



**Agencia
Nacional Digital**



SOC_Operativo_Wazuh

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	3
2. Objetivo General	4
3. Objetivos Específicos	4
4. Desarrollo	4
5. Marco Teórico.....	7
6. Marco Legal.....	8
7. Conclusión	9

1. Introducción

El presente documento tiene como propósito describir la implementación de un Centro de Operaciones de Seguridad (SOC) operativo, basado en la plataforma Wazuh, desplegado sobre un servidor dedicado para el monitoreo continuo y centralizado de eventos de ciberseguridad.



Agencia Nacional Digital



Esta solución permite fortalecer las capacidades de detección temprana de amenazas, análisis de eventos y respuesta ante incidentes, proporcionando visibilidad integral sobre el comportamiento de los activos tecnológicos. De esta manera, se contribuye al fortalecimiento de la postura de seguridad institucional de la Superintendencia de Transporte, alineándose con las buenas prácticas en gestión de riesgos y protección de la información.

2. Objetivo General

Implementar un SOC operativo basado en Wazuh que permita la detección, monitoreo, correlación y respuesta ante eventos de ciberseguridad en tiempo real, fortaleciendo la capacidad de prevención y gestión de incidentes dentro de la infraestructura tecnológica institucional.

3. Objetivos Específicos

- Implementar Wazuh como plataforma SIEM centralizada para la recolección, análisis y correlación de eventos de seguridad.
- Integrar Suricata como mecanismo de detección de intrusiones a nivel de red, ampliando la visibilidad sobre el tráfico y posibles amenazas.
- Configurar esquemas de alertamiento automático mediante correo electrónico para la notificación oportuna de eventos críticos.
- Establecer mecanismos de monitoreo continuo sobre la actividad de los dispositivos, incluyendo ejecución de programas, cambios en el sistema y comportamiento de los usuarios.
- Garantizar la actualización periódica de firmas, reglas y capacidades de detección, manteniendo el sistema alineado con el panorama actual de ciberamenazas.

4. Desarrollo

Se realizó la implementación del sistema SIEM Wazuh en un servidor dedicado, proporcionando una plataforma centralizada para la gestión, correlación y análisis de eventos de seguridad provenientes de los diferentes activos tecnológicos. El acceso al sistema se encuentra habilitado a través de la siguiente interfaz web:

URL:

<https://2.24.215.12:443>

Usuario:

admin

Contraseña: P8LtNj36m39wA6LqQXTVkgVvHAU.uMIe



Agencia
Nacional Digital



wazuh.
The Open Source Security Platform

Log in

La solución desplegada permite la recolección, normalización y correlación de eventos en tiempo real, facilitando la identificación de patrones anómalos, comportamientos sospechosos y posibles indicadores de compromiso (IoC). Wazuh actúa como un componente estratégico dentro del esquema de ciberseguridad, al integrar capacidades avanzadas de monitoreo continuo, detección de amenazas y generación de alertas basadas en reglas y firmas especializadas.

El sistema se encuentra integrado con Suricata, lo cual fortalece significativamente la capacidad de detección a nivel de red, permitiendo identificar tráfico malicioso, intentos de intrusión y comportamientos asociados a amenazas conocidas y emergentes. Esta integración amplía la visibilidad sobre el entorno tecnológico, proporcionando una capa adicional de análisis sobre el tráfico y los eventos generados.

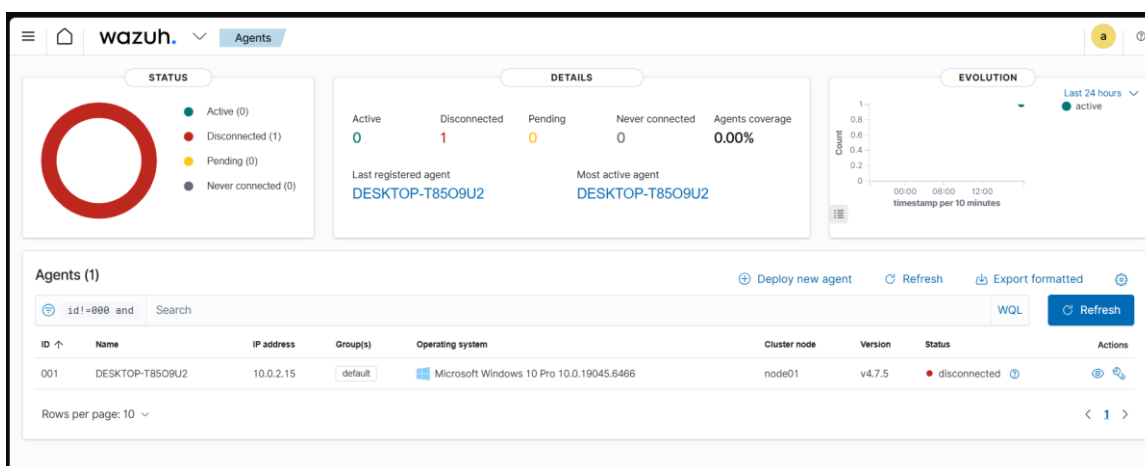
Adicionalmente, se ha configurado un esquema de notificación automática mediante correo electrónico hacia el equipo de ciberseguridad, específicamente a la dirección vialcodemail@gmail.com, garantizando una respuesta oportuna ante cualquier evento relevante. Este mecanismo permite una gestión proactiva de incidentes, reduciendo tiempos de detección y reacción ante posibles afectaciones a la seguridad de la información.

