

Informe de seguimiento

Superintendencia de Transporte
Entregables de la fase orientados al fortalecimiento
institucional de la ciberseguridad

ABRIL 2026

Documento técnico para entrega institucional



**Agencia
Nacional Digital**



CONTROL DE CAMBIOS DEL DOCUMENTO

REVISIÓN No.	FECHA	DESCRIPCIÓN	AUTOR DEL CAMBIO
1	09/04/2026	Creación del documento	Virgilio Salgado



Agencia Nacional Digital



Contenido

1. Introducción	4
2. Marco teórico.....	5
3. Marco legal	5
4. Objetivo general	6
5. Objetivos específicos	6
6. Seguimiento	7
7. Proyección de la siguiente fase.....	9



**Agencia
Nacional Digital**



1. Introducción

En el marco del fortalecimiento continuo de la postura institucional de ciberseguridad de la Superintendencia de Transporte, durante la presente fase adelantamos el seguimiento técnico y ejecutivo sobre plataformas y servicios identificados como terceros, pero que mantienen relación funcional, operativa o tecnológica con la Entidad. Este ejercicio resulta de alta relevancia, en la medida en que la exposición al riesgo cibernético no se limita únicamente a la infraestructura propia, sino que también se extiende a aquellos componentes externos que, de una u otra forma, participan en el procesamiento de información, prestación de servicios, interoperabilidad tecnológica o soporte a procesos institucionales.

La revisión desarrollada en esta fase permitió consolidar una visión más amplia del nivel de exposición existente en el ecosistema digital relacionado con la Superintendencia, evidenciando que la seguridad institucional debe entenderse como una responsabilidad integral que abarca tanto los activos internos como los servicios de terceros con los cuales existe dependencia operativa o tecnológica. Desde esta perspectiva, el seguimiento efectuado no solo aporta valor técnico, sino que también constituye un insumo de alto nivel para la toma de decisiones, la priorización de acciones correctivas y la definición de medidas urgentes de mitigación.

2. Marco teórico

La gestión moderna de la ciberseguridad parte del principio de que toda organización opera dentro de un ecosistema interconectado, en el que proveedores, plataformas externas, servicios en la nube, aplicaciones de terceros, integraciones y componentes compartidos pueden convertirse en puntos de exposición relevantes. En este contexto, la gestión de vulnerabilidades sobre terceros se consolida como una práctica esencial para identificar debilidades que, aun cuando no residan directamente en la infraestructura interna de la Entidad, pueden generar impactos significativos sobre la confidencialidad, integridad, disponibilidad y continuidad de los servicios institucionales.

Desde el enfoque conceptual, una vulnerabilidad corresponde a una debilidad técnica, lógica, de configuración o de control que puede ser aprovechada por un actor malicioso para materializar accesos no autorizados, fuga de información, interrupción de servicios, escalamiento de privilegios o afectación reputacional. Cuando estas debilidades están presentes en plataformas de terceros vinculadas con la operación institucional, el riesgo se amplifica, pues la Entidad puede verse afectada sin que el origen del incidente se encuentre necesariamente dentro de su perímetro tecnológico directo. Por ello, el seguimiento de estos escenarios debe considerarse una actividad permanente, estratégica y prioritaria dentro del modelo de gestión del riesgo cibernético.

De igual forma, la literatura y las buenas prácticas internacionales en ciberseguridad coinciden en que la identificación temprana, valoración de criticidad, priorización y tratamiento oportuno de hallazgos son elementos fundamentales para reducir la probabilidad de incidentes y fortalecer la resiliencia digital. Bajo esta lógica, el seguimiento a terceros no debe asumirse como una actividad aislada o meramente técnica, sino como un componente de gobierno, control y supervisión que contribuye directamente a la estabilidad operativa y al cumplimiento institucional.

3. Marco legal

El presente informe de seguimiento se enmarca en la normativa colombiana aplicable a la seguridad de la información, protección de datos personales, gestión digital del Estado y fortalecimiento de capacidades institucionales frente al riesgo cibernético. En ese sentido, constituye un ejercicio alineado con



Agencia Nacional Digital



la necesidad de proteger los activos de información institucionales y de prevenir escenarios que puedan comprometer derechos, servicios, datos y procesos estratégicos de la Superintendencia de Transporte.

Como referentes principales, este seguimiento se soporta en la Ley 1581 de 2012, relativa al régimen general de protección de datos personales; la Ley 1273 de 2009, mediante la cual se incorporan conductas penales relacionadas con la protección de la información y de los datos; la Ley 1712 de 2014, en materia de transparencia y acceso a la información pública; el Decreto 1078 de 2015, que compila la regulación del sector TIC; y el Decreto 620 de 2020, que establece lineamientos generales en materia de Gobierno Digital. De igual forma, se articula con los lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC, así como con buenas prácticas internacionales orientadas a la mejora continua de la seguridad institucional.

Bajo este marco, el seguimiento efectuado adquiere una relevancia no solo técnica, sino también jurídica y administrativa, dado que la permanencia de brechas de seguridad en entornos tecnológicos relacionados con la Entidad puede derivar en afectaciones operativas, riesgos de cumplimiento, impactos reputacionales y eventuales consecuencias sobre la protección de la información. En consecuencia, la remediación oportuna de los hallazgos identificados debe entenderse como una necesidad institucional inmediata.

