seguridad.

Alineación con Estándares y Marcos de Referencia

El proyecto se alinea con los principales estándares y marcos de referencia internacionales en ciberseguridad, garantizando que las actividades, controles y entregables cumplan con las mejores prácticas reconocidas:

NIST CSF

Marco de Ciberseguridad del NIST: Identificar, Proteger, Detectar, Responder y Recuperar.

ISO 27001

Sistema de Gestión de Seguridad de la Información (SGSI) para la protección de activos de información.

OWASP

Mejores prácticas para la seguridad de aplicaciones web y móviles en las pruebas de penetración.

MITRE ATT&CK

Marco de referencia para la identificación y análisis de tácticas, técnicas y procedimientos de amenazas cibernéticas.

CIS Controls

Controles de seguridad críticos para la protección de sistemas y redes institucionales.

Transformación Digital Segura

El proyecto contribuye de manera directa a la consolidación de la transformación digital segura de la Superintendencia de Transporte, alineándose con los objetivos del Convenio Marco suscrito con la Agencia Nacional Digital.

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.

Seguridad

Protección de la información institucional y los activos críticos

Resiliencia

Continuidad operativa ante eventos extraordinarios

Confianza

Entornos digitales confiables para las funciones misionales

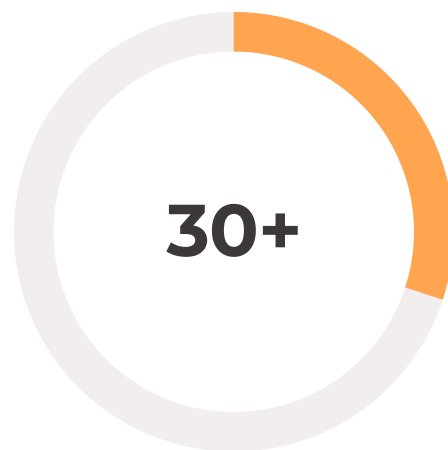
Resultados Esperados del Proyecto

Al finalizar la ejecución del Plan de Trabajo de Ciberseguridad – Fase II, la Superintendencia de Transporte contará con los siguientes resultados:



Fases completadas

Planeación, Línea Base y 11 subfases de ejecución técnica



Entregables documentales

Informes técnicos, ejecutivos, manuales y reportes de seguridad



Cobertura de seguimiento

Informes de seguimiento y control en todas las subfases

→ Infraestructura de ciberseguridad robustecida

Con SOC/EDR, hardening, IAM, segmentación de red y Zero Trust implementados.

→ Talento humano capacitado

Con plataforma educativa, charlas de hacking ético y simulaciones de phishing completadas.

→ Capacidades de respuesta fortalecidas

Con Manual IRP, Plan BC/DR y simulacros de incidentes ejecutados y validados.

→ Postura de ciberseguridad medida y documentada

Con evaluaciones de madurez inicial y final, roadmap futuro e informe ejecutivo CISO.

Conclusiones y Compromisos Institucionales

El Plan de Trabajo de Ciberseguridad – Fase II representa un compromiso institucional de alto nivel entre la Superintendencia de Transporte y la Agencia Nacional Digital, orientado a garantizar la protección, resiliencia y continuidad operativa de los sistemas de información que soportan las funciones misionales de Inspección, Vigilancia y Control a nivel nacional.



Protección Institucional

Garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.



Continuidad Operativa

Asegurar la continuidad de los servicios misionales ante eventos extraordinarios mediante planes BCP y DRP.



Mejora Continua

Incorporar recomendaciones orientadas a la mejora continua y al fortalecimiento sostenible de la postura de ciberseguridad institucional.



Fecha límite de ejecución: Todas las actividades deberán ejecutarse en su totalidad hasta el **treinta (30) de diciembre de 2026**, fecha límite para la culminación del plan y la entrega de los productos y resultados correspondientes. **Elaborado por:** Virgilio Salgado | Versión 1.0 | Marzo 2026.