

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. Objetivo General	4
3. Objetivos Específicos	4
4. Marco Legal.....	5
5. Marco Teórico.....	6
6. Desarrollo de la Fase 4.....	6
7. Conclusión	8



Agencia Nacional Digital



1. Introducción

En el marco del proyecto de fortalecimiento de la ciberseguridad institucional de la Superintendencia de Transporte, la Fase 4 se orienta a la implementación de controles técnicos y operativos enfocados en la reducción de la superficie de ataque, la mitigación de vulnerabilidades y el fortalecimiento de la capacidad de detección y respuesta ante incidentes de seguridad de la información.

Esta fase integra dos componentes fundamentales dentro de la estrategia de ciberseguridad: por un lado, el proceso de **hardening de plataformas tecnológicas**, enfocado en la aplicación de buenas prácticas de configuración segura; y por otro, la **implementación de un Centro de Operaciones de Seguridad (SOC)** basado en Wazuh, orientado al monitoreo continuo, correlación de eventos y gestión de incidentes.

Dado que no se contó con acceso directo al código fuente de las aplicaciones, el enfoque adoptado se fundamenta en estándares internacionales, análisis de vectores de ataque conocidos y lineamientos técnicos aplicables a múltiples tecnologías, garantizando así una aproximación integral y efectiva para la mitigación de riesgos.

2. Objetivo General

Fortalecer la postura de ciberseguridad de la Superintendencia de Transporte mediante la implementación de controles técnicos de hardening y la puesta en operación de un SOC basado en Wazuh, que permita la detección, monitoreo y respuesta oportuna ante eventos de seguridad.

3. Objetivos Específicos

- Implementar lineamientos de hardening orientados a la mitigación de vulnerabilidades críticas en entornos web y de infraestructura.
- Establecer controles de seguridad para prevenir ataques comunes como SQL Injection, XSS y Path Traversal.
- Desplegar una solución SIEM basada en Wazuh para la recolección, análisis y correlación de eventos de seguridad.



Agencia Nacional Digital



- Integrar herramientas de detección de intrusiones como Suricata para ampliar la visibilidad a nivel de red.
- Configurar mecanismos de monitoreo continuo y alertamiento automático para la gestión proactiva de incidentes.

4. Marco Legal

El desarrollo de la Fase 4 se fundamenta en un conjunto de normas, estándares y lineamientos que regulan la seguridad de la información en entidades públicas:

- **ISO/IEC 27001:2022:** Establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la gestión del riesgo.
- **Ley 1581 de 2012:** Regula la protección de datos personales en Colombia.
- **Ley 1273 de 2009:** Define los delitos informáticos y la protección de la información.
- **Decreto 1078 de 2015:** Establece lineamientos para la gestión de tecnologías de la información en el sector público.
- **Política de Gobierno Digital (MinTIC):** Define directrices para el uso estratégico y seguro de las TIC.
- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Orienta la implementación de controles de seguridad en entidades públicas.

Este marco normativo garantiza que las acciones implementadas se alineen con principios de legalidad, cumplimiento y buenas prácticas en ciberseguridad.



Agencia Nacional Digital



5. Marco Teórico

La seguridad de la información en entornos institucionales requiere la implementación de mecanismos que permitan no solo la protección preventiva, sino también la detección y respuesta ante amenazas. El **hardening** corresponde al proceso de fortalecimiento de sistemas mediante la reducción de vulnerabilidades, deshabilitación de servicios innecesarios y aplicación de configuraciones seguras. Este proceso busca minimizar la superficie de ataque y dificultar la explotación de fallas por parte de actores maliciosos.

Por su parte, un **SOC (Security Operations Center)** es una unidad centralizada encargada de monitorear, detectar y responder a incidentes de seguridad. Dentro de este esquema, los sistemas **SIEM (Security Information and Event Management)** como Wazuh permiten recolectar, normalizar y correlacionar eventos provenientes de múltiples fuentes, facilitando la identificación de patrones de ataque y comportamientos anómalos.

La integración de herramientas como **Suricata**, orientadas a la detección de intrusiones a nivel de red, complementa la visibilidad del entorno, permitiendo analizar tanto eventos del sistema como tráfico de red, logrando así un enfoque integral de seguridad.

