UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERIA

CARRERA DE TELECOMUNICACIONES

Implementación de una plataforma de seguridad open source mediante Wazuh para el monitoreo y gestión de incidentes de seguridad de la información en la infraestructura de la Dirección de Tecnología de Información y Comunicación de la Universidad Nacional de Chimborazo

Trabajo de Titulación para optar al título de:

Ingeniera en Telecomunicaciones

AUTOR:

Guailla Shulca, Lourdes Gabriela

TUTOR:

Mgs. Santillán Valdiviezo, Luis Gonzalo

Riobamba, Ecuador. 2026

DECLARATORIA DE AUTORÍA

Yo, **Lourdes Gabriela Guailla Shulca**, con cédula de identidad **060595504-6**, autora del trabajo de titulación titulado: **Implementación de una plataforma de seguridad open source mediante Wazuh para el monitoreo y gestión de incidentes de seguridad de la información en la infraestructura de la Dirección de Tecnología de Información y Comunicación de la Universidad Nacional de Chimborazo,** certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 27 de enero de 2026.

Lourdes Gabriela Guailla Shulca

C.I:060595504-6

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe**, Mgs. Luis Gonzalo Santillán Valdiviezo** catedrático adscrito a la Facultad de **Ingeniería,** por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de titulación **titulado: Implementación de una plataforma de seguridad open source mediante Wazuh para el monitoreo y gestión de incidentes de seguridad de la información en la infraestructura de la Dirección de Tecnología de Información y Comunicación de la Universidad Nacional de Chimborazo**, bajo la autoría de **Lourdes Gabriela Guailla Shulca**; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los **30 días** del mes de **enero** de **2026**

Firmado electrónicamente por:
LUIS GONZALO
SANTILLAN
VALDIVIEZO
Validar únicamente con FirmaEC

Mgs. Luis Gonzalo Santillán Valdiviezo

C.I: 060322535-0

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de titulación **Implementación de una plataforma de seguridad open source mediante Wazuh para el monitoreo y gestión de incidentes de seguridad de la información en la infraestructura de la Dirección de Tecnología de Información y Comunicación de la Universidad Nacional de Chimborazo**, por **Lourdes Gabriela Guailla Shulca,** con cédula de identidad número **060595504-6**, bajo la tutoría de **Mgs. Luis Gonzalo Santillán Valdiviezo**; certificamos que recomendamos la **APROBACIÓN** de este con fines de titulación. Previamente se ha evaluado el trabajo de titulación escuchada y la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba **10 de abril de 2026.**

Luis Patricio Tello, PhD.
PRESIDENTE DEL TRIBUNAL DE GRADO

Dr. Klever Torres
MIEMBRO DEL TRIBUNAL DE GRADO

José Luis Jinez, Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO

C E R T I F I C A C I Ó N

Que, **GUAILLA SHULCA LOURDES GABRIELA** con CC: **060595504-6**, estudiante de la Carrera **TELECOMUNICACIONES**, Facultad de **INGENIERÍA;** ha trabajado bajo mi tutoría el trabajo de investigación titulado **"IMPLEMENTACIÓN DE UNA PLATAFORMA DE SEGURIDAD OPEN SOURCE MEDIANTE WAZUH PARA EL MONITOREO Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA DE LA DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO"**, cumple con el **2% de similitud y 7 % de Inteligencia Artificial,** de acuerdo con el reporte del sistema Anti plagio **COMPILATIO,** porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, **20** de **febrero** de **2026**

LUIS GONZALO
SANTILLAN
VALDIVIESO

Mgs. Luis Santillán
TUTOR(A)

DEDICATORIA

A los seres que la vida me dio como un instante para hacerme fuerte y que hoy no pudieron estar en esta etapa conmigo, han sido fuente de inspiración para luchar día a día hasta conseguir este logro, esto es por ustedes y para ustedes, mis angelitos en el cielo.

A mis padres Salvador y María que han estado conmigo en todo momento apoyándome y han sido base sólida para cumplir mis sueños, gracias por impulsarme día a día a ser un mejor ser humano, por los días y noches que han luchado incansablemente para que yo llegue a culminar esta etapa porque este logro también es suyo.

A mis hermanos Alex, Adriana, Roberto y María José por estar para mí siempre, en los momentos difíciles su cariño y presencia han sido de gran importancia, gracias por apoyarme en cada etapa de mi vida, por todos los momentos vividos que han hecho que mi vida sea feliz.

A mis sobrinas Andrea y Brianna que llegaron alegrarme y hacerme disfrutar aún más de la vida, con su amor e inocencia han llenado mi corazón de alegría incluso en los momentos difíciles solo con una sonrisa lograron calmarme, gracias mis pequeñas por vivir esta etapa conmigo.

Con amor,
Gaby

AGRADECIMIENTO

Agradezco a mi familia por estar presente durante mi proceso de formación por sus palabras de aliento que han sido de vital importancia para que yo llegue a vivir este momento.

A la Universidad Nacional de Chimborazo por permitir formarme académicamente y ser parte de esta hermosa institución.

A mis docentes que han hecho que mi formación estudiantil sea valiosa, por su paciencia y sobre todo por no solo formarnos académicamente sino enseñarnos a ser mejores personas. En especial quiero agradecer al tutor de mi proyecto el Mgs. Luis Santillán por la predisposición y ayuda brindada durante todo este proceso.

A mis amigos que han estado presente y han vivido conmigo el paso por la Universidad, su compañía ha hecho que este camino no se sienta pesado, por los buenos y malos momentos compartidos, en realidad gracias por todo. (A.A.K)

A mi mejor amiga Andrea S, por siempre estar conmigo en los momentos más difíciles de mi vida apoyándome, cuidándome, gracias por tantos años de amistad y por alegrarte de cada uno de mis logros como si fueran tuyos.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La creciente incidencia de ataques informáticos en instituciones de educación superior ha puesto en evidencia la necesidad de fortalecer los mecanismos de seguridad de la información. En este contexto, la presente investigación tuvo como objetivo implementar una plataforma de seguridad open source Wazuh para el monitoreo y la gestión de incidentes de seguridad de la información en la infraestructura tecnológica de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad Nacional de Chimborazo.

El estudio se desarrolló bajo un enfoque cuantitativo, experimental y comparativo, mediante la ejecución de ataques informáticos controlados de fuerza bruta y denegación de servicio (DDoS) en un entorno seguro, con el fin de evaluar la capacidad de detección y el tiempo de respuesta de la plataforma implementada. Los datos obtenidos fueron procesados mediante técnicas de estadística descriptiva e inferencial, permitiendo analizar los tiempos de detección y comparar el desempeño del sistema frente a ambos tipos de ataque.

Los resultados evidenciaron que la plataforma Wazuh presenta una alta efectividad en la detección de ataques, logrando identificar en un alto porcentaje los eventos ejecutados, además de proporcionar tiempos de detección adecuados para un entorno institucional. Asimismo, el análisis estadístico permitió determinar diferencias significativas en los tiempos de detección según el tipo de ataque, siendo los ataques de fuerza bruta detectados en menor tiempo que los ataques de denegación de servicio (DDoS).

Palabras clave: Wazuh, detección, ataques, DDoS, Fuerza bruta

ABSTRACT

The growing incidence of cyberattacks in higher education institutions has highlighted the need to strengthen information security mechanisms. In this context, this research aimed to implement the open-source security platform Wazuh to monitor and manage information security incidents across the Directorate of Information and Communication Technologies (DTIC) at the National University of Chimborazo. The study was conducted using a quantitative, experimental, and comparative approach by executing controlled brute-force and denial-of-service (DDoS) attacks in a secure environment to evaluate the detection capability and response time of the implemented platform. The data obtained were processed using descriptive and inferential statistical techniques, enabling the analysis of detection times and the comparison of the system's performance against both types of attacks. The results showed that the Wazuh platform is highly effective in attack detection, successfully identifying a high percentage of the executed events, while also providing detection times suitable for an institutional environment. Likewise, the statistical analysis revealed significant differences in detection times depending on the type of attack, with brute force attacks being detected in less time than denial-of-service (DDoS) attacks.

Keywords: Wazuh, detection, attacks, DDoS, Brute force.

Reviewed by:
Mgs. Hugo Romero
ENGLISH PROFESSOR
C.C. 0603156258

CAPÍTULO I. INTRODUCCIÓN

En un entorno digital cada vez más avanzado, la seguridad informática se ha convertido en un pilar crítico dentro de todos los sectores. En un estudio reciente se evidencia que el aumento de ataques cibernéticos mayormente está relacionado con el phishing, y Ecuador se encuentra como uno de los países más afectados lo que demanda un avance en la seguridad digital, es por lo que se ha expuesto la necesidad de adoptar nuevas estrategias que permitan identificar y mitigar riesgos [1].

El sistema de educación superior no está exento de presentar desafíos en la protección de sus activos digitales, dado que almacena información de carácter sensible[2]. En muchas universidades del mundo y del país aún existe la ausencia de sistemas de monitoreo de seguridad provocando que no exista la detección temprana de brechas y la toma de decisiones efectivas, ocasionando graves consecuencias como, el robo de información confidencial, exposición a virus y malware e interrupción de servicios[3].

Es así como las herramientas de código abierto han emergido como una solución viable para mejorar la seguridad dentro de las instituciones del Ecuador, estas herramientas son llamativas en instituciones que cuentan con un presupuesto reducido siendo una alternativa económica y eficiente en la detección de intrusos y gestión de tráfico[1]. Es por esto por lo que, el objetivo principal de este proyecto de investigación es fortalecer la seguridad de la información en la Dirección de Tecnologías de la información y Comunicación (DTIC) de la Universidad Nacional de Chimborazo mediante la implementación de una plataforma de seguridad open source basada en Wazuh, la cual será la encargada del monitoreo y gestión para garantizar la seguridad de sus activos, con esta plataforma se busca tener un análisis constante de los sucesos que pongan en riesgo la información y dar respuesta oportuna.

Además, se procederá a la evaluación de la efectividad de la plataforma realizando pruebas a través de ataques controlados que evidencien que la plataforma está trabajando de manera correcta. Es crucial para el sector educativo contar con un Sistema de monitoreo y gestión de vulnerabilidades que enfrente los desafíos en el tratamiento de la información siendo un paso importante para establecer una base sólida dentro de la seguridad informática de las instituciones.

1.1. Planteamiento del Problema

El sector educativo, en particular, enfrenta desafíos en la protección de sus activos digitales, debido a que las instituciones cuentan con sistemas obsoletos y antiguos para el tratamiento de amenazas[4]. Las universidades en su mayoría priorizan la mejora de sus instalaciones por encima de otros factores como la ciberseguridad, es por lo que los ciberdelincuentes aprovechan de esas oportunidades para formular ataques que exploten las vulnerabilidades de la institución[4].

En 2021, los sectores de educación superior enfrentaron un aumento del 75% en ciberataques con un promedio de 1605 ataques a organizaciones solamente en una semana. En un informe del FBI en 2022 se indicó que se encontraron credenciales de inicio de sesión de sistemas informáticos de colegios y universidades a la venta en una página web[5]. En 2023, la Universidad de Michigan enfrentó un problema de ciberseguridad por lo que tuvo que suspender los sistemas y servicio de tecnologías de la información (TI), algunas de las ciberamenazas que presentaron fue inyecciones SQL, phishing y ataques de ransomware[4]. En Ecuador según EcuCERT en 2023, mediante un informe documentó 70.608 direcciones IP comprometidas y 201.627 sucesos relacionados a ciberataques, esto indica que las universidades necesitan de forma inmediata un fortalecimiento en sus defensas cibernéticas siendo un paso crucial para la gestión eficiente de datos y mejorar la ciberseguridad en el país[1].

En la actualidad la Dirección de Tecnologías de la información y Comunicación (DTIC) de la UNACH cuenta con un servicio contratado por su proveedor CEDIA de un Centro de Respuestas a Incidentes Informáticos (CSIRT),ellos son responsables de prevenir, identificar y responder los incidentes de seguridad informática[6], sin embargo, la DTIC no cuenta con una plataforma propia que permita el monitoreo y la gestión de incidentes, por lo tanto, no se puede actuar de manera rápida en el tratamiento y protección de la información que se encuentra en peligro[7].

Este estudio propone evaluar la eficacia de una plataforma open source Wazuh como mecanismo de detección y respuesta ante amenazas informáticas dentro de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad Nacional de Chimborazo. En este contexto, se plantea la siguiente pregunta de investigación: ¿Puede la

implementación de una plataforma de seguridad basada en Wazuh mejorar el monitoreo y la gestión de incidentes de seguridad de la información en la infraestructura tecnológica de la DTIC? Para dar respuesta a esta interrogante, se formula la hipótesis de que la implementación de Wazuh en la infraestructura tecnológica en la DTIC de la UNACH mejorará significativamente la detección de vulnerabilidades y la capacidad de respuesta ante incidentes de seguridad informática.

1.2. Objetivos

1.2.1. General

- Implementar una plataforma de monitoreo y gestión de incidentes basada en Wazuh para fortalecer la seguridad de la información en la infraestructura tecnológica de la Dirección de Tecnologías de la Información y Comunicación de la UNACH.

1.2.2. Específicos

- Analizar las vulnerabilidades y necesidades de monitoreo de incidentes de seguridad en la infraestructura tecnológica de la DTIC de la Universidad Nacional de Chimborazo, mediante la aplicación de herramientas de diagnóstico de seguridad (como escáneres de vulnerabilidades, revisión de logs y entrevistas técnicas), con base en estándares internacionales, para identificar brechas y requerimientos prioritarios que orienten la implementación de Wazuh.

- Implementar la plataforma Wazuh configurada para la detección, análisis y respuesta ante eventos de seguridad de la información.

- Evaluar la efectividad de la plataforma mediante pruebas de operación, generación de alertas y respuesta ante incidentes.

CAPÍTULO II. MARCO TEÓRICO

2.1. Estado del arte

En [8] se presenta la implementación de un Sistema de Gestión de Eventos e Información de Seguridad (SIEM) basado en Wazuh, enfocada en su instalación y configuración inicial bajo una arquitectura "todo en uno". El estudio detalla la definición de parámetros básicos de operación, la habilitación de módulos de seguridad relevantes y la gestión del almacenamiento de logs mediante políticas de retención, evidenciando la capacidad de Wazuh para centralizar y administrar eventos de seguridad. Asimismo, se establece un entorno de desarrollo y pruebas con servidores virtuales, en el que se implementan el Wazuh Manager y los agentes encargados de la recolección y análisis de registros, utilizando reglas orientadas principalmente a la detección de servicios y cambios en la infraestructura. Adicionalmente, el trabajo demuestra la capacidad de integración de Wazuh con diversas herramientas de seguridad, como firewalls, Azure Entra ID y sistemas EDR, validando su interoperabilidad en entornos controlados. Como aporte principal, este estudio confirma la viabilidad técnica y operativa de Wazuh como plataforma SIEM de código abierto; sin embargo, su alcance se limita a una validación funcional, sin evaluar métricas cuantitativas de desempeño como el tiempo de detección o la efectividad de la respuesta ante ataques específicos.

En[9] propone la implementación de hacking ético para mejorar la detección y evaluación de vulnerabilidades de la seguridad de la información en una infraestructura minera de Lima-Perú, este proyecto tuvo como objetivo realizar un informe sobre las vulnerabilidades que presenta el sistema este proceso se llevó a cabo con un Ethical Hacker, el profesional a través de distintas fases pudo ir exponiendo vulnerabilidades que afecten a la seguridad de la infraestructura, dentro de las herramientas de escaneo que utilizó en cada fase esta Kali Linux, Nessus, Nmap, Metasploit Framework . Esto ha permitido conocer la exposición que tiene la información que almacena la empresa frente a las amenazas, en el documento se detalla cada una de las vulnerabilidades encontradas y por consecuencia se emite la solución para cada problema. Se ha manifestado que como tal no se deja ningún sistema implementado de forma tangible, en su lugar plantea sugerencias que permitan la mitigación de las vulnerabilidades identificadas y con ello evitar futuros ataques. En las recomendaciones indican que es prioritario que la empresa cuente con un sistema

automatizado para la identificación y tratamiento de los niveles de riesgo, además de cumplir con el reglamento regulatorio de las normas de seguridad nacional.

