

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDPS) PARA MITIGAR VULNERABILIDADES EN EL ACCESO A LA RED DE LA UNIDAD EDUCATIVA "PIO LOPEZ"

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información

ÁREA: Gestión de tecnologías de la información

LÍNEA DE INVESTIGACIÓN: Tecnologías de la información y Sistemas de control

AUTOR: Brayan Stiven Alomaliza Chuca

TUTOR: Ing. David Omar Guevara Aulestia, Mg.

Ambato - Ecuador

julio - 2025

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDPS) PARA MITIGAR VULNERABILIDADES EN EL ACCESO A LA RED DE LA UNIDAD EDUCATIVA "PIO LOPEZ", desarrollado bajo la modalidad Proyecto de Investigación por el señor Brayan Stiven Alomaliza Chuca, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, julio 2025.

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA
Validar únicamente con FirmaEC

Ing. David Omar Guevara Aulestia, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDPS) PARA MITIGAR VULNERABILIDADES EN EL ACCESO A LA RED DE LA UNIDAD EDUCATIVA "PIO LOPEZ", es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, julio 2025.



Brayan Stiven Alomaliza Chuca

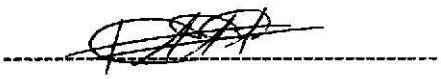
C.C. 1850094507

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, julio 2025.



Brayan Stiven Alomaliza Chuca
C.C. 1850094507
AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Brayan Stiven Alomaliza Chuca , estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDPS) PARA MITIGAR VULNERABILIDADES EN EL ACCESO A LA RED DE LA UNIDAD EDUCATIVA "PIO LOPEZ", nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor Presidente del Tribunal.

Ambato, julio 2025.



Ing. Franklin Oswaldo Mayorga Mayorga Mg.
PRESIDENTE DEL TRIBUNAL



Ing. Franklin Mayorga Mayorga Mg.
PROFESOR CALIFICADOR



Ing. Daniel Maldonado Ruiz, PhD.
PROFESOR CALIFICADOR

DEDICATORIA

Este proyecto se lo dedico con todo mi amor y gratitud a mis padres, Luzmila y Mario, cuyo apoyo, guía y sacrificio han sido fundamentales a lo largo de mi vida. Gracias por ser mi ejemplo de esfuerzo, responsabilidad y amor incondicional. Cada paso en este camino lo he dado con la fuerza que me han transmitido.

A mis hermanos, Johan y Monserrath, por ser una fuente constante de apoyo y motivación para seguir adelante, y por inspirarme a ser un buen ejemplo para ellos.

A mi abuela Carmen, por ser un inquebrantable refugio de amor y sabiduría, siempre dispuesta a ofrecerme su cariño. Y a la memoria de mi abuelo Carlos, cuya presencia continúa acompañándonos y protegiéndonos desde el cielo.

A toda mi familia, por estar siempre presente, por su cariño sincero y por brindarme el apoyo necesario para continuar, incluso en los momentos más difíciles.

AGRADECIMIENTO

Primero quiero agradecer a Dios por darme vida, saluda y sabiduría por permitirme termina mi carrera universitaria.

A mis padres Luzmila y Mario, cuyo apoyo, guía y sacrificio han sido fundamentales durante cada proceso de mi vida por inspirarme con su ejemplo de lucha incansable.

A Luis y Alex, por brindarme su apoyo, consejos y enseñanzas tanto dentro como fuera de la universidad, siendo una fuente constante de motivación.

A mí tutoro el Ing. David Guevara por su apoyo, conocimientos y guía para la elaboración de este proyecto de investigación.

A mis amigos Erika, Gloria, Paul y Bryan, por su valiosa compañía durante la universidad. Su motivación y enseñanzas hicieron este trayecto mucho más llevadero. Gracias, muchachos; me quedo con los momentos compartidos, dentro y fuera del aula.

A mi prima Cristina, por ser como una hermana, mi confidente y compañera de aventuras. Gracias por estar siempre, especialmente en los momentos difíciles.

A toda mi familia, por brindarme siempre su apoyo y cariño incondicional.

Finalmente, a todo el personal de la Unidad Educativa Pío López, por su valiosa colaboración en el desarrollo de este proyecto. En especial, a la Lcda. Silvia, docente de la institución, por el apoyo brindado para que este proyecto se llevase a cabo.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA ..... **i**

APROBACIÓN DEL TUTOR ..... **ii**

AUTORÍA ..... **iii**

DERECHOS DE AUTOR ..... ¡Error! Marcador no definido.