En conjunto, estos componentes permiten la construcción de una arquitectura de ciberseguridad basada en monitoreo continuo, análisis de eventos y respuesta proactiva ante incidentes.

6. Desarrollo de la Fase 4

Durante la ejecución de la Fase 4 llevamos a cabo múltiples actividades orientadas al fortalecimiento técnico de la infraestructura tecnológica de la Superintendencia de Transporte, integrando prácticas de hardening con capacidades avanzadas de monitoreo y detección.

En primer lugar, desarrollamos un proceso de **hardening de plataformas**, enfocado en la mitigación de vulnerabilidades críticas identificadas en entornos web. A pesar de no contar con acceso al código fuente, logramos establecer lineamientos técnicos basados en buenas prácticas internacionales, permitiendo abordar riesgos asociados a ataques comunes como SQL Injection, Cross-Site Scripting (XSS) y Path Traversal. Para ello, se promovió el uso de consultas parametrizadas, validación estricta de entradas,



Agencia Nacional Digital



sanitización de datos y aplicación del principio de mínimo privilegio en bases de datos.

Adicionalmente, definimos configuraciones seguras para servidores web como **Apache y Nginx**, incluyendo la implementación de headers de seguridad, restricciones de métodos HTTP, uso de mecanismos de protección como WAF (Web Application Firewall) y control de tamaño de peticiones. También establecimos medidas transversales como el uso obligatorio de HTTPS, implementación de HSTS, gestión segura de logs y monitoreo continuo.

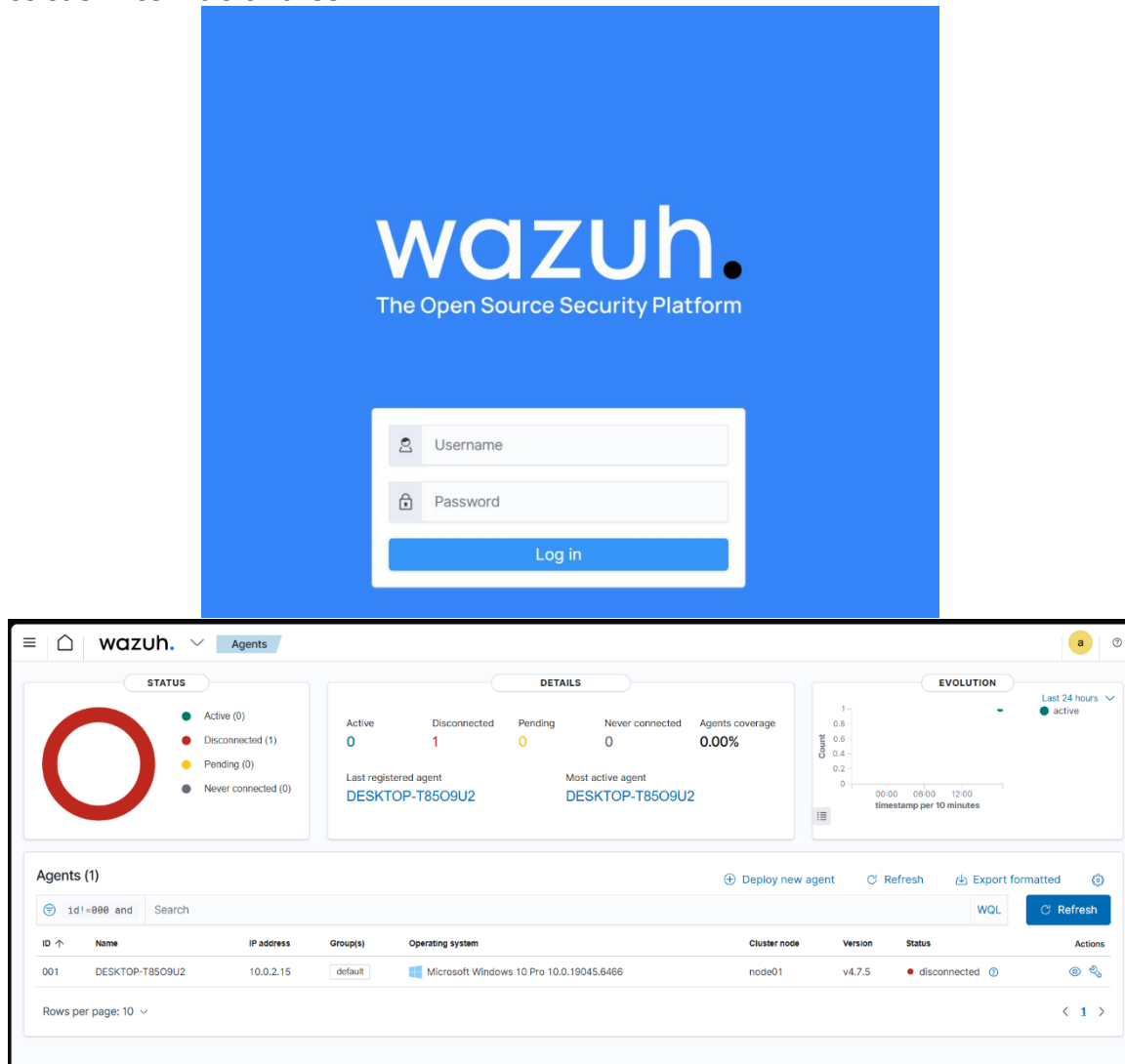
Como complemento a estas acciones, destacamos la importancia de la **gestión de dependencias seguras**, considerando que el uso de librerías desactualizadas representa uno de los principales vectores de ataque en aplicaciones modernas. En este sentido, recomendamos la implementación de herramientas de análisis de composición de software (SCA) y monitoreo de vulnerabilidades (CVE).