4. Objetivo general

Realizar el seguimiento técnico y gerencial a la evaluación de seguridad efectuada sobre aplicaciones y plataformas de terceros relacionadas con la Superintendencia de Transporte, con el fin de identificar el nivel de exposición al riesgo, consolidar el estado de criticidad de los hallazgos detectados y aportar insumos para la toma de decisiones orientadas a su tratamiento prioritario.

5. Objetivos específicos

Identificar y consolidar de manera ejecutiva los resultados obtenidos durante la revisión de seguridad realizada sobre plataformas de terceros vinculadas tecnológica o funcionalmente con la Entidad.



Agencia Nacional Digital



Valorar la criticidad general de los hallazgos detectados, presentando una visión estadística que permita dimensionar el nivel de urgencia requerido para su atención.

Fortalecer la toma de decisiones institucional mediante la entrega de un informe de seguimiento orientado a la priorización de acciones correctivas y preventivas.

Establecer la continuidad del plan de trabajo en ciberseguridad, proyectando las actividades de la siguiente fase enfocadas en monitoreo, correlación de eventos y fortalecimiento de configuraciones seguras.

6. Seguimiento

Durante esta fase llevamos a cabo el reporte de vulnerabilidades sobre aplicaciones identificadas como terceras de la Superintendencia de Transporte, consolidando una revisión con enfoque técnico y gerencial que permitió dimensionar el nivel de exposición asociado a servicios externos relacionados con la operación institucional. Como resultado del ejercicio realizado, documentamos un total de **4 hallazgos relevantes**, de los cuales **2 corresponden a vulnerabilidades de alta criticidad** y **2 a vulnerabilidades de criticidad media**, sin registro de hallazgos clasificados en nivel bajo dentro del universo evaluado. Esta distribución evidencia un escenario que demanda atención prioritaria, debido a que el 50% de los hallazgos identificados se ubica en la franja de mayor severidad, lo que incrementa de forma considerable la probabilidad de afectaciones sobre la seguridad, disponibilidad, continuidad y confiabilidad de los servicios relacionados.

Desde una perspectiva ejecutiva, los resultados obtenidos en esta fase reflejan que la superficie de exposición asociada a terceros representa un riesgo real y vigente para la Entidad. La presencia de hallazgos de alta criticidad implica que existen condiciones que, de no ser intervenidas con urgencia, podrían facilitar escenarios de compromiso operacional, afectación a la trazabilidad de la información, impactos reputacionales, incremento del riesgo jurídico y debilitamiento general de la postura institucional de ciberseguridad. En términos gerenciales, no se trata de hallazgos menores ni diferibles, sino de situaciones que exigen acciones inmediatas de contención, tratamiento y seguimiento, debido a que su permanencia en el tiempo amplía la posibilidad de explotación y eleva el costo potencial de un incidente materializado.



Agencia Nacional Digital



En ese orden, el seguimiento de esta fase permite concluir que la Entidad requiere avanzar con prontitud en la remediación de los hallazgos identificados, bajo un enfoque de priorización por criticidad, impacto y exposición. La evidencia consolidada demuestra la necesidad de fortalecer de forma inmediata los mecanismos de control, supervisión y exigencia de seguridad sobre los entornos de terceros, con el fin de reducir la ventana de riesgo existente y evitar que debilidades actualmente detectadas puedan traducirse en eventos de afectación real para la Superintendencia de Transporte. La atención oportuna de estos resultados no solo constituye una medida de mejora técnica, sino una decisión estratégica indispensable para la protección institucional.

Resumen Estadístico de la Fase

Total de hallazgos identificados: 4

Categoría	Cantidad	Porcentaje
Alta Criticidad	2 hallazgos	50%
Criticidad Media	2 hallazgos	50%
Criticidad Baja	0 hallazgos	0%

7. Proyección de la siguiente fase

Como continuidad del plan de trabajo, se establece que la **fase 4** estará orientada al desarrollo de un componente de **SOC/SIEM** sobre los dispositivos que sean suministrados o compartidos para tal fin, con el propósito de fortalecer la capacidad de monitoreo, visibilidad, correlación de eventos y detección temprana de comportamientos anómalos o potencialmente maliciosos dentro del entorno tecnológico analizado. Esta siguiente etapa buscará avanzar desde una visión de hallazgos puntuales hacia una capacidad más estructurada de vigilancia y análisis de seguridad, permitiendo mejorar el nivel de madurez institucional frente a amenazas activas y eventos de riesgo. De igual manera, en dicha fase se contempla la elaboración de un **reporte de hardening** sobre las plataformas que fueron compartidas, enfocado en la revisión y fortalecimiento de configuraciones de seguridad, reducción de superficie de ataque, endurecimiento de servicios expuestos y mejora de controles técnicos base. Este componente será fundamental para traducir los hallazgos actuales en acciones concretas de fortalecimiento, contribuyendo a que la Entidad no solo identifique debilidades, sino que avance hacia su corrección estructural y la consolidación de una postura de seguridad más robusta, preventiva y sostenible.