APROBACIÓN DEL TRIBUNAL DE GRADO ..... **v**

DEDICATORIA ..... **vi**

AGRADECIMIENTO ..... **vii**

ÍNDICE DE TABLAS ..... **xii**

ÍNDICE DE FIGURAS ..... **xiii**

ÍNDICE DE ANEXOS ..... **xv**

RESUMEN EJECUTIVO ..... **xvi**

ABSTRACT ..... **xvii**

CAPÍTULO I. MARCO TEÓRICO **1**

1.1 Tema de investigación 1

1.1.1 Planteamiento del problema 1

1.2 Antecedentes investigativos 2

1.3 Fundamentación teórica 5

1.3.1 Tecnologías de la Información y Comunicación (TIC) 5

1.3.2 Sistema de Detección y Prevención de Intrusiones (IDPS) 6

1.3.3 Implementación de Software 6

1.3.4 Seguridad Informática 7

1.3.5 Normativas y Políticas de Ciberseguridad 8

1.3.6 Gestión de Red 8

1.3.7 Vulnerabilidades en el Acceso de la Red 9

1.4 Objetivos 11

1.4.1 Objetivo general 11

1.4.2 Objetivos específicos 11

CAPÍTULO II. METODOLOGÍA 12

2.1 Materiales 12

2.1.1 Entrevista al rector de la ¨Unidad Educativa Pio López¨ 12

2.1.2 Encuesta dirigida a los docentes de la “Unidad Educativa Pio López” 12

2.1.3 Ficha de observación 13

2.2 Métodos 14

2.2.1 Modalidad de la investigación 14

2.2.2 Población y muestra 15

2.2.3 Recolección de información 16

CAPÍTULO III. RESULTADOS Y DISCUSIÓN 26

3.1 Análisis y discusión de los resultados 26

3.1.1 Análisis de la infraestructura de red 27

3.1.2 Identificación de activos críticos 27

3.1.3 Evaluación de riesgos y amenazas 29

3.1.4 Clasificación de vulnerabilidades 31

3.1.5 Controles de seguridad seleccionados ISO/IEC 27001 32

3.2 Implementación del sistema IDPS (Fase de Ejecución) 34

3.2.1 Metodología para el proyecto 34

3.2.2 Diseño de la arquitectura de red 35

3.2.3 Selección e instalación de Suricata 36

3.2.4 Configuración de reglas personalizadas 41

3.2.5 Integración con ELK Stack para monitoreo 43

3.2.6 Adaptaciones en la infraestructura física 44

3.3 Evaluación de la eficacia del sistema (Fase de Verificación) 45

3.3.1 Pruebas funcionales del IDPS 46

3.3.2 Simulación de incidentes y análisis de respuesta 46

3.3.3 Métricas de desempeño (detección, precisión, tiempo de respuesta) 48

3.3.4 Comparación con estado inicial 50

3.4 Mejora continua del SGSI (Fase de Actuación) 51

3.4.1 Ajustes realizados tras la implementación 51

3.4.2 Recomendaciones para la actualización de reglas y políticas 51

3.4.3 Proyecciones de escalabilidad y mantenimiento 52

3.4.4 Lecciones aprendidas y sostenibilidad del sistema 53

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 55

4.1 Conclusiones 55

4.2 Recomendaciones 56

REFERENCIAS BIBLIOGRÁFICAS 57

ANEXOS 60

ÍNDICE DE TABLAS

Tabla 1. Cadenas de búsquedas. 2

Tabla 2. Criterios de inclusión y exclusión. 3

Tabla 3. Ficha de observación. 13

Tabla 4. Población de estudio. 15

Tabla 5. Entrevista al rector de la institución. 16

Tabla 6. Activos en la Institución. 28

Tabla 7. Evaluación de riesgo. 31

Tabla 8. Resumen de Vulnerabilidades. 31

Tabla 9. Controles de la norma ISO/IEC 27001. 33

Tabla 10. Comparativa de software IDS/IPS[24]. 37

ÍNDICE DE FIGURAS

Figura 1. Datos de la pregunta 1. 19

Figura 2. Datos de la pregunta 2. 20

Figura 3. Datos de la pregunta 3. 20

Figura 4. Datos de la pregunta 4. 21

Figura 5. Datos de la pregunta 5. 22

Figura 6. Datos de la pregunta 6. 22

Figura 7. Datos de la pregunta 7. 23

Figura 8. Datos de la pregunta 8. 24

Figura 9. Datos de la pregunta 9. 24

Figura 10. Datos de la pregunta 10. 25

Figura 11. Topología de red de la institucion. 27

Figura 12. Topología de red. 35

Figura 13. Configuración del perfil. 40

Figura 14. Instalación de Suricata. 41

Figura 15. Reglas de suricata. 42

Figura 16. Editor de archivos de suricata. 42

Figura 17. Visualizacion de Logs. 44

Figura 18. Esquema de red con el switch. 45

Figura 19. Registro de log de Suricata. 47

Figura 20. Registro de eventos en elastic. 47

Figura 21. Ataque de utilizando hping3. 48

Figura 22. Registro del ataque en Elastic. 48

ÍNDICE DE ANEXOS

ANEXO A. ENCUESTA A DOCENTES DE LA INSTITUCION 60

ANEXO B. GUIA DE INSTALACION UBUNTU SERVER..... 62

ANEXO C. GUÍA DE INSTALACIÓN SURICATA..... 71

ANEXO D. INSTALACIÓN Y CONFIGURACIÓN DE ELK STACK..... 79

ANEXO E. GUIA DE CREACION DE REGLAS..... 86

RESUMEN EJECUTIVO