Paralelamente, llevamos a cabo la **implementación de un SOC operativo basado en Wazuh**, desplegado sobre un servidor dedicado, permitiendo la centralización de eventos de seguridad provenientes de los diferentes activos tecnológicos. Esta solución habilita capacidades de recolección, normalización y correlación de eventos en tiempo real, facilitando la identificación de comportamientos anómalos y posibles indicadores de compromiso.

El sistema fue integrado con **Suricata**, fortaleciendo la detección a nivel de red mediante el análisis del tráfico y la identificación de patrones asociados a amenazas conocidas y emergentes. Esta integración permite una visión más completa del entorno, combinando eventos de red con eventos del sistema. Asimismo, se configuró un esquema de **alertamiento automático por correo electrónico**, garantizando la notificación oportuna de eventos críticos al equipo de ciberseguridad, lo cual permite reducir los tiempos de respuesta ante incidentes.

Como parte del despliegue, implementamos **agentes en los dispositivos monitoreados**, los cuales permiten recolectar información detallada sobre la actividad del sistema, ejecución de procesos, cambios en configuraciones y comportamiento de usuarios. Esto proporciona trazabilidad completa sobre los activos tecnológicos y facilita la detección de actividades sospechosas. configuramos el SOC con **actualizaciones automáticas diarias**, asegurando la incorporación constante de nuevas reglas, firmas y capacidades de detección, manteniendo el sistema alineado con el panorama actual de amenazas.

En conjunto, estas acciones consolidan un entorno de seguridad robusto, basado en prevención, detección y respuesta, alineado con las mejores prácticas internacionales.



7. Conclusión

La ejecución de la Fase 4 representa un avance significativo en el fortalecimiento de la ciberseguridad de la Superintendencia de Transporte, al integrar controles de hardening con capacidades de monitoreo continuo mediante un SOC operativo.



Agencia Nacional Digital



Entre las principales ventajas de lo implementado se destacan:

- Reducción significativa de la superficie de ataque mediante configuraciones seguras.
- Mitigación de vulnerabilidades críticas en aplicaciones e infraestructura.
- Visibilidad centralizada de eventos de seguridad en tiempo real.
- Capacidad de detección temprana de amenazas e incidentes.
- Mejora en los tiempos de respuesta ante eventos de ciberseguridad.
- Fortalecimiento del control sobre los activos tecnológicos institucionales.

No obstante, la ciberseguridad no debe entenderse como un proceso estático, sino como un **proceso continuo de mejora**. En este sentido, recomendamos que la Superintendencia de Transporte mantenga un enfoque evolutivo, incorporando auditorías periódicas, ejercicios de simulación (Red Team / Blue Team), fortalecimiento del SOC y actualización constante de controles de seguridad.

La consolidación de una cultura de ciberseguridad, junto con la mejora continua de los mecanismos técnicos y operativos, permitirá a la entidad enfrentar de manera efectiva un entorno de amenazas cada vez más dinámico y sofisticado.