En [10] se propone la implementación de plataformas SIEM para la defensa activa ante intrusiones en redes, comparando específicamente Wazuh y Arista con el fin de evaluar su efectividad en la monitorización de ataques. El estudio utiliza el simulador GNS3 para diseñar topologías de red independientes que incluyen un servidor, una máquina atacante y un usuario legítimo, estableciendo un entorno controlado para la ejecución de pruebas. Los ataques se generan mediante la herramienta Gophish, permitiendo evaluar la capacidad de los SIEM para detectar y generar alertas en tiempo real frente a ataques de phishing. Como aporte relevante, el trabajo evidencia la capacidad de estas plataformas para identificar eventos de seguridad y proporcionar información detallada sobre los incidentes, así como una comparación funcional de sus principales características. No obstante, el alcance del estudio se limita a un único vector de ataque, lo que restringe la generalización de sus resultados y deja abierta la necesidad de evaluar el desempeño de los SIEM frente a otros tipos de amenazas. En este sentido, el trabajo constituye un antecedente comparativo importante, aunque su enfoque experimental controlado y su limitada diversidad de ataques difieren del enfoque más amplio y aplicado de la presente investigación.

En el trabajo se plantea la implementación de un centro de operaciones de seguridad y redes (NSOC) usando herramientas open source para la infraestructura industrial de la empresa eléctrica Quito, como punto de partida se realiza un análisis de características de diferentes herramientas para establecer un diseño que conste de herramientas de gestión de redes de datos, análisis de vulnerabilidades y registro de eventos, esta solución tecnológica se instalará en el software Oracle VM VirtualBox. Dentro de la solución tecnológica se instala a Zabbix como herramienta para el monitoreo de la red de datos, OpenVas como herramienta de gestión de vulnerabilidades y LogAnalyzer&Report como herramienta para analizar y visualizar datos de registro. Luego de haber integrado a las herramientas con los equipos terminales se procede a la configuración de alertas tempranas que serán enviadas a través de correo electrónico. Finalmente, para comprobar el funcionamiento de cada una de las herramientas instaladas se procede a realizar plas pruebasutilizando diferentes protocolos, así como pruebas sobre la generación de alertas y generación de reportes, mediante la implementación se concluyó que es importante contar con herramientas para la gestión de

red de datos, pero, al ser una solución recién implementada falto realizar más pruebas ya que en la mayoría de pruebas solo fueron de funcionamiento y no con diferente tipos de ataques [11].

En [12] se realizó un estudio comparativo de Sistemas de Detección de Intrusiones (IDS) de software Libre como: Suricata, Snort y Zeek para conocer sus funciones, rendimiento y eficiencia, con el objetivo de implementar una de esas herramientas y eludir intrusiones maliciosas que pongan en riesgo la seguridad de la información de los laboratorios de Ingeniería de la Universidad Nacional de Chimborazo. Dentro de las vulnerabilidades de nivel medio se halló denegación de servicio, intercepción o modificación del tráfico, versión antigua del software NTP, entre otras. Luego del análisis y de acuerdo con las necesidades encontradas se seleccionó como IDS a Suricata, y mediante pruebas realizadas se pudo conocer la eficacia del sistema en la detección de intrusiones, su capacidad de respuesta ante amenazas y estabilidad operativa. Finalmente, se menciona que los resultados obtenidos en la investigación sirvan de cimientos para futuras investigaciones que permitan fortalecer la red de seguridad de la Universidad.

En [13] se lleva a cabo la implementación de un T-pot en el servidor de la Facultad de Informática y Electrónica de la Escuela Politécnica de Chimborazo con el objetivo de analizar ataques internos y externos a la infraestructura de datos de la institución. A través del honeypost se recolecta información sobre protocolos y puertos que están siendo atacados, con dicha información se realiza un registro sobre los ataques que está presentando la red institucional. Además, se procedió a clonar la página de la ESPOCH para evidenciar de una forma más realista a los posibles atacantes a la red institucional, este proceso se realizó utilizando la plataforma de Kali Linux y el programa Httrack con la intención de formar un señuelo con los servicios web de la institución. Finalmente, luego de varias semanas de funcionamiento del sistema, en los honeypost se recolecto información importante sobre la interacciones y ataques que ha recibido la página de la ESPOCH, por lo tanto, se concluye que a través de esta herramienta es posible evidenciar la actividad permanente que tienen los hackers y permite la prevención contra los ataques de seguridad informática.

En[14] se plantea un análisis de tráfico malicioso mediante técnicas maching learning, utilizando OPNids en la red del edificio de la Facultad de Informática y Electrónica (FIE),

se realiza en la primera etapa el análisis de la infraestructura del edificio para recolectar información y establecer un diseño para la implementación de la plataforma OPNids. Luego se instala la plataforma OPNids en el servidor HP del edificio de la FIE, pero, para potenciar su funcionamiento se combina con un Sistema de detección de intrusos (IDS)como Suricata que además es un software de código abierto. Mediante un entorno controlado se configura y empieza a analizar el tráfico a la vez se realiza ataques como denegación de servicio (DoS), Usuario a Root(U2R), Remoto a local (R2L) y escaneo (Scan o Probin) para comprobar que la plataforma implementada detecta este tipo de ataques y genera alertas. Por lo tanto, se concluye que la plataforma OPNids combinada con otra herramienta como Suricata ayuda en la automatización de procesos de control en la seguridad de la red.

A diferencia de los trabajos anteriormente analizados, que evidencian que existen investigaciones que abordan la implementación de plataformas open source como los SIEM, también demuestran la funcionalidad básica de Wazuh, pero, con la presente investigación se amplia y profundiza dicho enfoque al integrar otras herramientas de seguridad como un IDS para fortalecer la seguridad informática, ya que ninguno aborda la detección de eventos, respuesta activa en entornos reales como en una institución educativa pública. Con esta investigación se contribuye a cerrar esta brecha como solución efectiva para la gestión de incidentes de seguridad.

2.2. Fundamentación Teórica

2.2.1. La Seguridad de la Información

Se define como procesos destinados a guardar la integridad de la información, proteger los sistemas de información del acceso, uso o divulgación no autorizada. Este concepto en definitiva indica que se deben proteger los datos y recursos de una infraestructura tecnológica de quienes buscan hacer mal uso de ellas[15]. De modo que, la seguridad de la información se enfoca tanto en proteger un archivador que contenga documentos de gran importancia, así como, proteger una base de datos pertenecientes a una empresa u organización[16].

2.2.2. Principios de la Seguridad de la Información

- **Confidencialidad**

Este principio tiene como finalidad mantener los datos y recursos de forma privada, es decir, asegurar el acceso a la información a través del cifrado de datos y solamente conceder el acceso a la misma a quienes lo necesiten[17].

- **Integridad**

Garantiza que los datos no hayan sufrido alteraciones por personas no autorizadas, a través de un seguimiento durante el almacenamiento, procesamiento y tránsito de la información con la finalidad de proteger los datos de los sistemas[18].

- **Disponibilidad**

Se refiere a que la información se encuentre disponible, segura y confiable en el momento en que las personas autorizadas lo requieran sin tener interrupciones de servicios[18].

2.2.3. Sistema de Gestión de Eventos e Información de Seguridad (SIEM)

Es una herramienta que ofrece capacidades predictivas y proactivas para identificar y mitigar amenazas cibernéticas antes de que materialicen su impacto. Su objetivo principal es fortalecer la postura de seguridad mediante la prevención de ataques[19].

Dada la necesidad de visualizar el estado de la red y tener a salvo la información estas herramientas se han convertido en una solución indispensable en los centros de operaciones de seguridad (SOC) que tiene las empresas[20].

Los SIEM tienen la capacidad de recolectar y analizar eventos de forma automatizada, además que facilitan la respuesta a incidentes. [21]. Es por eso que cuenta con una gran variedad de opciones, pero, lo esencial es encontrar una herramienta que vaya conforme a

las necesidades del usuario, por ello se presenta a continuación algunas herramientas gratuitas:

- **QRADAR:** plataforma de gestión de seguridad, obteniendo información simultanea y soporte de políticas[19].

- **WAZUH:** Es una plataforma de código abierto, implementado para la detección de amenazas basados en el host[20].

- **ALIEN VAULT:** es una herramienta que permite gestionar la seguridad informática como los eventos causados en un determinado tiempo[19].

- **SYMANTEC:** conocida como principalmente por su software antivirus para la seguridad informática[19].

2.2.4. WAZUH

Wazuh es una plataforma open-source y gratuita que es utilizada para la detección, prevención y respuesta ante amenazas. Es empleado por diferentes organizaciones en el mundo, desde pequeñas hasta grandes empresas por su capacidad de proteger los activos digitales y mejorar la ciberseguridad a través de sus servicios[22]. Su funcionalidad más importante es su compatibilidad con diferentes sistemas operativos, además de su capacidad de integrarse con otras herramientas de seguridad para potenciar su capacidad analítica[21].

2.2.4.1 Componentes Wazuh

Para la solución Wazuh se conforma de dos partes, el agente wazuh que se implementa en los puntos finales monitorizados y en 3 componentes centrales que son:

1. **Indexador de wazuh**: Es un motor de búsqueda y análisis de texto completo enormemente escalable. Este componente central ordena y almacena en el servidor wazuh las alarmas que se genera[23].

2. **Servidor de wazuh**: Analiza los datos que recibe de los agentes y los procesa mediante decodificadores para buscar indicadores de vulnerabilidad, además este componente se utiliza para administrar los agentes, configurándolos y actualizándolos cuando sea necesario de forma remota[23].

3. **Panel de control de wazuh**: el panel de control es la interfaz web para visualización y análisis de datos, también permite gestionar la configuración de wazuh y supervisar su estado[22].

2.2.4.2 Funciones de Wazuh

Por otra parte, es importante contar con recursos que permiten prevenir ataques es por lo que Wazuh ofrece las siguientes funciones:

1. **Detección de intrusos**: los sistemas monitorizados son analizados en busca de malware, anomalías e inconsistencias de respuesta al llamado del sistema, además tiene la capacidad de detectar archivos ocultos y procesos encubiertos[23].

2. **Análisis de datos de registro**: cuando no existe un agente wazuh implementado el servidor puede actuar analizando los logs con reglas predefinidas es decir detección de ataques, anomalías y posterior las almacena para generar alertas o reportes de cumplimiento[23].

3. **Detección de vulnerabilidades**: La evaluación automatizada de vulnerabilidades le ayuda a encontrar los puntos débiles en sus activos críticos y tomar medidas correctivas antes de que los atacantes los exploten para sabotear su negocio o robar datos confidenciales[20].

4. **Respuesta ante incidentes:** proporciona respuestas activas que pueden ser utilizadas si se cumple con ciertos criterios, como bloquear el acceso a un sistema desde la fuente de la amenaza[24].

5. **Seguridad en la nube**: facilita la monitorización de la infraestructura en la nube a nivel de API mediante módulos de integración que tiene la capacidad de enviar datos

de forma segura desde proveedores de nube reconocidos como Azure, AWS, Amazon[24].

2.2.5. Suricata

Es un software de código abierto y alto rendimiento, capaz de alertar a los administradores sobre amenazas, gracias a que maneja un conjunto de reglas que le permiten trabajar como un guardián de red, analiza el tráfico en tiempo real e identifica patrones maliciosos[25]. Es robusto, rápido, tiene la capacidad de detectar intrusos en tiempo real complementando con el monitoreo de seguridad de red siendo un punto importante para la generación de alertas y la detección de anomalías en tiempos cortos[12].

2.2.6. Hping3

Es una herramienta de red capaz de enviar paquetes ICMP/UDP/TCP personalizados y mostrar respuestas de destino como ping con las respuestas ICMP. Gestiona la fragmentación, el cuerpo y tamaño arbitrarios de los paquetes, y permite transferir archivos bajo los protocolos compatibles, además es utilizado por usuarios que realizan hacking ético con la finalidad de probar la seguridad de la red[26].

2.2.7. Hydra

Es un cracker de inicio de sesión paralelizado compatible con numerosos protocolos de ataque. Es muy rápido y flexible, y es fácil añadir nuevos módulos. Esta herramienta permite a los investigadores y consultores de seguridad mostrar lo fácil que sería obtener acceso no autorizado a un sistema de forma remota[27].

2.2.8. Vulnerabilidad

Se refiere a un fallo que puede poner en peligro a los sistemas informáticos[28].

2.2.9. Amenaza

Un evento que solo puede existir si hay vulnerabilidades previas[29].

2.2.10. Logs

Los logs o también conocidos como registro de eventos son archivos que almacenan información sobre el comportamiento de equipos o sistemas informáticos, son necesarios para auditorias y cumplimiento de normativas, detección de fallos ya que recolectan datos que permiten identificar patrones que indiquen la ocurrencia de un evento[30].

2.2.11. Ataque de fuerza bruta

Es un tipo de ataque suele ser uno de los más frecuentes en entornos educativos debido a que prueba distintas combinaciones de contraseñas con la finalidad de conseguir accesos no autorizados[8].

2.2.12. Ataque de denegación de servicio (DoS)

Es un tipo de ciberataque que tiene como propósito inundar con solicitudes hasta que el tráfico normal quede abrumado incapaz de que los usuarios puedan acceder a la información sea de máquinas o servidores, es importante saber que este tipo de ataque se puede realizar utilizando una sola máquina, no solo satura recursos, sino que compromete el principio de disponibilidad y representa una amenaza en infraestructuras expuestas a redes pública. [31].

2.2.13. Respuesta activa

Es un método de protección de los activos, que automatiza acciones de respuesta ante incidentes de seguridad con la finalidad de mitigar amenazas[32].Además es una estrategia que permite mejorar la eficiencia en el tiempo de mitigación de amenazas[21].

CAPÍTULO III. METODOLOGÍA

3.1. Tipo de Investigación

La presente investigación se orienta hacia un enfoque aplicado y experimental, con el objetivo de implementar la plataforma Wazuh como una solución tangible a un requerimiento real en la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la UNACH. En el contexto de una implementación en un entorno real, se utiliza una metodología experimental que facilita la observación y evaluación del funcionamiento del sistema en respuesta a eventos de seguridad simulados en un entorno controlado.

3.2. Diseño de investigación

El presente estudio adopta un diseño cuantitativo de tipo experimental, orientado a evaluar el desempeño de una plataforma de seguridad informática mediante la recopilación de eventos, alertas emitidas por parte de la plataforma y el tiempo de detección de eventos.

3.3. Fuentes de recopilación de información

En el presente proyecto de investigación se utilizaron las siguientes técnicas:

- **Análisis documental:** revisión de estándares de seguridad de la información, metodologías SIEM y documentación técnica de Wazuh.

- **Diagnóstico técnico:** mediante herramientas de escaneo de vulnerabilidades, análisis de logs y configuración actual de los sistemas DTIC.

- **Simulación controlada de eventos:** generación de ataques controlados/simulados (DoS, acceso no autorizado, intentos de inicio de sesión, entre otros.) para evaluar la capacidad de detección de la plataforma.

- **Registro de datos:** a través de los reportes generados automáticamente por Wazuh y los indicadores de gestión de seguridad.