Como parte del despliegue operativo, se incluye un instalador en formato .bat que facilita la incorporación de agentes en los diferentes equipos monitoreados. Estos agentes permiten la recopilación detallada de eventos relacionados con la actividad del sistema, ejecución de programas, cambios en configuraciones, accesos y otros indicadores relevantes, consolidando una visión integral del comportamiento de los activos.

El entorno implementado contempla monitoreo continuo de la actividad de los dispositivos, incluyendo la trazabilidad del uso de aplicaciones y procesos ejecutados, lo cual permite detectar comportamientos atípicos o no autorizados dentro de los sistemas. Esta capacidad es clave para la prevención de incidentes internos, uso indebido de recursos o ejecución de software potencialmente riesgoso.

El sistema ha sido configurado para realizar actualizaciones automáticas de manera diaria a las 3:00 AM, asegurando la incorporación constante de nuevas firmas de detección, reglas de correlación y capacidades de análisis frente a amenazas emergentes. Esto garantiza que la plataforma se mantenga alineada con el panorama actual de ciberamenazas.

El SOC operativo permanecerá habilitado durante todo el tiempo de vigencia del contrato, proporcionando monitoreo permanente, análisis de eventos y respuesta ante incidentes. Se cuenta con personal especializado que realizará seguimiento continuo sobre los activos monitoreados, evaluando alertas, validando eventos y gestionando posibles incidentes de ciberseguridad, con el objetivo de proteger la integridad, disponibilidad y confidencialidad de la información institucional.



5. Marco Teórico

Un SOC (Security Operations Center) es una unidad centralizada encargada de monitorear, detectar, analizar y responder a incidentes de seguridad en sistemas informáticos. Su función principal es mantener la visibilidad continua sobre los activos tecnológicos de una organización, permitiendo la identificación temprana de amenazas y la gestión oportuna de incidentes de ciberseguridad.

Dentro de este contexto, los SIEM (Security Information and Event Management) como Wazuh desempeñan un papel fundamental, ya que permiten la recolección, normalización, correlación y análisis de grandes volúmenes de eventos provenientes de múltiples fuentes. Estas plataformas facilitan la detección de comportamientos anómalos, la generación de alertas en tiempo real y la trazabilidad de eventos de seguridad, lo que contribuye a una gestión más eficiente del riesgo.

Wazuh se compone de varios elementos clave que trabajan de manera integrada. Por un lado, el servidor central actúa como el núcleo de procesamiento, encargado de recibir, analizar y correlacionar los eventos. Por otro lado, los agentes de Wazuh son componentes instalados en los dispositivos finales (equipos de usuario, servidores, entre otros), cuya función es recolectar información del sistema, tales como registros de eventos, cambios en archivos, ejecución de procesos, actividad de usuarios y configuraciones del sistema operativo.

Estos agentes permiten una visibilidad detallada del comportamiento interno de cada activo, facilitando la detección de actividades sospechosas como ejecuciones no autorizadas, modificaciones críticas en el sistema o intentos de acceso indebido. Además, soportan mecanismos de integridad de archivos (FIM), monitoreo de logs, detección de rootkits y validación de configuraciones de seguridad, lo cual fortalece el control sobre los entornos monitoreados.

Adicionalmente, Wazuh permite la aplicación de reglas de correlación que analizan múltiples eventos en conjunto para identificar patrones complejos de ataque, lo cual resulta clave en escenarios donde las amenazas no son evidentes a partir de un único evento aislado.