El avance tecnológico en instituciones educativas ha generado una creciente preocupación por la seguridad informática. La protección contra ataques cibernéticos es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información dentro de la institución educativa "Pío López". Ante esta necesidad, se desarrolló un Sistema de Detección y Prevención de Intrusiones (IDPS) con el propósito de fortalecer la seguridad de la infraestructura y mitigar amenazas en un entorno académico, la metodología aplicada dentro del presente proyecto es la ISO/IEC 27001 que consto con cuatro fases. En la primera etapa se realizó un análisis de riesgos empleando Nmap para el escaneo de puertos y sistemas, y OpenVAS para la detección de vulnerabilidades, obteniendo un diagnóstico detallado de la infraestructura. Se registraron algunas vulnerabilidades y configuraciones por defecto de los equipos tecnológicos.

La segunda fase se centró en la implementación de un switch centralizado, implementación de un IDPS con Suricata, integrando un sistema de visualización con ELK Stack. Para la tercera etapa se evaluó el funcionamiento a través de simulaciones de ataques, que incluyeron Slowloris, DoS, Man-in the-middle para verificar la efectividad del sistema, registrando los eventos y su correcto funcionamiento. En la cuarta fase se ajustaron umbrales de duración de conexiones y volúmenes de datos para mejorar la detección de ataques lentos como Slowloris.

Como resultado, el sistema desarrollado demostró ser robusto y escalable, con un bajo costo operativo. Logró detectar comportamientos sospechosos y mitigar ataques en tiempo real, mejorando significativamente la seguridad de la red institucional.

El IDPS implementado proporciona un modelo replicable para otras instituciones educativas, mejorando la protección contra ciberamenazas.

Palabras clave: Aplicación de ISO/IEC 27001, seguridad informática educativa, IDPS, vulnerabilidades, mitigación, suricata.

ABSTRACT

Technological advancement in educational institutions has generated growing concern about cybersecurity. Protection against cyberattacks is essential to ensure the confidentiality, integrity, and availability of information within the "Pío López" educational institution. In response to this need, an Intrusion Detection and Prevention System (IDPS) was developed to strengthen infrastructure security and mitigate threats in an academic environment. The methodology applied in this project is ISO/IEC 27001, which consisted of four phases. In the first phase, a risk analysis was performed using Nmap for port and system scanning, and OpenVAS for vulnerability detection, obtaining a detailed diagnosis of the infrastructure. Some vulnerabilities and default configurations of the technological equipment were recorded.

The second phase focused on the implementation of a centralized switch, an IDPS with Suricata, and integrating a visualization system with the ELK Stack. For the third phase, performance was evaluated through attack simulations, including Slowloris, DoS, and Man-in-the-Middle attacks, to verify the system's effectiveness, logging events, and proper operation. In the fourth phase, connection duration thresholds and data volumes were adjusted to improve the detection of slow attacks like Slowloris.

As a result, the developed system proved to be robust and scalable, with a low operating cost. It was able to detect suspicious behavior and mitigate attacks in real time, significantly improving the security of the institutional network.

The implemented IDPS provides a replicable model for other educational institutions, improving protection against cyberthreats.

Keywords: Application of ISO/IEC 27001, educational computer security, IDPS, vulnerabilities, mitigation, meerkat.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

SISTEMA DE DETECCION Y PREVENCIÓN DE INTRUSIONES (IDPS) PARA MITIGAR VULNERABILIDADES EN EL ACCESO A LA RED DE LA UNIDAD EDUCATIVA “PIO LOPEZ”.

1.1.1 Planteamiento del problema

La seguridad digital es un aspecto crucial en la actualidad, donde las Tecnologías de la Información y la Comunicación (TIC) han transformado todos los sectores, incluido el educativo. La tecnología a través de dispositivos electrónicos y plataformas digitales se ha vuelto indispensable en la educación superior, facilitando el acceso a la información, la comunicación y la realización de actividades académicas de manera eficiente[1].