3.4. Procedimiento

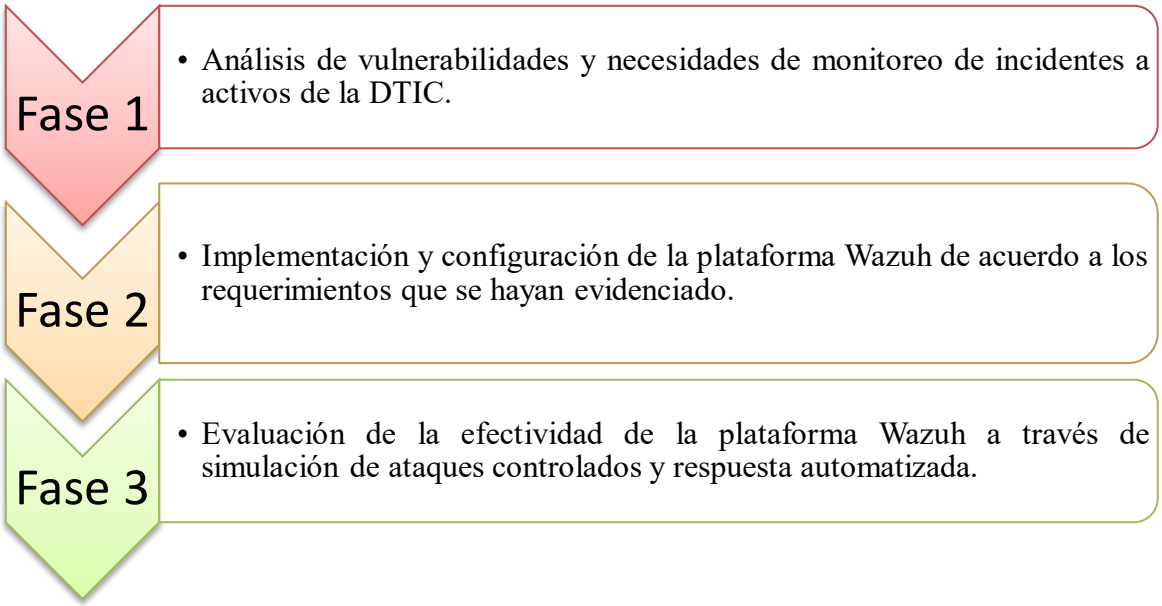


Figura 1. Diagrama de fases del proyecto

3.4.1. Análisis de vulnerabilidades y necesidades de monitoreo de incidentes a activos de la DTIC

En esta fase, se llevó a cabo una investigación bibliográfica sobre el funcionamiento de Wazuh como plataforma de detección y respuesta ante amenazas. Paralelamente, se realizó un escaneo en el cual se detectó vulnerabilidades en dispositivos finales y que en las siguientes tablas se detalla la información encontrada, esta información sirvió como punto de partida para el desarrollo del proyecto de investigación.

3.4.1.2. Estado actual de la DTIC

En el estado actual de las máquinas de la DTIC se encontró las siguientes vulnerabilidades.

- **Agente 001**

En la figura 2, detalla las vulnerabilidades detectadas en el agente 001, esta información se encuentra en la sección Detección de Vulnerabilidades del panel de control de la plataforma Wazuh. En la tabla 1, se describe los CVE de las vulnerabilidades más importantes, así como el tipo de gravedad.

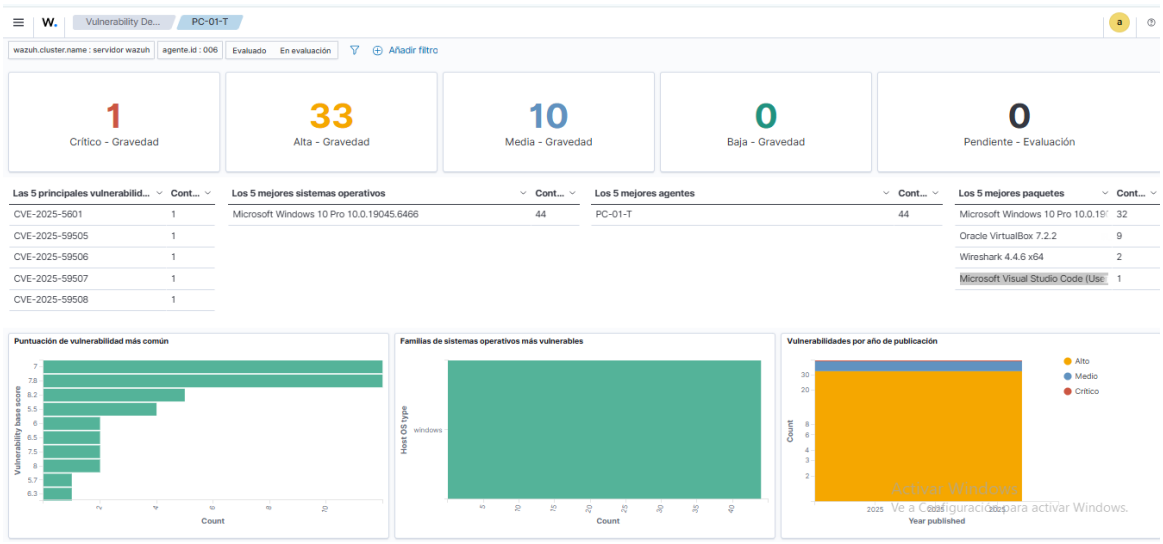


Figura 2. Vulnerabilidades Agente 001

Tabla 1. Vulnerabilidades Agente 001

Cantidad	Tipo de Gravedad	Vulnerabilidad	Descripción
1	**Crítico**	**CVE-2025-60724**	El desbordamiento de búfer basado en montón en el componente de gráficos de Microsoft permite que un atacante no autorizado ejecute código a través de una red.
		CVE-2025-5601	Los fallos en el manejo de columnas en Wireshark 4.4.0 a 4.4.6 y 4.2.0 a 4.2.12 permiten la denegación de servicio mediante inyección de paquetes o un archivo de captura manipulado.
			La doble liberación en la tarjeta inteligente de Windows permite

33	**Alta**	**CVE-2025-59505**	que un atacante autorizado eleve privilegios localmente.
		CVE-2025-59506	La ejecución concurrente utilizando un recurso compartido con sincronización incorrecta ('condición de carrera') en Windows DirectX permite que un atacante autorizado eleve privilegios localmente.
		CVE-2025-59507	
		CVE-2025-59508	
10	**Media**	**CVE-2025-59509**	La inserción de información confidencial en los datos enviados en Windows Speech permite que un atacante autorizado divulgue información localmente.
		CVE-2025-59510	La resolución de enlace incorrecta antes del acceso a un archivo ("seguimiento de enlace") en el Servicio de enrutamiento y acceso remoto de Windows (RRAS) permite que un atacante autorizado deniegue el servicio localmente.
		CVE-2025-59513	La lectura fuera de límites en el controlador del protocolo RFCOM de Bluetooth de Windows permite que un atacante autorizado divulgue información localmente.
		CVE-2025-60706	La lectura fuera de límites en Windows Hyper-V permite que un atacante autorizado divulgue información localmente**.**
		CVE-2025-60708	La desreferencia de puntero no confiable en el controlador Storvsp.sys permite que un atacante autorizado deniegue el servicio localmente.

La tabla 2, resume todas las vulnerabilidades encontradas en el agente 001, como se observa estas vulnerabilidades están relacionadas directamente a aplicaciones que se encuentran instaladas en la máquina monitoreada, pero, que ponen en riesgo la seguridad porque de acuerdo con la descripción de los CVE las vulnerabilidades pueden ser explotadas.

Tabla 2. Paquetes de Vulnerabilidades

CANTIDAD	PAQUETES
32	Microsoft Windows 10 Pro-10
9	Oracle VirtualBox 7.2.2
2	Wireshark 4.4.6 x64
1	Microsoft Visual Studio Code (User)
	Total :44

- **Agente 002**

En la figura 3, indica en panel de control de Wazuh con las vulnerabilidades detectadas en el agente 002. En la tabla 3, se describe los CVE de las vulnerabilidades más importantes, así como el tipo de gravedad y la cantidad.

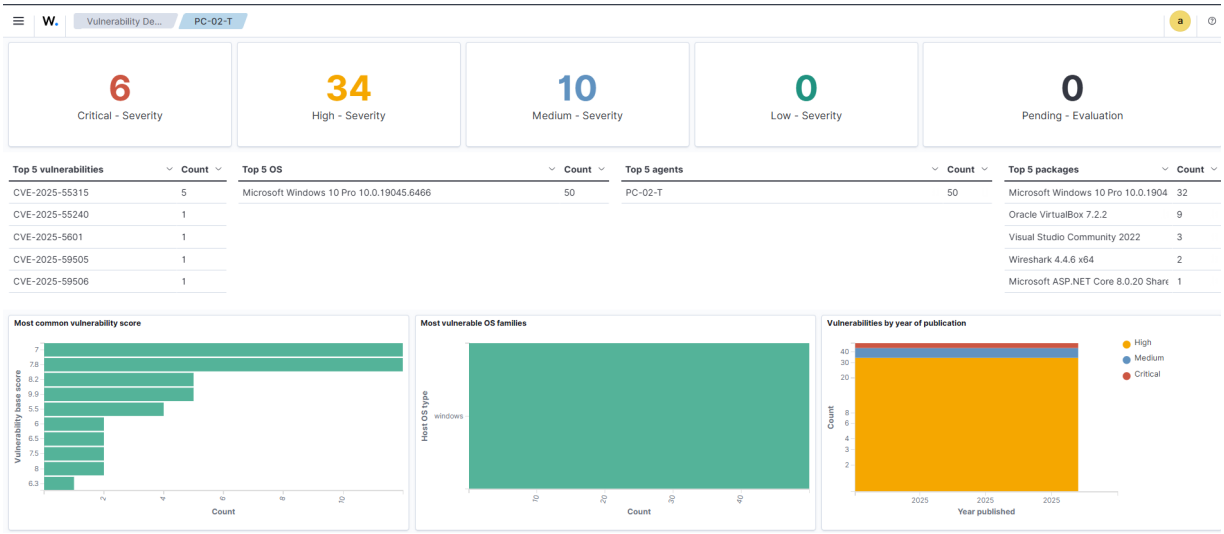


Figura 3. Vulnerabilidades Agente 002

Tabla 3. Vulnerabilidades Agente 002

Cantidad	Tipo de Gravedad	Vulnerabilidad	Descripción
6	**Crítico**	**CVE-2025-60724**	El desbordamiento de búfer basado en montón en el componente de gráficos de Microsoft permite que un atacante no autorizado ejecute código a través de una red.
		CVE-2025-62452	
34	**Alta**	**CVE-2025-62215**	La ejecución concurrente utilizando un recurso compartido con sincronización incorrecta ('condición de carrera') en el kernel de Windows permite que un atacante autorizado eleve privilegios localmente
		CVE-2025-60720	La sobrelectura del búfer en Windows TDX.sys permite que un atacante autorizado eleve privilegios localmente.
		CVE-2025-59506	La ejecución concurrente utilizando un recurso compartido con sincronización incorrecta ('condición de carrera') en Windows DirectX permite que un
		CVE-2025-59508	

			atacante autorizado eleve privilegios localmente
10	**Media**	**CVE-2025-59509**	La inserción de información confidencial en los datos enviados en Windows Speech permite que un atacante autorizado divulgue información localmente.
		CVE-2025-60723	La ejecución concurrente utilizando un recurso compartido con sincronización incorrecta ('condición de carrera') en Windows DirectX permite que un atacante autorizado deniegue el servicio a través de una red.
		CVE-2025-59513	La lectura fuera de límites en el controlador del protocolo RFCOM de Bluetooth de Windows permite que un atacante autorizado divulgue información localmente.
		CVE-2025-60706	La lectura fuera de límites en Windows Hyper-V permite que un atacante autorizado divulgue información localmente**.**
		CVE-2025-5601	El manejo de columnas falla en Wireshark 4.4.0 a 4.4.6 y 4.2.0 a 4.2.12, lo que permite la denegación de servicio mediante inyección de paquetes o un archivo de captura creado.

En la tabla 4, se detalla la cantidad de paquetes de las vulnerabilidades encontradas en el agente, esto refleja que las vulnerabilidades están relacionadas a aplicaciones que se encuentran instaladas en el agente monitorizado, tomando en cuenta la descripción de los CVE de la tabla 3, existe riesgo debido a que las vulnerabilidades por más indefensas pueden ser explotadas sumando un riesgo a la seguridad de la DTIC.

Tabla 4. Paquetes de vulnerabilidades Agente 002

CANTIDAD	PAQUETES
31	Microsoft Windows 10 Pro-10
9	Oracle VirtualBox 7.2.2
2	Wireshark 4.4.6 x64
3	Visual Studio Community 2022
5	Microsoft ASP.NET Core 8.0.20 Shared Framework(x64)
Total :50	

- **Agente 003**

En la figura 4, muestra las vulnerabilidades detectadas en el agente 003, esta información se encuentra en el panel de control de Wazuh. En la tabla 5, se describe los CVE de las vulnerabilidades más comunes, así como la cantidad de cada vulnerabilidad de acuerdo con el tipo de gravedad.

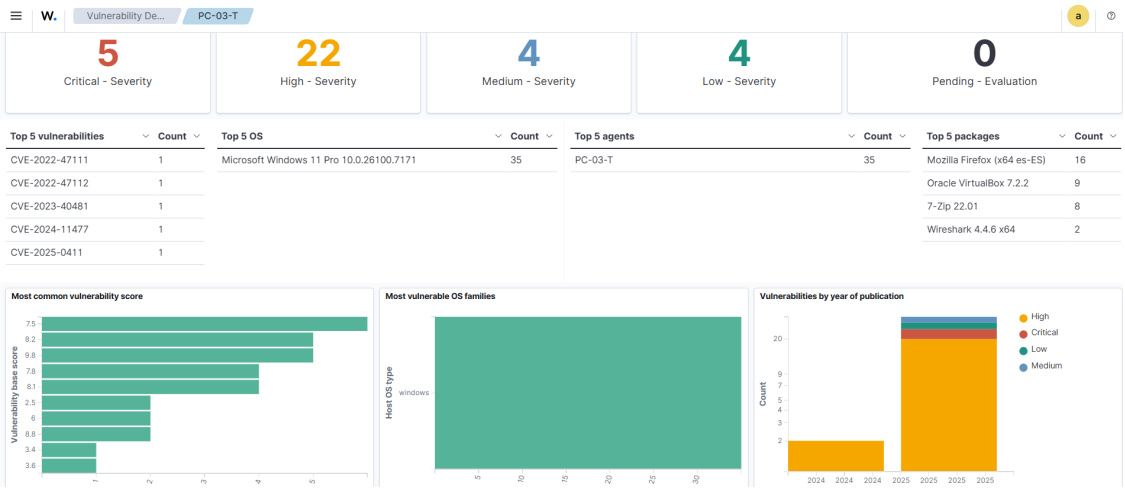


Figura 4. Vulnerabilidades Agente 003

Tabla 5. Vulnerabilidades Agente 003

Cantidad	Tipo de Gravedad	Vulnerabilidad	Descripción
5	**Crítico**	**CVE-2025-13023**	Escape de la zona protegida debido a condiciones de contorno incorrectas en el componente Gráficos: WebGPU. Esta vulnerabilidad afecta a Firefox (versión anterior a 145) y Thunderbird (versión anterior a 145).
		CVE-2025-13026	
		CVE-2025-13024	Error de compilación JIT en el motor de JavaScript: componente JIT. Esta vulnerabilidad afecta a Firefox (versión anterior a 145) y Thunderbird (versión anterior a 145).
22	**Alta**	**CVE-2025-13017**	Omisión de la política del mismo origen en el componente DOM: Notificaciones. Esta vulnerabilidad afecta a Firefox (versión anterior a 145), Firefox ESR (versión anterior a 140.5), Thunderbird (versión anterior a 145) y Thunderbird (versión anterior a 140.5).
		CVE-2025-13018	Omisión de mitigación en el componente DOM: Seguridad. Esta vulnerabilidad afecta a Firefox < 145, Firefox ESR < 140.5, Thunderbird < 145 y Thunderbird < 140.5.
		CVE-2025-13019	
		CVE-2025-13020	Uso posterior a la liberación en el componente de audio/vídeo de WebRTC. Esta vulnerabilidad afecta a Firefox (versión anterior a 145), Firefox ESR (versión anterior a 140.5), Thunderbird (versión anterior a 145) y Thunderbird (versión anterior a 140.5).
4	**Media**	**CVE-2025-0411**	Vulnerabilidad de evasión de la marca de la web en 7-Zip. Esta vulnerabilidad permite a atacantes remotos evadir el mecanismo de

			protección de la marca de la web en las instalaciones afectadas de 7-Zip. Para explotar esta vulnerabilidad, se requiere la interacción del usuario, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso.
		CVE-2025-13021	Condiciones de contorno incorrectas en el componente Gráficos: WebGPU. Esta vulnerabilidad afecta a Firefox (versión anterior a 145) y Thunderbird (versión anterior a 145).
		CVE-2025-13499	El fallo del disector de Kafka en Wireshark 4.6.0 y 4.4.0 a 4.4.10 permite la denegación de servicio
4	**Baja**	**CVE-2025-13015**	Problema de suplantación de identidad en Firefox. Esta vulnerabilidad afecta a Firefox < 145, Firefox ESR < 140.5, Firefox ESR < 115.30, Thunderbird < 145 y Thunderbird < 140.5.
		CVE-2022-47112	7-Zip 22.01 no informa de un error para ciertos archivos xz no válidos, relacionados con indicadores de flujo y bits reservados. Algunas versiones posteriores no se ven afectadas.