Por su parte, Suricata es un sistema de detección y prevención de intrusiones (IDS/IPS) que analiza el tráfico de red en tiempo real, identificando patrones asociados a amenazas conocidas, anomalías en protocolos y comportamientos maliciosos. Su integración con el SIEM permite enriquecer el análisis,



Agencia Nacional Digital



combinando eventos de red con eventos del sistema, logrando así una visibilidad más completa del entorno.

La integración de estas herramientas permite una visión integral de la seguridad, facilitando la gestión proactiva de riesgos, el fortalecimiento de los controles de seguridad y la mejora continua en la capacidad de detección y respuesta ante incidentes.

6. Marco Legal

El presente proyecto se fundamenta en un conjunto de normativas, estándares y lineamientos nacionales e internacionales que orientan la gestión de la seguridad de la información, la protección de datos y la implementación de controles de ciberseguridad en entidades públicas.

En primer lugar, se toma como referencia la **ISO/IEC 27001:2022**, estándar internacional que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este marco proporciona un enfoque estructurado basado en la gestión del riesgo, permitiendo la protección de la confidencialidad, integridad y disponibilidad de la información mediante controles organizacionales, técnicos y operativos.

A nivel normativo nacional, se destaca la **Ley 1581 de 2012**, la cual regula la protección de datos personales en Colombia, estableciendo principios, derechos y obligaciones para el tratamiento adecuado de la información, especialmente aquella de carácter sensible. Su aplicación resulta fundamental en entornos donde se procesan datos de ciudadanos y usuarios.

Asimismo, la **Ley 1273 de 2009** introduce el marco legal relacionado con los delitos informáticos, tipificando conductas que atentan contra la seguridad de los sistemas y la información, lo cual refuerza la necesidad de implementar mecanismos de monitoreo, detección y respuesta ante incidentes de ciberseguridad.

El **Decreto 1078 de 2015**, como Decreto Único Reglamentario del Sector TIC, establece lineamientos para la gestión de tecnologías de la información en entidades públicas, promoviendo la adopción de buenas prácticas en seguridad digital y la protección de los activos de información.

De igual forma, la **Política de Gobierno Digital en Colombia**, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), define directrices para el uso estratégico de las TIC, incluyendo componentes de seguridad digital, gestión del riesgo y fortalecimiento de capacidades institucionales en ciberseguridad.



Agencia Nacional Digital



En complemento, el **Modelo de Seguridad y Privacidad de la Información (MSPI)** proporciona una guía estructurada para la implementación de controles de seguridad en entidades públicas, alineando la gestión de riesgos con estándares internacionales y promoviendo la mejora continua de la postura de seguridad.

En conjunto, estos marcos normativos y técnicos garantizan que la implementación del SOC operativo y la solución SIEM se desarrollen bajo principios de legalidad, cumplimiento y buenas prácticas, fortaleciendo la protección de la información institucional y la capacidad de respuesta frente a amenazas cibernéticas.

7. Conclusión

La implementación del SOC operativo basado en Wazuh constituye un avance estratégico en el fortalecimiento de las capacidades de ciberseguridad de la Superintendencia de Transporte, al permitir una gestión centralizada, continua y proactiva de los eventos de seguridad sobre los activos tecnológicos de la entidad.

La integración con Suricata, junto con el monitoreo permanente, la correlación de eventos en tiempo real, la generación automatizada de alertas y la actualización constante de firmas de detección, consolida un entorno robusto de vigilancia y análisis, orientado a la identificación temprana de amenazas y la mitigación oportuna de riesgos.

Este enfoque integral no solo mejora la capacidad de detección, sino que también optimiza los tiempos de respuesta ante incidentes, reduciendo el impacto potencial sobre la operación institucional y garantizando mayores niveles de protección sobre la información crítica.

Adicionalmente, el acompañamiento por parte de profesionales especializados asegura una supervisión continua, análisis contextual de las alertas generadas y una adecuada gestión de incidentes, permitiendo la toma de decisiones informadas y el fortalecimiento progresivo de la postura de seguridad.

En este sentido, el SOC operativo se consolida como un componente fundamental para la continuidad del negocio, la protección de los activos de información y el cumplimiento de los lineamientos normativos en materia de seguridad digital, contribuyendo de manera directa a la resiliencia tecnológica de la entidad frente a un entorno de amenazas cada vez más dinámico y sofisticado.



Agencia Nacional Digital