En la tabla 6, refleja un resumen de las vulnerabilidades encontradas dentro del agente, esta información es de suma importancia debido a que indica a que se relaciona la vulnerabilidad encontrada, y de acuerdo con los CVE de la tabla 5, existen vulnerabilidades que puedes ser explotadas y poner en riesgo la seguridad de la información.

Tabla 6. Paquetes de Vulnerabilidades

CANTIDAD	PAQUETES
16	Mozilla Firefox (x64 es-ES)
9	Oracle VirtualBox 7.2.2
8	7-Zip 22.01
2	Wireshark 4.4.6 x64
Total :35	

En la tabla 7, se puede observar la clasificación total de vulnerabilidades obtenidas de las máquinas de la DTIC. Como se muestra es una cantidad alta y de acuerdo con la descripción de los CVE (Vulnerabilidades y exposiciones comunes) existen vulnerabilidades que pueden ser explotadas por atacantes, y uno de los ataques que se podría llevar a cabo es la denegación de servicio.

Tabla 7. Vulnerabilidades totales de Agentes

Tipo de Gravedad	Cantidad
Crítica	12
Alta	89
Media	24
Baja	4
Total	129

3.4.2. Implementación y configuración de la plataforma Wazuh

La segunda fase correspondiente a la implementación y configuración de la plataforma Wazuh consistió en la instalación del servidor de Wazuh, así como la instalación del componente Agente de Wazuh en los dispositivos que fueron monitoreados, posteriormente se configuro la plataforma para la detección y respuesta automatizada ante ataques tomando como guía la fase 1, a continuación de detalla el proceso de instalación e implementación.

3.4.2.1 Instalación de Wazuh

Wazuh ofrece diferentes alternativas de instalación y para este proyecto se utilizó la máquina virtual que contiene la última versión de Wazuh que es la 4.14, para ello inicialmente se

descarga el archivo OVA (Open Virtual Appliance) que se encuentra en la documentación oficial de Wazuh[33].

Figura 5. Alternativas de instalación

Cabe recalcar que la máquina virtual es compatible con sistemas operativos host de 64 bits con arquitectura x86_64/AMD64[33]. Wazuh OVA viene configurada con las siguientes especificaciones, pero, si se desea se puede modificar de acuerdo con los endpoints que se vayan a monitorear:

- 4 CPU (núcleos)
- 8GB de RAM
- 50GB de almacenamiento

Una vez descargado, se importa el archivo OVA a VirtualBox u otro sistema de virtualización compatible y se modifica el controlador gráfico a VMSVGA puesto que, otros controladores podrían bloquear la ventana de la máquina virtual[33].

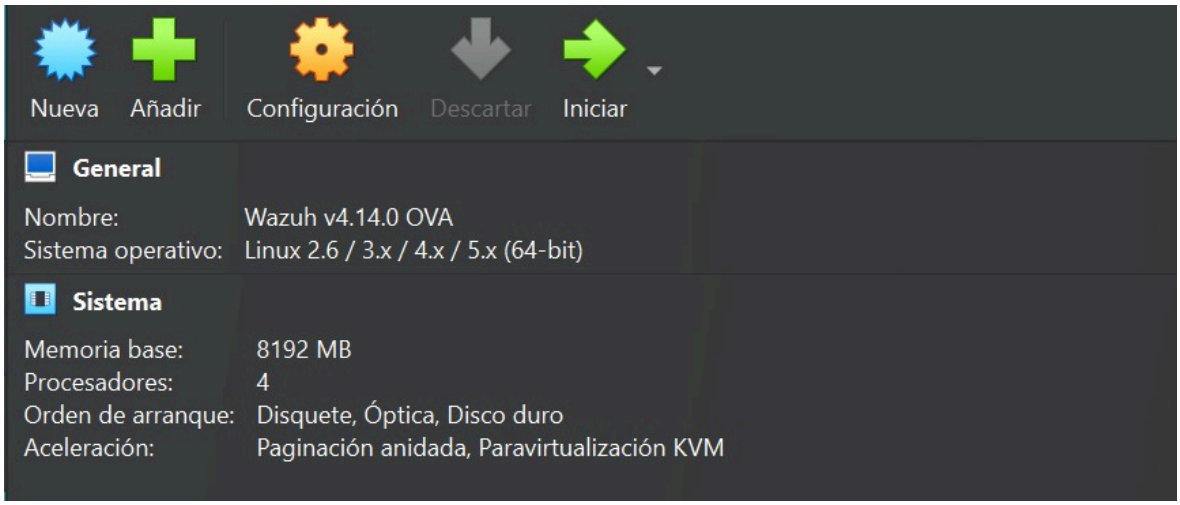


Figura 6. Requisitos de Hardware

Finalizada la configuración del hardware necesario para la importación de la máquina virtual de Wazuh, se procede a iniciar la máquina virtual donde se mostrará la siguiente pantalla que indica las credenciales de inicio de sesión.

Figura 7. Credenciales de inicio al servidor Wazuh

Una vez realizado el inicio de sesión identificamos la dirección IP de la máquina a través del comando **ip a**, que sirve para ingresar en un navegador web al panel de control de Wazuh con la dirección web **https://<dirección_IP>.** Wazuh en su documentación proporciona credenciales por defecto para ingresar al panel de control que son las siguientes:

- **user:** admin
- **password:** admin.

Figura 8. Plataforma Wazuh

Cuando se ingresa al panel de control por primera vez se observa de la siguiente manera:

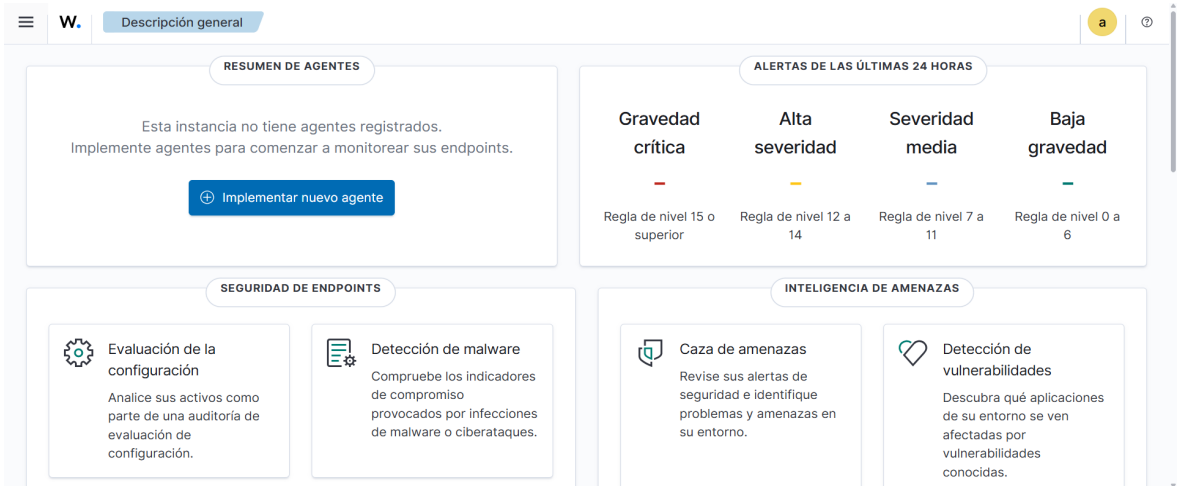


Figura 9. Panel de control de Wazuh

Para mayor seguridad de la plataforma fue necesario cambiar la contraseña del administrador ya que las credenciales que se indica son por defecto, entonces se realizó el siguiente proceso.

En el servidor de Wazuh en modo root se ingresa al siguiente directorio:

- /usr/share/wazuh-indexer/plugins/OpenSearch-security/tools/

Dentro del directorio se emite el siguiente comando y se indica para que usuario se requiere cambiar la contraseña.

- bash wazuh-passwords-tool.sh -u admin -p “Contraseña.”

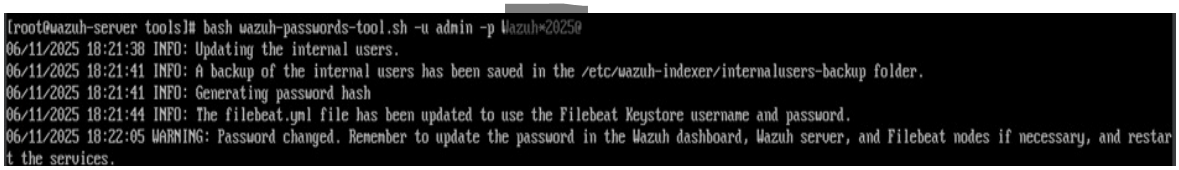


Figura 10. Cambio de contraseña del dashboard de Wazuh

En la figura 10, se observa que exitosamente la contraseña ha sido cambiada para el usuario administrador e indica que se reinicie los servicios.

3.4.2.2 Configuración de Wazuh

La máquina virtual de Wazuh ya cuenta con todos los componentes necesarios para funcionar, sin embargo, si se requiere realizar configuraciones personalizadas se puede hacer mediante sus archivos de configuración que se encuentran en las siguientes ubicaciones[33]:

- **Gerente de Wazuh**:/var/ossec/etc/ossec.conf
- **Indexador Wazuh**:/etc/wazuh-indexer/opensearch.yml
- **Filebeat-OSS**:/etc/filebeat/filebeat.yml

Dashboard de Wazuh:

- /etc/wazuh-dashboard/opensearch_dashboards.yml
- /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml

Es así como Wazuh se encuentra lista para funcionar, sin embargo, por defecto, Wazuh no escanea el propio servidor/manager. En este proyecto se procedió activarlo con la finalidad de monitorear al servidor e identificar también si existen amenazas y esta modificación se

realiza a través de su archivo internal_option.conf que se puede encontrar la siguiente ubicación:

- /var/ossec/etc/internal_options.conf

Utilizando el editor nano abrimos el archivo y buscamos la línea:

- vulnerability-detection. disable_scan_manager=1

Una vez identificada la línea cambiamos el valor de 1 a 0, con ello se activa el escaneo del manager.

- vulnerability-detection. disable_scan_manager=0

3.4.2.3 Configuración de Agentes Wazuh

Para el desarrollo de este proyecto se utilizó máquinas Windows, de acuerdo con la documentación se puede instalar en diferentes sistemas operativos y dispositivos. Los pasos por seguir para la configuración de los agentes son:

1. Al ingresar al panel de control de Wazuh, encontramos una pestaña de Puntos Finales o “Endpoints”, escogemos la opción implementar nuevo agente. A continuación, se escoge el sistema operativo, en este caso Windows.

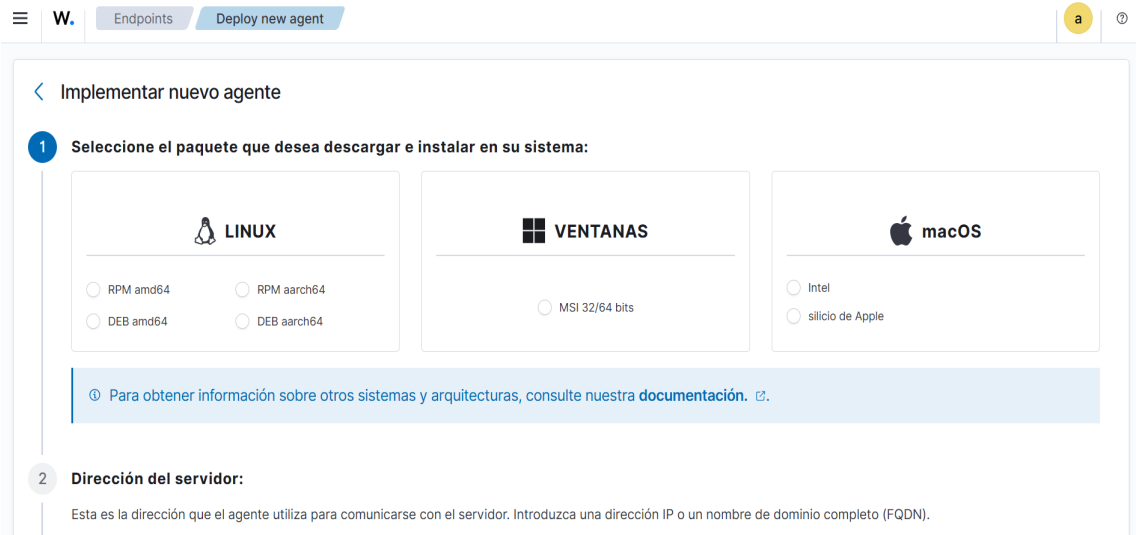


Figura 11. Implementación de agente Wazuh

2. Ingresamos la dirección IP del servidor, cabe destacar que esta dirección de preferencia debe ser un IP fija para luego no tener inconvenientes en la comunicación entre el agente y el servidor.

3. Se asigna un nombre único para cada agente con la finalidad de poder diferenciarlo dentro del dashboard.

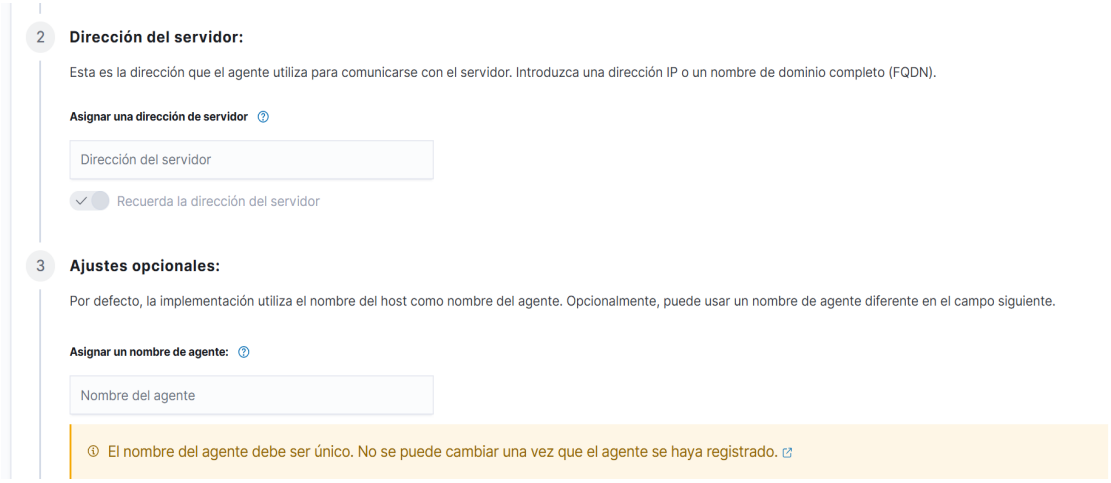


Figura 12. Configuración de parámetros de agente Wazuh

4. Una vez ingresado los datos del servidor y el nombre, se genera automáticamente un código que sirve para descargar e instalar el agente. Este código se debe ejecutar en la máquina Windows en modo administrador sea en Powershell 3.0 o una versión más actual.

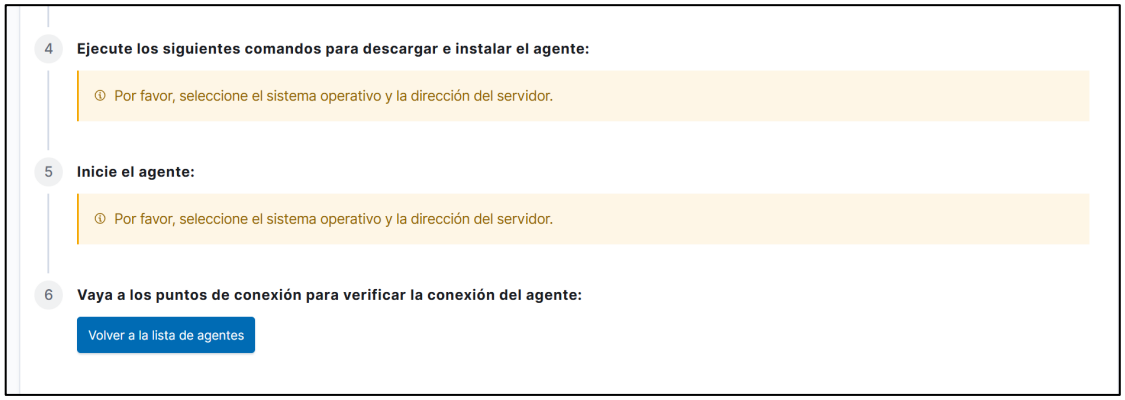


Figura 13. Configuración de parámetros de Agente Wazuh

5. Al finalizar la descarga del agente se debe iniciar el servicio con “**NET START WAZUH**”

6. Finalmente se podrá visualizar el agente en el panel de control de Wazuh.

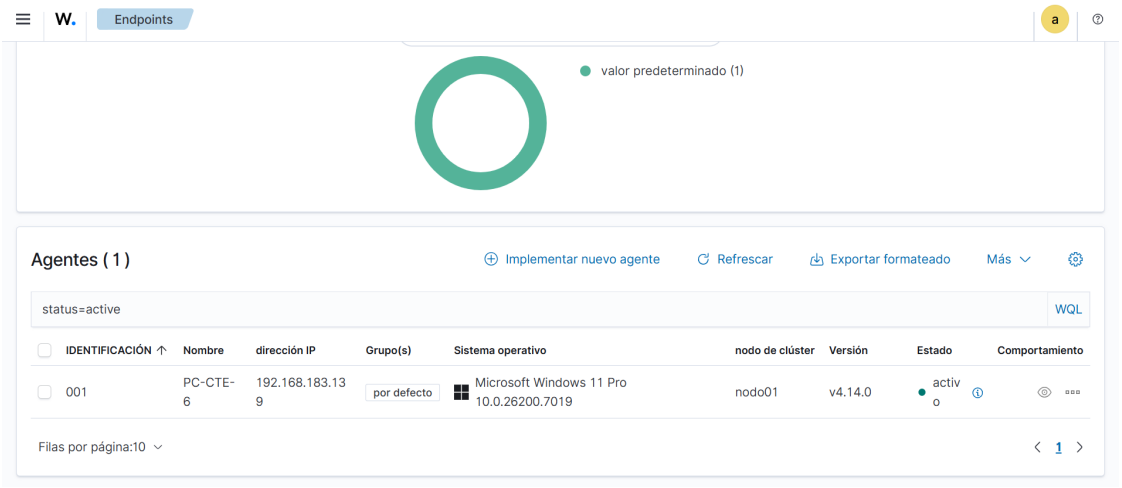


Figura 14. Agente instalado

3.4.2.4 Integración con Suricata

Para realizar la integración de Wazuh con Suricata se deben seguir los siguientes pasos en la máquina Windows es decir, agente de Wazuh:

1. Descargamos npcap que es una biblioteca que sirve como controlador de web para windows que permite capturar y analizar el trafico de red.
2. Descargamos suricata para windows x64bits
3. Instalamos la aplicación de npcap
4. Instalamos suricata

Concluida la instalación de ambos programas ingresamos en el disco C: archivos de programa y carpeta suricata. (C:\Program Files\Suricata\suricata.yml) para editar el archivo **suricata.yml** que contiene toda la información sobre suricata. Dentro del archivo en la seccion de Home_Net se edita la direccion IP que regularmente debe estar la red de confianza que son todas las direcciones que pertencen a esa red y por lo cual no genera eventos pero, como prueba se ha puesto como direccion IP de confianza solo la direccion IP de el agente

y si alguien envia tráfico desde otra direccion IP que no sea del agente eventualmente generará un evento en Wazuh.

```
3
4   # Suricata configuration file. In addition to the comments describing all
5   # options in this file, full documentation can be found at:
6   # https://docs.suricata.io/en/latest/configuration/suricata-yaml.html
7
8   # This configuration file generated by Suricata 7.0.0.
9   suricata-version: "7.0"
10
11  ##
12  ## Step 1: Inform Suricata about your network
13  ##
14
15  vars:
16    # more specific is better for alert accuracy and performance
17    address-groups:
18      HOME_NET: "[192.168.0.175]"
19      #HOME_NET: "[192.168.0.0/16]"
20      #HOME_NET: "[10.0.0.0/8]"
21      #HOME_NET: "[172.16.0.0/12]"
22      #HOME_NET: "any"
```

Figura 15. Configuración de IP en Suricata

En la sección **rule_files** se encuentran reglas que trae por defecto suricata pero, para este proyecto se descargó un paquete de reglas actualizado en la página https://rules.emergingthreats.net/open/. Entonces primero se debe comentar las reglas anteriores con la finalidad que no presente errores al incluir las nuevas reglas.

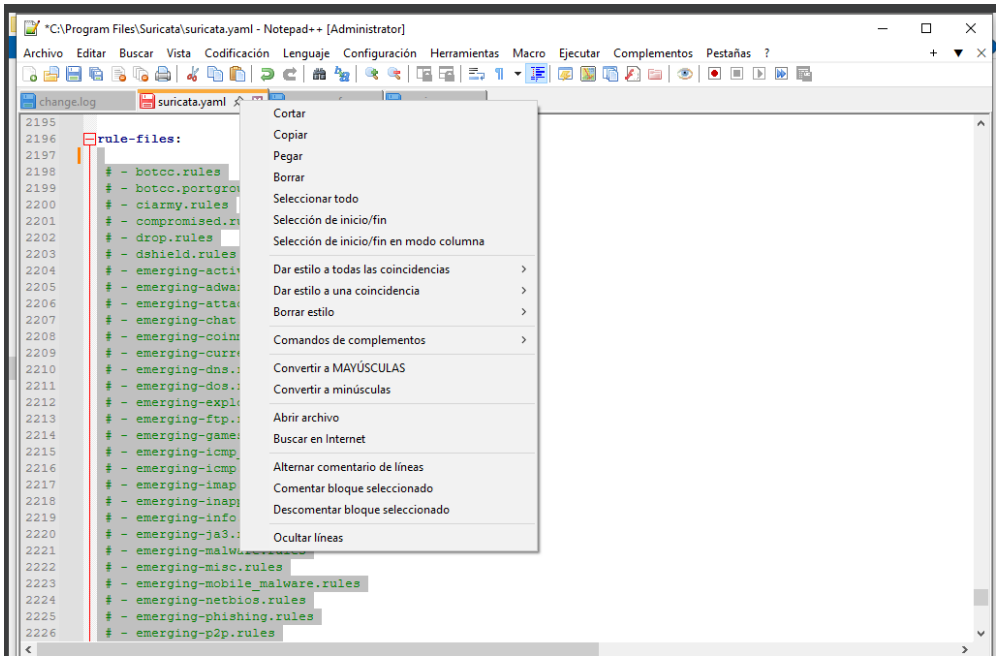


Figura 16. Reglas Suricata

En la carpeta de rules de suricata copiamos y pegamos el archivo de la nuevas reglas y posteriormente en la sección de rule-files incluimos la línea con el nombre del archivo del parquete de reglas.

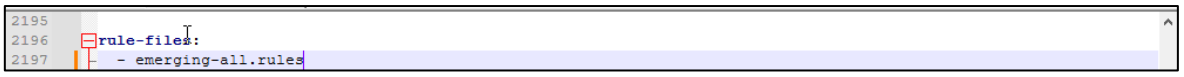


Figura 17. Reglas Suricata actualizadas

Guardamos el archivo de suricata.yml y abrimos el CMD con permisos de administrador y ejecutamos el siguiente comando: *"C:\Program Files\Suricata\suricata.exe" -c "C:\Program Files\Suricata\suricata.yaml" -i <IP_Agente>* para iniciar el servicio de suricata.

Una vez que se ejecuta el comando en la carpeta de log se crean cuatro archivos que demuestra que Suricata esta funcionando.

- Eve.json
- Fast.log
- Suricata
- Stat.log

Para verificar el funcionamiento de suricata se realiza una prueba básica que consiste en enviar un ping desde el SIEM hacia el agente wazuh para generar tráfico, este tráfico generado se puede evidenciar en el archivo **eve.json** donde se almacenan todos los eventos producidos en el agente.

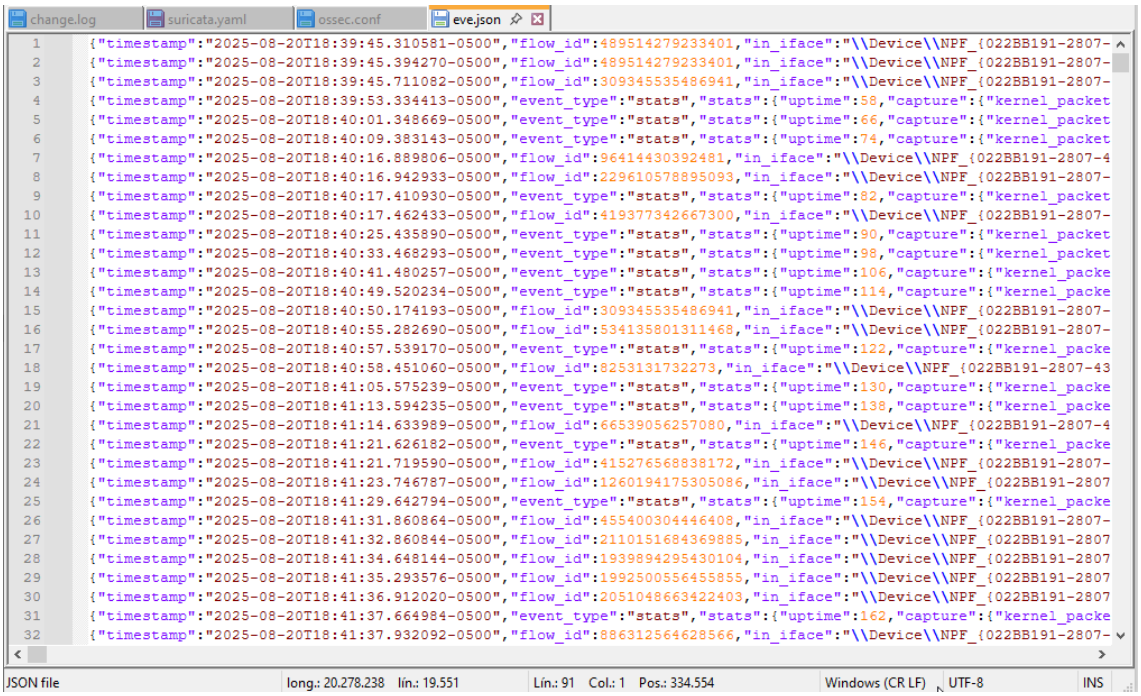


Figura 18. Archivo eve. json

En el agente wazuh modificamos el archivo **ossec.config** y añadimos la siguiente código, este código permite que la informacion del archivo **eve.json** se envie al wazuh-manager para que lo procese y muestre las alertas en el panel de control.

<ossec_config>

<localfile>

<log_format>json</log_format>

<location>C:\Program Files\Suricata\log\eve.json</location>

</localfile>

</ossec_config>

Guardamos los cambios y reiniciamos el servicio de Wazuh a traves del CMD. Para visualizar las alertas generamos de nuevo tráfico a través de un ping desde otra máquina o desde el servidor hacia el agente y por consiguiente en el panel de Wazuh se puede observar las alertas generadas por suricata.

3.4.2.5 Configuración de la respuesta activa

Para la configuración de la respuesta activa se edita el archivo ossec.config del manager, por defecto Wazuh ya tiene una preconfiguración, pero, en este proyecto se realizó algunos cambios siguiendo la documentación oficial[32].

- Utilizando un editor de texto abrimos el archivo ossec.config que se encuentra en la siguiente ruta /var/ossec/etc/ossec.config

- Dentro del archivo se puede encontrar los <command> que son scripts predeterminados. Wazuh cuenta con scripts por defecto, para este proyecto se utilizó un script de Windows que viene predeterminado o si se prefiere se puede crear scripts personalizados.

- Añadimos el parámetro de rules_id, tomando la ID de la regla que se generó al momento de realizar el ataque, para cuando aparezca esta regla se ejecute el script que se debe define en <command>.

- El parámetro de timeout se refiere al tiempo que se desea bloquear, esto puede definirse en segundos contemplando el tiempo que se va a bloquear al atacante o establecer un valor de 0 para que se bloquee permanentemente.

En la figura 19, muestra la configuración del active response como mitigación al ataque de fuerza bruta.

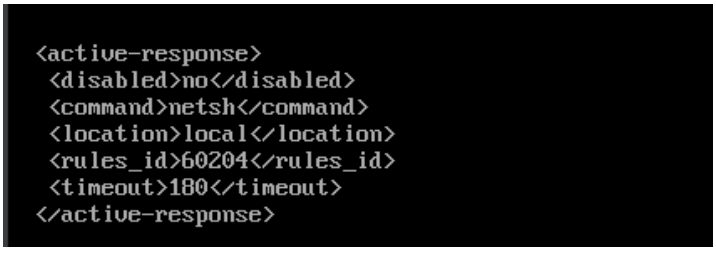


Figura 19. Configuración de respuesta activa

3.4.3 Evaluación de la efectividad de Wazuh

Esta fase consistió en ejecutar ataques controlados que sirvieron para recolectar datos. A continuación, se detalla el proceso para la evaluación mediante una simulación de ataques controlados para ello se establece un entorno de pruebas que se detalla en las tablas 1, 2 y 3.

3.4.3.1. Entorno de Pruebas

Para el entorno de pruebas los siguientes recursos, en la tabla 8, detalla los equipos que forman parte de la topología de red, esta información fue proporcionada por la DTIC.

Tabla 8. Equipos de Red

Equipos
Switch Core
Switch de distribución
Switch Juniper CX4100-24MP

En el ambiente de pruebas se utilizó computadoras de la sala de internet de la DTIC como agentes monitorizados, además utilizan la red cableada que se encuentran dentro de la siguiente VLAN.

Tabla 9. Direccionamiento

Número de VLAN	**NOMBRE**	**Direccionamiento IP**
VLAN 36	Vlan_CTE_Salas_de_Internet	172.30.36.0/24

- **Hardware y software del escenario de pruebas**

Utilizar una combinación entre entornos físicos y virtuales ayuda a la evaluación de la efectividad de la plataforma para ello se utilizó lo siguiente:

Tabla 10. Hardware para entorno de pruebas

Equipo	Especificaciones	Descripción
Laptop	HP /Intel Core i7 /20GB RAM/ 2.40GHZ	Computadora personal utilizada para el servidor de Wazuh
OptiPlex AIO 7420 65W	HP / Intel Core i7 / 16GB RAM	Máquinas de la DTIC utilizadas como agentes de Wazuh y una máquina utilizada como atacante con Kali Linux

En la tabla 11, se detalla los diferentes softwares utilizados para el desarrollo de la investigación.

Tabla 11. Software para entorno de pruebas

Software	**Descripción**
Wazuh	Plataforma de monitoreo y gestión de código abierto y gratuita.
Kali Linux	Distribución de Linux utilizada para ejecutar los ataques a las maquinas del escenario de pruebas.
Suricata	Sistema de detección de intrusos para visualizar el tráfico en tiempo real en las máquinas monitoreadas.

3.4.3.1. Ataques Realizados

Una vez establecido el entorno donde se llevó a cabo la simulación de ataques controlados se procedió a ejecutar ataques de fuerza bruta y denegación de servicio.

3.4.3.2.1 Ataque de Fuerza Bruta

El ataque de inicio de sesión se puede realizar a varios protocolos, pero, en este caso se decidió atacar al protocolo RDP (Protocolo de escritorio remoto) y para ello hay que identificar que el servicio este habilitado[34]. Para este proceso previamente se creó un archivo de texto con contraseñas aleatorias, luego con la herramienta hydra de Kali Linux a través del comando **hydra -l** "usuario" **-p** "archivo.txt" **rdp**//IP_VICTIMA como se muestra en la figura 20, se efectúa el ataque a la máquina víctima utilizando el archivo de contraseñas e indicando el nombre de usuario al que se intentará ingresar.

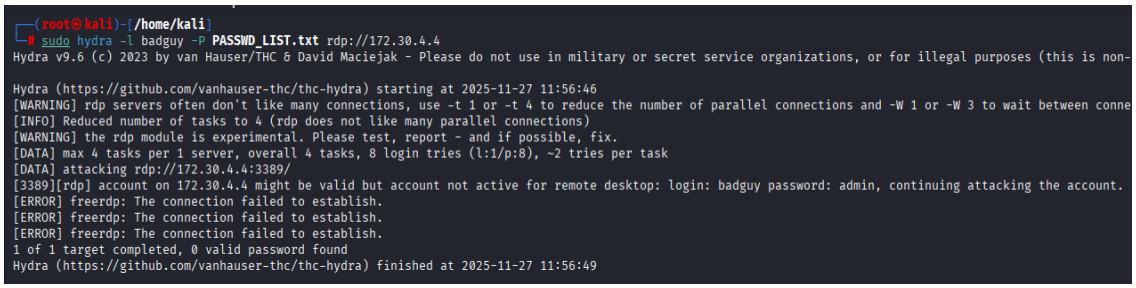


Figura 20. Ataque de fuerza bruta

3.4.3.2.2 Ataque de denegación de servicio (DoS)

Para llevar a cabo este ataque fue necesario primero realizar una integración con un IDS como suricata que permite capturar el tráfico en tiempo real. Es importante contemplar que para cada agente se efectuó una cantidad de ataques utilizando la herramienta hping3 de Kali Linux a través del siguiente comando **hping3 –flood –rand-source "ÏP_VICTIMA"** que se puede visualizar en la figura 21.

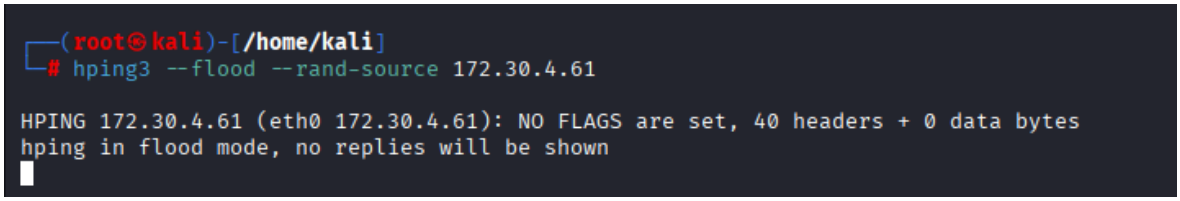


Figura 21. Ataque DDoS

Luego de la simulación de ataques de fuerza bruta y denegación de servicio (DDoS), Wazuh a través de su dashboard muestra la generación de alertas y posteriormente la ejecución de la respuesta activa como método de defensa contra ataques, como se describe a continuación.

- **Generación de alerta**

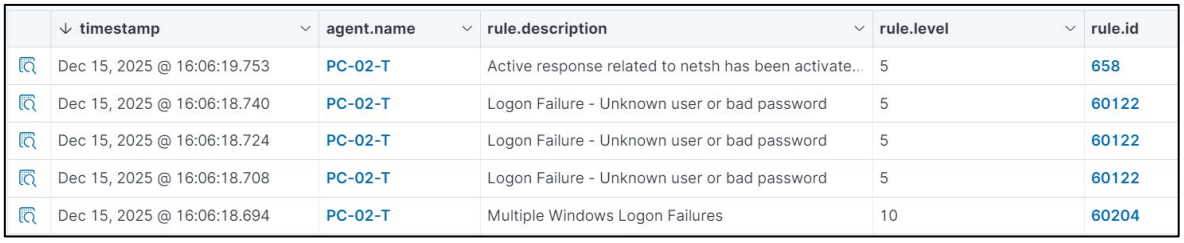
Wazuh a través del panel de control muestra la información que llega de sus agentes como la generación de alertas que indica que ataque o anomalía está ocurriendo dentro de los agentes monitorizados. En la figura 22, se puede visualizar como la plataforma registra un ataque, indicando la fecha, hora y el nombre del agente que está generando la alerta.

27 de noviembre de 2025 a las 11:54:08.144	PC-02-T	Múltiples fallos de inicio de sesión de Windows
27 de noviembre de 2025 a las 11:54:08.127	PC-02-T	Error de inicio de sesión: usuario desconocido o contraseña incorrecta

Figura 22. Generación de alerta

- **Respuesta activa**

En la figura 23 y 24 se observa como en el dashboard de Wazuh muestra un aviso que se puso en marcha la respuesta activa para cada uno de los ataques, evidenciando que se muestra primero la alerta del ataque y posteriormente se inicia el mecanismo de defensa previamente configurado.



↓ timestamp	agent.name	rule.description	rule.level	rule.id
Dec 15, 2025 @ 16:06:19.753	PC-02-T	Active response related to netsh has been activate..	5	658
Dec 15, 2025 @ 16:06:18.740	PC-02-T	Logon Failure - Unknown user or bad password	5	60122
Dec 15, 2025 @ 16:06:18.724	PC-02-T	Logon Failure - Unknown user or bad password	5	60122
Dec 15, 2025 @ 16:06:18.708	PC-02-T	Logon Failure - Unknown user or bad password	5	60122
Dec 15, 2025 @ 16:06:18.694	PC-02-T	Multiple Windows Logon Failures	10	60204

Figura 23. Respuesta activa

PRUEBA	16 de diciembre de 2025 a las 00:45:40.255	El agente Wazuh empezó.	3
PRUEBA	16 de diciembre de 2025 a las 00:44:27.690	Respuesta activa: restart-wazuh.exe - agregar	3

Figura 24. Respuesta activa en DDoS

3.5. Operacionalización de variables

Tabla 12. Operación de Variables

Variable	Tipo	Indicador	Técnica de medición	Instrumento
Tipo de ataque informático ejecutado	**Independiente**	Categoría del ataque ejecutado	Observación técnica y análisis de registros del sistema	Categoría del ataque ejecutado
Cantidad de ataques detectados	**Dependiente**	Número de eventos maliciosos identificados	Análisis de reportes del sistema	Reportes de alertas de Dashboard de Wazuh
Tiempo de detección de ataques	**Dependiente**	Tiempo transcurrido desde la ejecución del ataque hasta la generación de la alerta	Medición automática del tiempo a partir de marcas temporales (timestamps) registrados en los logs del sistema de seguridad	Registro (logs) y del sistema Wazuh y Suricata; consola de eventos del SIEM.

3.5.1. Población de estudio y tamaño de muestra

Población

La población de estudio está constituida por los eventos del ataque informático ejecutados de manera controlada dentro del entorno tecnológico definido para la investigación,

específicamente ataques de fuerza bruta y ataques de denegación de servicio (DDoS) registrados y analizados mediante la plataforma de seguridad implementada.

Muestra

La muestra se determinó mediante un muestreo no probabilístico por conveniencia técnica, considerando la naturaleza experimental del estudio, la repetibilidad de los eventos de ataque y las condiciones operativas del entorno de pruebas. El tamaño muestral se estableció con el propósito de garantizar estabilidad en las mediciones y permitir la aplicación de técnicas de análisis estadístico-acordes al diseño de la investigación.

3.6. Métodos de análisis y procesamiento

Para el análisis y procesamiento de datos se utilizó el software IBM SPSS Statistics que permitió el procesamiento de datos recolectados durante la implementación, con el software se realizó una estadística descriptiva que garantiza la fiabilidad y validez de los resultados obtenidos en la simulación de ataques de fuerza bruta y DDoS, además se realizó una prueba de normalidad para visualizar si los datos se distribuyen normalmente y posteriormente se realizó una comparación de medias con respecto al tiempo de detección de cada tipo de ataque efectuado con la finalidad de saber para qué tipo de ataque la plataforma detecta en un menor tiempo.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

En el presente capítulo se presentan y analizan los resultados obtenidos a partir de la ejecución controlada de ataques informáticos en el entorno experimental, con el objetivo de evaluar el desempeño del sistema de seguridad implementado en términos de tiempo de detección y número de alertas generadas.

Las pruebas se realizaron para ataques de fuerza bruta y ataques de denegación de servicio (DDoS), manteniendo constantes la configuración del sistema, las reglas de detección y las condiciones del entorno tecnológico, con el fin de garantizar la comparabilidad de los resultados.

4.1. Resultados

A continuación, se expone los resultados tras un análisis estadístico para validar los datos obtenidos luego de los ataques ejecutados.

En la tabla 13, se indica el total de ataques ejecutados para el ataque de fuerza bruta siendo 60 eventos. En la tabla 14, indica los porcentajes para los ataques detectados y no detectados, obteniendo 56 ataques detectados que corresponde a un 93,3% del total, así mismo 4 ataques que no fueron detectados representando un 6,7% del total.

Tabla 13. Total, de ataques de fuerza bruta

Estadísticos		
Detección		
N	**Válido**	60
	Perdidos	0

Tabla 14. Porcentajes de detección

Detección					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	**No detecto**	4	6,7	6,7	6,7
	Detecto	56	93,3	93,3	100,0
	Total	60	100,0	100,0	

En la figura 25, se visualiza un resumen de la cantidad de ataques que fueron detectados y no detectados, este resultado demuestra la efectividad de la plataforma Wazuh en la detección de ataques de fuerza bruta con más del 90% de detección. Así mismo para los ataques que no fueron detectados se debe a que la plataforma recibe mucha información proveniente de los agentes monitorizados y este tipo de ataque debe cumplir un umbral de intentos fallidos antes de mostrar una alerta, es decir que si no llega al umbral de intentos fallidos Wazuh no indicará el ataque en su panel de control.

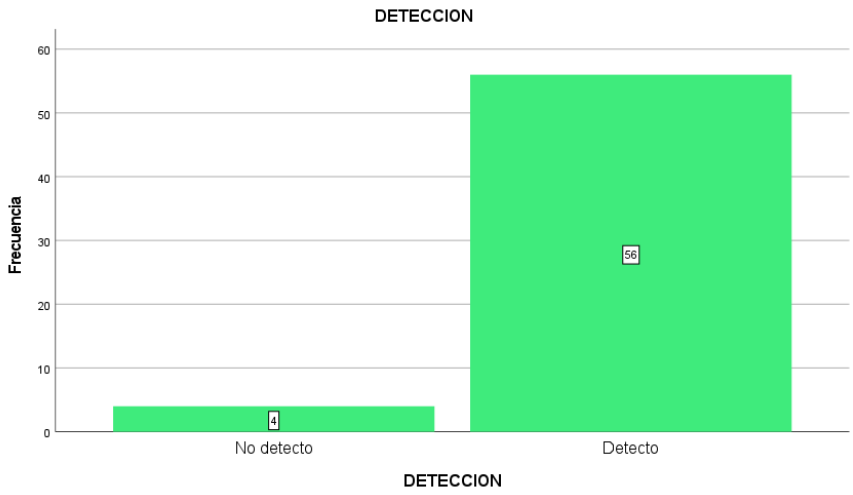


Figura 25. Resumen de detección de ataques

En la tabla 15, indica que para el ataque de denegación de servicio se ejecutaron un total de 30 intentos. En la tabla 16, se obtiene que 25 ataques fueron detectados representando un 83,3% del total, y 5 ataques que no fueron detectados correspondiente al 16,7% del total. Es así como se obtiene que más del 80% del total de los ataques ejecutados fueron detectados, demostrando que la plataforma es efectiva en la detección de ataques de este tipo.

Tabla 15. Total, de ataques para DDoS

Estadísticos		
Detección		
N	**Válido**	30
	Perdidos	0

Tabla 16. Porcentaje de detección de ataques

Detección					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	**No detecto**	5	16,7	16,7	16,7
	Detecto	25	83,3	83,3	100,0
	Total	30	100,0	100,0	

En la figura 26, la gráfica representa la cantidad de ataques que fueron detectados y no detectados para denegación de servicio obteniendo una cantidad alta de detección, pero, hay una cantidad de ataques que no fueron detectados esto puede deberse a ataques que fueron ejecutados en un tiempo menor en relación con los ataques que si fueron detectados motivo por el cual Wazuh no registro el evento y por ende no se generó la alerta.

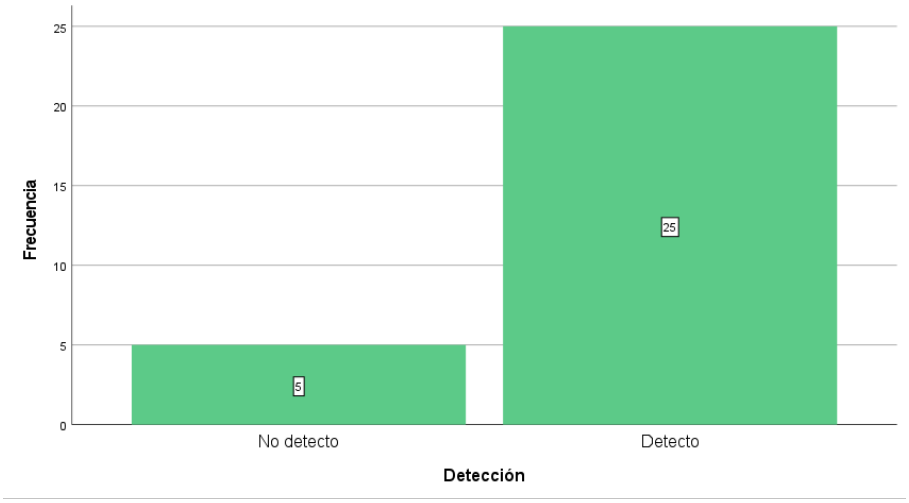


Figura 26. Detección de ataque DDoS

La tabla 17, representa el total de ataques ejecutados para demostrar el funcionamiento de Wazuh en relación con la detección. La tabla 18, muestra el porcentaje de los ataques obteniendo 81 ataques detectados que representa el 90% del total y 9 ataques que no fueron detectados correspondiente al 10%. Con este resultado se demuestra la efectividad de la plataforma con un porcentaje alto en la detección de ataques.

Tabla 17. Total, de ataques ejecutados

Estadísticos		
Detección		
N	**Válido**	90
	Perdidos	0

Tabla 18. Porcentaje de ataques ejecutados

Detección					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	**No detecto**	9	10,0	10,0	10,0
	Detecto	81	90,0	90,0	100,0
	Total	90	100,0	100,0	

La figura 27, representa el total de ataques detectados y no detectados es así como los resultados evidencian que 81 eventos fueron detectados por la plataforma, lo que indica una que las detecciones positivas son predominantes. Esta distribución señala que el sistema de detección tiene una alta capacidad para detectar ataques. Asimismo, los eventos no detectados pueden deberse a que los ataques deben cumplir con ciertas reglas antes de que la plataforma lo tome como un ataque y muestre la alerta en el panel de control de Wazuh.

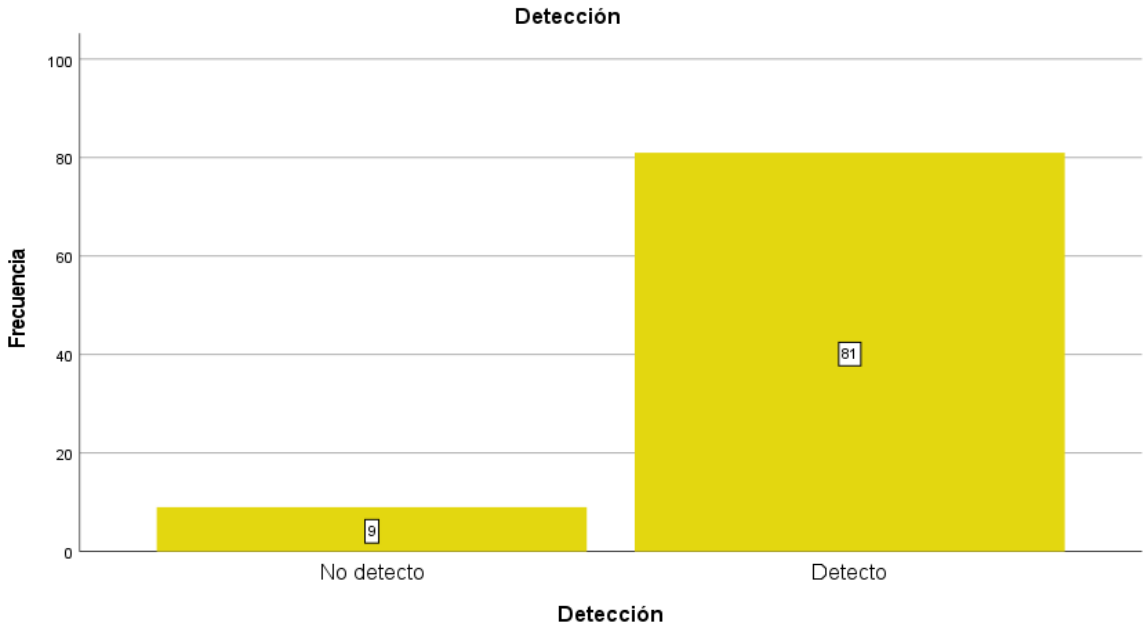


Figura 27. Ataques detectados y no detectados

4.2. Resultados del tiempo de detección

En la tabla 19, se presentan las medidas descriptivas correspondientes al tiempo de detección de los ataques ejecutados, incluyendo la media y la desviación estándar para cada tipo de ataque analizado. Los resultados evidencian que el sistema de seguridad implementado logra detectar los eventos de ataque en intervalos de tiempo reducido, lo que refleja una respuesta oportuna frente a las amenazas simuladas en el entorno experimental.

De acuerdo con la tabla 19, los ataques DDoS mostraron un tiempo promedio de detección de 5,71 segundos y una desviación estándar de 1,083 segundos, lo que señala una variabilidad moderada y tiempos relativamente constantes. Por el contrario, los ataques de fuerza bruta mostraron un tiempo medio más corto de 4,79 segundos, pero con una dispersión más alta. Además, indica que el tiempo mínimo en la detección del ataque es de 4,029 segundos y un tiempo máximo de 7,982 para ataques de denegación de servicio y para ataques de fuerza bruta se obtiene un tiempo mínimo de detección de 2,93 segundos y tiempo máximo de 7,983 segundos. Con respecto al tiempo máximo para ambos ataques se obtuvo un tiempo similar.

Tabla 19. Tiempos medios de detección

Descriptivos				
	Tipo de ataque		**Estadístico**	**Error estándar**
Tiempo en Segundos	**DDoS**	Media	5,71120	,216723
		Mediana	5,68700	
		Varianza	1,174	
		Desviación estándar	1,083615	
		Mínimo	4,029	
		Máximo	7,982	
		Rango	3,953	
	Fuerza bruta	Media	4,79809	,166670
		Mediana	4,68050	
		Varianza	1,556	
		Desviación estándar	1,247243	
		Mínimo	2,935	
		Máximo	7,983	
		Rango	5,048	

En la figura 28, representa la distribución del tiempo de detección para el ataque de denegación de servicio (DDoS), se observa que la mayoría de los datos se concentran en el intervalo de 5 a 6 segundos, lo cual concuerda con la media de 5.71 segundos y una desviación estándar de 1.083 segundos, indicando así una variabilidad moderada. La distribución muestra una forma que es aproximadamente simétrica con tiempos que varían entre 4 y 8 segundos.

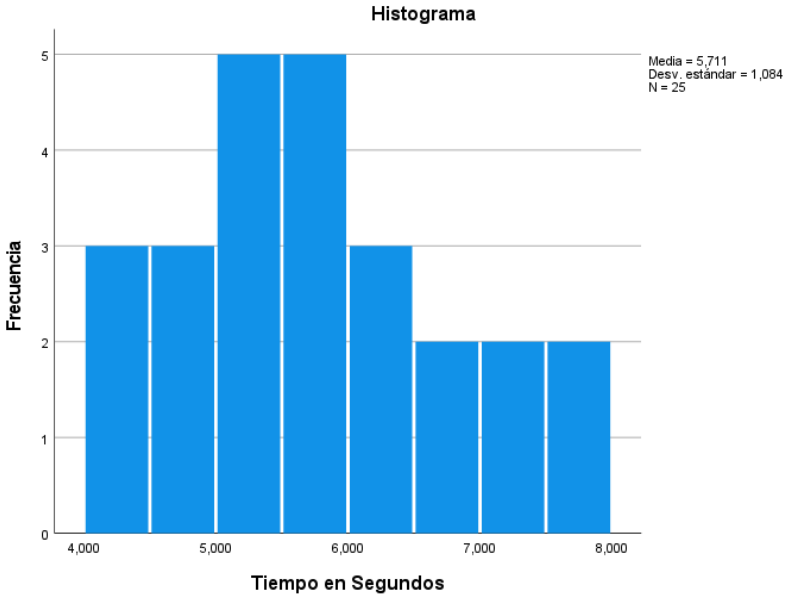


Figura 28. Distribución de tiempo de detección en DDoS

El histograma de la figura 29, representa la distribución del tiempo de detección para el ataque de fuerza bruta, se observa que la mayor concentración se encuentra entre 4 y 5 segundos lo que concuerda que la media sea de 4,79 segundos, además la desviación estándar de 1,24 segundos evidencia que existe una dispersión moderada, obteniendo valores que se extienden desde 3 a 8 segundos. De acuerdo con la gráfica también se visualiza la existencia de tiempos de detección.

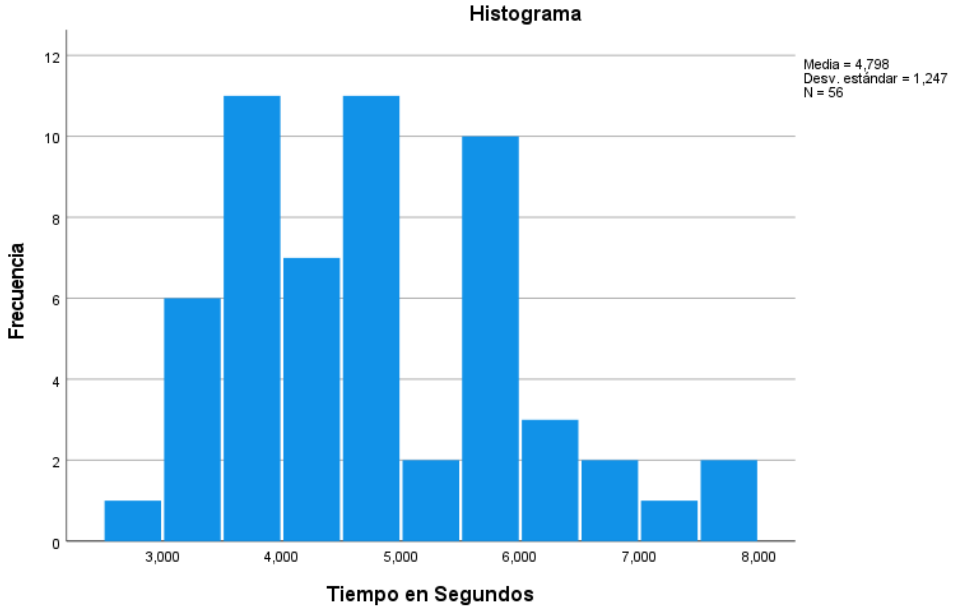


Figura 29. Distribución de tiempo de detección en fuerza bruta

4.3. Verificación del supuesto de Normalidad

Previo a la aplicación de pruebas paramétricas, se verificó el supuesto de normalidad de datos correspondientes al tiempo de detección. Para el caso de los ataques de fuerza bruta, al contar con un tamaño muestral mayor a 50 (n=60), se aplicó la prueba de Kolmogorov-Smirnov, obteniéndose un valor de significancia de p=0,200, lo que indica que los datos siguen una distribución normal. En el caso de los ataques DDoS, con un tamaño muestral menor (n=25), se utilizó la prueba de Shapiro-Wilk, cuyo resultado fue p=0,447, indicando igualmente la normalidad en los datos. En consecuencia, se cumple el supuesto de normalidad requerido para la aplicación de pruebas estadísticas paramétricas y se puede verificar esto datos en la tabla 20.

Tabla 20. Resultado prueba de normalidad

Pruebas de normalidad							
	Tipo de ataque	**Kolmogorov-Smirnov[a]**			**Shapiro-Wilk**		
		Estadístico	**gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Tiempo en segundos	DDoS	,119	25	,200*	,962	25	,447
	Fuerza bruta	,096	56	,200*	,952	56	,025

HIPOTESIS PARA PRUEBA DE NORMALIDAD

Para saber si los datos se distribuyen con normalidad de plantea las siguientes hipótesis:

Hipótesis nula (H_0): Los datos se distribuyen normalmente para el ataque de denegación de servicio

Hipótesis alternativa (H_1): Los datos no se distribuyen normalmente para el ataque de denegación de servicio

Como P-valor = 0,447 > 0,05 no se rechaza H_0 es decir los datos si se distribuyen normalmente para el ataque de denegación de servicio. En la figura 30, se puede observar que efectivamente los datos siguen una distribución normal debido a que se alinean a la recta diagonal de referencia y no se observan desviaciones pronunciadas, sino más bien confirman el resultado estadístico donde indica que el P-valor es mayor que 0,05 indicando una normalidad en los datos.

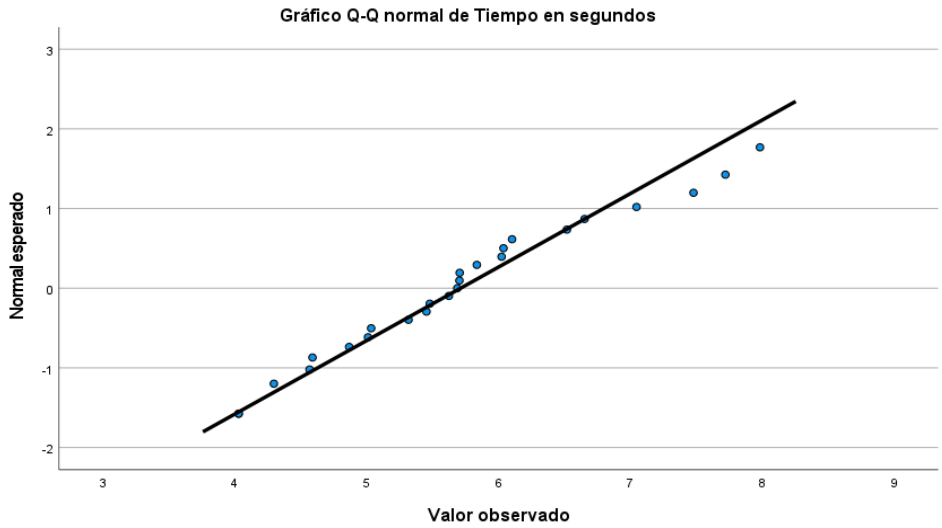


Figura 30. Distribución normal en el ataque DDoS

Hipótesis nula (H_0): Los datos se distribuyen normalmente para el ataque de fuerza bruta
Hipótesis alternativa (H_1): Los datos no se distribuyen normalmente para ataque de fuerza bruta

Como P-valor = 0,200 > 0,05 no se rechaza H_0 es decir que los datos si se distribuyen normalmente para el ataque de fuerza bruta. En términos generales, la figura 31, respalda que los datos del ataque de fuerza bruta se adecuan a una distribución normal, lo cual coincide con el resultado de la prueba de normalidad en la que el p-valor es superior a 0,05.

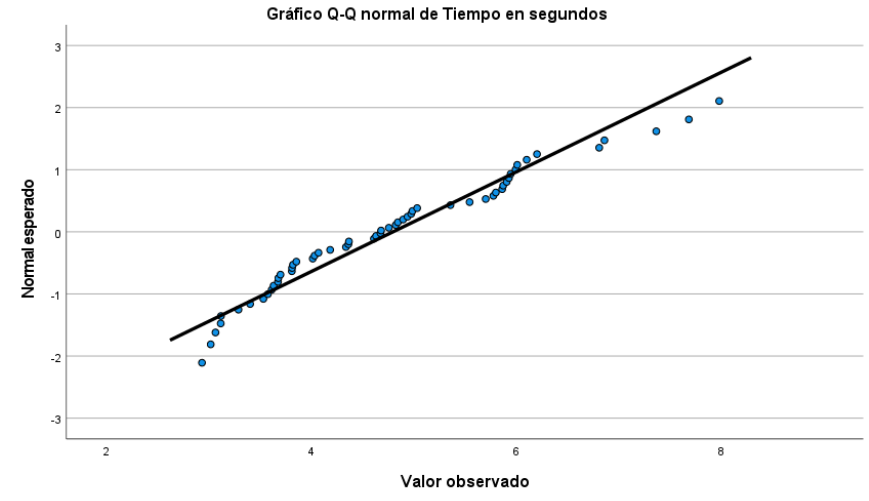


Figura 31. Distribución normal en ataque de fuerza bruta

4.4. Análisis estadístico mediante la prueba T de Student

Con el propósito de determinar si existen diferencias estadísticamente significativas en el tiempo de detección de los ataques informáticos, se aplicó una prueba t de Student para muestras relacionadas, considerando un nivel de significancia de α= 0,05. Los resultados obtenidos evidencian una diferencia significativa entre las medias comparadas, con un valor de t =3,164, gl= 79 y p= 0,002. Asimismo, el intervalo de confianza al 95% para la diferencia de medias se ubicó en 0,913111, lo que confirma la consistencia del resultado observado, es así como se concluye que el tiempo de detección es menor para ataques de fuerza bruta.

Tabla 21. T student independientes

Estadísticas de grupo					
	Tipo de ataque	N	Media	Desviación estándar	Media de error estándar
Tiempo en segundos	DDoS	25	5,71120	1,083615	,216723
	Fuerza bruta	56	4,79809	1,247243	,166670

Tabla 22. Comparación de medias del tiempo de detección

		t	**gl**	**Sig. (bilateral)**	**Diferencia de medias**	**Diferencia de error estándar**
Tiempo en segundos	**Se asumen varianzas iguales**	3,164	79	,002	,913111	,288617
	No se asumen varianzas iguales	3,340	52,734	,002	,913111	,273400

HIPOTESIS PARA MEDIAS

Hipótesis Nula (H_0): No existen diferencias estadísticamente significativas entre las medias del tiempo de detección entre el ataque de denegación de servicios y la media del tiempo de detección del ataque de fuerza bruta.

Hipótesis Alternativa (H_1): Existen diferencias estadísticamente significativas entre las medias del tiempo de detección entre el ataque de denegación de servicios y la media del tiempo de detección del ataque de fuerza bruta.

El valor de $p = 0.002 < 0.05$ de acuerdo con lo que se visualiza en la tabla 20**, se** rechaza la hipótesis nula (H_0)**.** Por lo tanto, se toma la hipótesis alternativa, tomando en cuenta esto se puede indicar que el tiempo de detección del ataque de fuerza bruta es más rápido como se puede observar en el diagrama de caja de la figura 32. En ataques DDoS, la mediana se sitúa en 5,7 segundos con una distribución más concentrada es por ello por lo que la caja está más compacta, pero, con un valor atípico que representa un evento que le llevo más tiempo en ser detectado. Por otra parte, en los ataques de fuerza bruta la mediana se encuentra en 4.7 segundos indicando que la plataforma detecta los ataques en un menor tiempo, pero, de acuerdo con la gráfica para este tipo de ataque la detección es menos uniforme con respecto al ataque DDoS, ya que la caja se abre de 3 hasta 8 segundos existiendo una mayor variabilidad en los tiempos de detección.

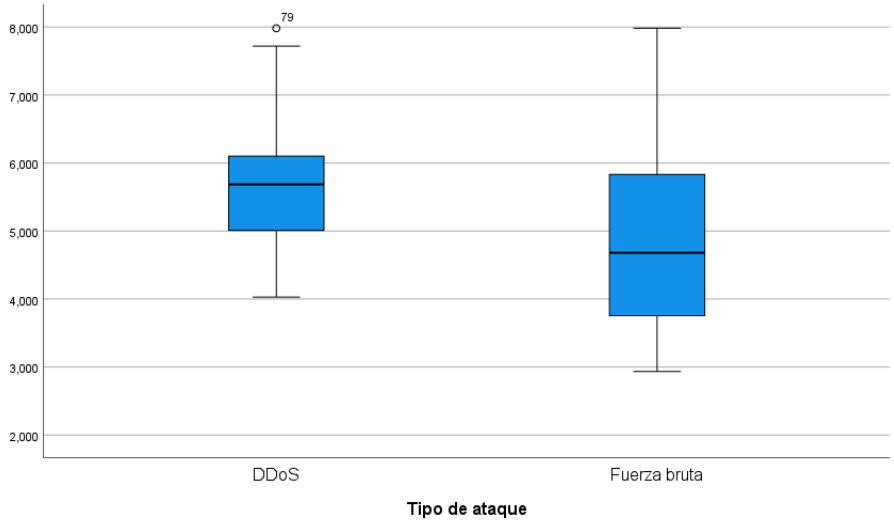


Figura 32. Comparativa de tiempos de detección en ataques

4.5. Discusión

El análisis de los resultados obtenidos permite una valoración integral del desempeño del sistema de seguridad implementado frente a ataques informáticos realizados en el entorno experimental, teniendo en cuenta como principales variables el tiempo de detección y el número de eventos generados. En cuanto al tiempo de detección, los resultados muestran que el sistema es capaz de identificar eventos de ataque en intervalos de tiempos cortos, lo cual es un aspecto importante para una gestión eficaz de los incidentes de seguridad.
La reducción observada en el tiempo de detección refleja la adecuada integración de los componentes del sistema de seguridad, así como la correcta configuración de las reglas de detección utilizadas. El cumplimiento del supuesto de normalidad permitió el uso de pruebas estadísticas paramétricas, que garantizaron la validez de los análisis realizados.

Una prueba t de Student aplicada a los datos obtenidos en este contexto mostró la existencia de una diferencia estadísticamente significativa en el tiempo de detección, confirmando que el comportamiento del sistema no es resultado del azar, sino una consecuencia directa de la implementación propuesta. Además, el cálculo del tamaño del efecto mostró que la magnitud de la diferencia observada es relevante desde un punto de vista práctico. Esto significa que la mejora en el tiempo de detección no sólo es estadísticamente significativa, sino que también tiene un impacto real en la capacidad del sistema para responder a los incidentes de seguridad de manera oportuna.

En cuanto al número de eventos generados, los resultados muestran que el sistema responde consistentemente a la ejecución de ataques y registra alarmas que permiten identificar la ocurrencia de eventos maliciosos. Este comportamiento es fundamental en procesos posteriores de seguimiento y análisis, ya que la adecuada generación de alertas facilita la correlación entre los eventos y la toma de decisiones por parte del personal de seguridad.

En particular, la generación de alertas se mantuvo dentro de rangos controlados, lo que indica un equilibrio adecuado entre la sensibilidad y la precisión del sistema. Esto es importante porque un exceso de alertas puede provocar fatiga operativa, mientras que un número insuficiente puede impedir la detección oportuna de amenazas. En este sentido, los resultados obtenidos muestran que el sistema proporciona un rendimiento suficiente para su uso en un entorno institucional. Desde una perspectiva global, los resultados analizados

permiten confirmar que el sistema de seguridad implementado contribuye significativamente al fortalecimiento de la capacidad de detección y respuesta a ataques informáticos.

La combinación de un tiempo de detección reducido y una generación uniforme de alarmas demuestra la eficacia de la solución propuesta y respalda su aplicabilidad en escenarios operativos reales. Finalmente, los resultados obtenidos se alinean con los objetivos planteados en el estudio y sustentan las hipótesis propuestas, las cuales prueban que la implementación del sistema de seguridad es un aporte significativo a la mejora de los procesos de monitoreo y gestión de incidentes en la infraestructura tecnológica analizada.

CAPÍTULO V. CONCLUSIONES y RECOMENDACIONES

5.1 Conclusiones

- Se logró implementar y evaluar un sistema de seguridad basado en la integración de Wazuh y Suricata, el cual permitió detectar de manera efectiva ataques de fuerza bruta y ataques de denegación de servicio distribuido (DDoS) en el entorno experimental definido. La correcta configuración de los componentes del sistema y de las reglas de detección posibilitó la identificación oportuna de eventos maliciosos, cumpliendo con el objetivo general de la investigación.

- Los resultados obtenidos evidencian una mejora significativa en el tiempo de detección de los ataques informáticos, lo cual fue confirmado mediante la aplicación de pruebas estadísticas paramétricas. La prueba t de Student demostró diferencias estadísticamente significativas en los tiempos de detección, respaldadas por un tamaño del efecto relevante, lo que indica que la mejora observada no es atribuible al azar, sino al desempeño del sistema de seguridad implementado.

- El análisis del número de alertas generadas mostró un comportamiento consistente del sistema frente a los ataques ejecutados, permitiendo registrar de manera adecuada los eventos de seguridad sin incurrir en una generación excesiva de alertas. Este equilibrio entre sensibilidad y precisión resulta fundamental para la gestión eficiente de incidentes y para evitar la saturación operativa del personal de seguridad.

- La verificación del supuesto de normalidad y la aplicación de técnicas estadísticas apropiadas fortalecieron la validez de los resultados obtenidos, garantizando un análisis riguroso y confiable del desempeño del sistema. La metodología empleada permitió evaluar de forma objetiva las variables definidas, asegurando la coherencia entre el diseño experimental, el análisis de datos y las conclusiones alcanzadas.

- En conjunto, los hallazgos de la investigación confirman que la implementación del sistema de seguridad propuesto contribuye de manera efectiva a fortalecer los procesos de monitoreo y detección de incidentes informáticos, constituyéndose en

una alternativa viable para mejorar la capacidad de respuesta ante amenazas en infraestructuras tecnológicas institucionales similares al entorno analizado.

5.2 Recomendaciones

- Para obtener una vista unificada de toda la infraestructura tecnológica, se sugiere que la implementación de agentes Wazuh se expanda a otros sistemas y dispositivos esenciales, incluyendo servidores académicos, sistemas de gestión, firewalls y equipos de red.
- Fomentar una cultura de concienciación en ciberseguridad en toda la comunidad universitaria, a través de capacitaciones, campañas informativas y buenas prácticas dirigidas a estudiantes, profesores y personal administrativo, teniendo en cuenta que la seguridad de la información es un deber compartido.
- Se recomienda integrar otras herramientas de seguridad que trabajen en conjunto con la plataforma Wazuh con la finalidad de ampliar la capacidad de detección ante amenazas, esto permitirá una protección de la infraestructura más completa.

BIBLIOGRÁFIA

[1] Derenzin Martinez Feddor, "¿Están los institutos universitarios en Ecuador preparados para los ciberataques?," *593 Digital Publisher CEIT*, vol. 9, no. 6, pp. 1220–1232, Nov. 2024, doi: doi.org/10.33386/593dp.2024.6.2864.

[2] Asamblea Nacional, "LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES." Accessed: May 03, 2025. [Online]. Available: www.lexis.com.ec

[3] Córdova Vela Juan, "Despliegue de controles de nube con base en análisis de riesgos," Universidad de los Andes, Bogotá, 2023. Accessed: May 14, 2025. [Online]. Available: https://repositorio.uniandes.edu.co/server/api/core/bitstreams/af88f564-9bbd-46c0-af55-1edc1fcefb17/content

[4] Revista Electrónica Cyber Defense, "Por qué la educación superior es tan vulnerable a los ciberataques y qué hacer." Accessed: Jun. 16, 2025. [Online]. Available: https://www.cyberdefensemagazine.com/why-higher-education-is-so-vulnerable-to-cyber-attacks-and-what-to-do/

[5] Jackins Trevor, "La seguridad de TI es una prioridad máxima para la educación superior." Accessed: Jun. 16, 2025. [Online]. Available: https://www.splashtop.com/es/blog/research-finds-it-security-a-top-priority-for-higher-ed?srsltid=AfmBOorAvuIm1GFJM-BXsWiCivJYEmVbpnhCFM_fTdRFgUPE2K8QaF13

[6] Chacha Chunata Estefanía, "ANÁLISIS DE LAS METODOLOGÍAS ENISA Y APCERT PARA LA CREACIÓN DEL CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS (CSIRT). CASO PRÁCTICO: PROTOTIPO DE UN CSIRT EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO," Riobamba, 2019.

[7] Paredes Pablo and Medina Patricio, "Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador," *3C TIC: Cuadernos de desarrollo aplicados a las TIC*, vol. 10, no. 2, pp. 49–75, Jun. 2021, doi: 10.17993/3ctic.2021.102.49-75.

[8] Gálvez Soriano Pol, "Despliegue e implantación de un SIEM con Wazuh," Universitat Politécnica de Catalunya, Barcelona, 2024. Accessed: May 14, 2025. [Online]. Available: https://upcommons.upc.edu/handle/2117/418178

[9] Granados Dávila Juan, "Implementación de hacking ético para mejorar la detección y evaluación de vulnerabilidades de la seguridad en la infraestructura minera en la

ciudad de Lima - 2021," Universidad Tecnológica del Perú, Lima, 2021. Accessed: May 19, 2025. [Online]. Available: http://repositorio.utp.edu.pe/handle/20.500.12867/5189

[10] Cantuña Pinto Josue, "Implementación de un SIEM para la defensa activa ante intrusiones en una red," Escuela Politécnica Nacional, Quito, 2024. Accessed: May 14, 2025. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/25830

[11] Herrera Lara Luis, "Implementación de un Centro de Operaciones de Seguridad y Redes (NSOC) Usando Herramientas Open Source para la Infraestructura Industrial de la Empresa Eléctrica Quito.," Escuela Politécnica Nacional, Quito, 2022. Accessed: Jun. 23, 2025. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/22864

[12] Silva Marroquín Andrés, "Estudio comparativo de sistemas de detección de intrusiones (ids) en software libre e implementación en los laboratorios de la Facultad de Ingeniería de Universidad Nacional de Chimborazo.," Universidad Nacional de Chimborazo, Riobamba, 2024. Accessed: May 19, 2025. [Online]. Available: http://dspace.unach.edu.ec/handle/51000/13154

[13] Gallegos Guanopatín Jaime, "ANÁLISIS DE ATAQUES Y ATACANTES EXTERNOS A LA INFRAESTRUCTURA DE DATOS DE LA ESPOCH, MEDIANTE LA IMPLEMENTACIÓN DE UN HONEYPOT DEL TIPO (T-POT)," Escuela Politécnica de Chimborazo, Riobamba, 2021. Accessed: Jun. 08, 2025. [Online]. Available: https://dspace.espoch.edu.ec:8080/server/api/core/bitstreams/f2b68aeb-1768-424d-99ff-0ebec7b21463/content

[14] Herrera Silva Jhonatan, "Análisis de tráfico de datos maliciosos mediante técnicas Machine Learning, utilizando OPNids en la red del edificio de la FIE.," Escuela Superior Politecnica de Chimborazo, Riobamba, 2021. Accessed: Jun. 23, 2025. [Online]. Available: https://dspace.espoch.edu.ec/items/bca960ca-6dbe-4cf2-b0d5-a35650ecdfef

[15] Vega Briceño Edgar, *SEGURIDAD DE LA INFORMACIÓN*, Primera edición. 2021. doi: https://doi.org/10.17993/tics.2021.4.

[16] LISA Institute, "Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de – LISA Institute." Accessed: Oct. 27, 2025. [Online]. Available: https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-

informatica-seguridad-informacion?srsltid=AfmBOoomZo6H6fnY7dzcH8-wb8QveUqkebOQPOmQ-tC5gxN9xbM47mBP

[17] OptiSec Zero Trust Security, "¿Qué es la Tríada CID en Ciberseguridad? - Notiemp." Accessed: Oct. 27, 2025. [Online]. Available: https://notiemp.com.mx/2023/05/04/que-es-la-triada-cid-en-ciberseguridad/

[18] Sánchez José, "Las dimensiones fundamentales en Ciberseguridad - Club CISO." Accessed: Oct. 27, 2025. [Online]. Available: https://club-ciso.aec.es/las-dimensiones-fundamentales-en-ciberseguridad/

[19] Pachamama Edison, "Implementación de un SIEM para la defensa activa ante un ataque por malware.," 2024. Accessed: May 12, 2025. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/25910

[20] M. A. Alcocer Bahamonde, J. P. del Castillo Soto, B. E. Gomez Cumbajin, and C. L. Hidalgo Llumiquinga, "Implementación y análisis de un sistema de monitorización y correlación de eventos para infraestructuras empresariales," Universidad Internacional del Ecuador, Quito, 2022. Accessed: May 14, 2025. [Online]. Available: https://repositorio.uide.edu.ec/handle/37000/5608

[21] Fernández Danny, "Propuesta de monitorización de eventos de seguridad con WAZUH para Instituciones de Educación Superior," 2023. Accessed: May 12, 2025. [Online]. Available: http://repositorio.uisrael.edu.ec/handle/47000/3950

[22] "Documentación de Wazuh." Accessed: May 07, 2025. [Online]. Available: https://documentation.wazuh.com/current/getting-started/components/index.html

[23] "Wazuh:La plataforma de seguridad de código abierto. Protección unificada XDR y SIEM para endpoints y cargas de trabajo en la nube." Accessed: May 07, 2025. [Online]. Available: https://github.com/wazuh/wazuh

[24] "¿Qué es Suricata en ciberseguridad? | KeepCoding Bootcamps." Accessed: Dec. 12, 2025. [Online]. Available: https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

[25] "hping3 | Herramientas de Kali Linux." Accessed: Dec. 12, 2025. [Online]. Available: https://www.kali.org/tools/hping3/

[26] "hydra | Herramientas de Kali Linux." Accessed: Dec. 12, 2025. [Online]. Available: https://www.kali.org/tools/hydra/

[27] “Recurso Nucleus | ¿Qué es una vulnerabilidad de seguridad?” Accessed: Nov. 11, 2025. [Online]. Available: https://nucleussec.com/resources/knowledge-center/what-is-a-security-vulnerability/

[28] “¿Qué es una amenaza de ciberseguridad? | Glosario | HPE LAMERICA.” Accessed: Nov. 11, 2025. [Online]. Available: https://www.hpe.com/lamerica/es/what-is/cybersecurity-threats.html

[29] Equipo GoDaddy, “Logs: Qué son y cómo se usan para monitorizar sistemas y seguridad.” Accessed: Jun. 18, 2025. [Online]. Available: https://www.godaddy.com/resources/latam/tecnologia/log-que-es

[30] “Ataque de denegación de Servicio | Ataque Smurf | Cloudflare.” Accessed: Nov. 25, 2025. [Online]. Available: https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

[31] “Respuesta activa - Capacidades · Documentación de Wazuh.” Accessed: Jan. 18, 2026. [Online]. Available: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html

[32] “Máquina virtual (VM): alternativas de instalación · Documentación de Wazuh.” Accessed: Dec. 13, 2025. [Online]. Available: https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

[33] “Detección de un ataque de fuerza bruta: guía de prueba de concepto.” Accessed: Jan. 25, 2026. [Online]. Available: https://documentation.wazuh.com/current/proof-of-concept-guide/detect-brute-force-attack.html

ANEXOS

Dirección de Tecnologías de la
Información y Comunicación
VICERRECTORADO ADMINISTRATIVO

en movimiento

ACTA DE CONFORMIDAD

El suscrito Director de Tecnologías de la Información y Comunicación, tiene a bien informar que el 13 de enero, 2026 a las 10h30 se ha recibido el proyecto de titulación denominado **"Implementación de una plataforma de seguridad open source mediante Wazuh para el monitoreo y gestión de incidentes de seguridad de la información en la infraestructura de la Dirección de Tecnología de Información y Comunicación de la Universidad Nacional de Chimborazo"**, desarrollado por la señorita Lourdes Gabriela Guailla Shulca con C.C: 0605955046, estudiante de la carrera de Telecomunicaciones, y habiendo revisado que cumple con todos los requerimiento de la DTIC se procede a recibir a conformidad.

Riobamba, 19 de enero de 2026.

Atentamente,

JOSE JAVIER HARO MENDOZA

Ing. Javier Haro Mendoza
DIRECTOR DE TECNOLOGÍAS DE
LA INFORMACIÓN y COMUNICACIÓN

JH:mzs.

Campus Norte | Av. Antonio José de Sucre, Km 1 ½ vía a Guano | Teléfonos: (593-3) 3730880 - Ext.: 1300-1310

Figura 33. Acta de conformidad DTIC