En Ecuador, aunque la ciberseguridad ha sido declarada una política pública, aún no existe una estrategia nacional integral que establezca lineamientos claros para proteger los servicios, las infraestructuras críticas y la información frente a ciberamenazas. Esta falta de regulación y protección afecta significativamente a las Instituciones de Educación Superior, donde el uso creciente de plataformas web y móviles ha incrementado la exposición a riesgos de ciberataques[2]. Un estudio realizado en la provincia de Tungurahua reveló que los Institutos Tecnológicos Superiores enfrentan vulnerabilidades debido a la escasez de personal capacitado en ciberseguridad y a la ausencia de planes de respuesta ante incidentes informáticos. Esto compromete la integridad de los datos de docentes y estudiantes, quienes dependen de estas plataformas para el desarrollo de sus actividades académicas[2].

La expansión digital ha traído consigo un mayor riesgo cibernéticos. Debido al alto valor de los datos, estos se han convertido en un objetivo clave para los cibercriminales, lo que ha generado numerosas brechas de seguridad. Los atacantes emplean diversas técnicas para conseguir sus objetivos. Un ejemplo relevante se dio en 2014, cuando varias empresas, como Target, Home Depot y UPS, fueron víctimas

de un ataque relacionado con malware Point of Sale, que permitió el robo de más de 40 millones de números de tarjetas de crédito y débito. [3].

1.2 Antecedentes investigativos

Para el desarrollo del presente proyecto, se llevó a cabo una revisión de literatura mediante la exploración de diversas fuentes científicas. Las cadenas de búsqueda fueron diseñadas cuidadosamente, empleando palabras claves relevantes como 'Sistema de Detección y Prevención', 'seguridad de red', 'mitigación de vulnerabilidades'. Como resultado de estas búsquedas, se obtuvieron los siguientes hallazgos que se muestran en la Tabla 1.

Tabla 1. Cadenas de búsquedas.

Base de Datos	**Cadenas de Búsqueda**	**Núm. de Artículos**
Scopus	TITLE-ABS-KEY ("Intrusion Detection and Prevention System" AND ("network security" OR "vulnerability mitigation")) AND PUBYEAR > 2019 AND (LIMIT-TO (LANGUAGE, "English")	20
	TITLE-ABS-KEY ("Intrusion Detection" AND "access control" OR "vulnerability management" AND NOT "physical security") AND PUBYEAR > 2019 AND (LIMIT-TO (LANGUAGE, "English"))	4
IEEE Xplore	("All Metadata":"Intrusion Detection System" AND ("cybersecurity" OR "attack prevention")) Filters Applied: 2020 – 2024	5
	("All Metadata":"IDPS" AND "vulnerability assessment" OR "network monitoring" NOT "data center security") Filters Applied: 2020 – 2024	4

Base de Datos	Cadenas de Búsqueda	Núm. de Artículos
Scielo	("Intrusion Detection System") Filtros activados: 2020 - 2023	6
	("network traffic monitoring") Filtros activados: 2020 - 2024	2
Total		41

A partir de la revisión literaria pertinente, se llevó a cabo un análisis minucioso de la documentación relacionada con el proceso de selección. Como resultado, se identificó 5 artículos que cumplen con los criterios previamente establecidos para un análisis más exhaustivo, utilizando criterios específicos de inclusión y exclusión. Estos artículos fueron seleccionados utilizando criterios de inclusión y exclusión, los cuales se detallan en la Tabla 2.

Tabla 2. Criterios de inclusión y exclusión.

Inclusión	• Artículos o estudios que analicen el uso de herramientas de código abierto en el ámbito de la seguridad informática y redes. • Investigaciones relacionadas con la implementación de sistemas de control y monitoreo en redes educativas. • Casos de éxito o estudios prácticos aplicados a entorno educativos con características similares.
Exclusión	• Publicaciones que no consideren herramientas de código abierto. • Estudios que no estén relacionados con redes educativas o que se enfoquen exclusivamente en entornos empresariales. • Artículos con acceso restringido o que requieran pagos para su consulta. • Investigaciones puramente teóricas sin ejemplos prácticos en escenarios reales. • Documentos duplicados o con información redundante.

Molina et al.[4] trabajaron en estrategias y herramientas para reducir los riesgos relacionados con ataques DDoS, como los vectores de ataque más comunes de inundación de ancho de banda de red y sobrecarga de recursos de aplicación. Los autores avanzaron sistemas de monitoreo en tiempo real, filtros de tráfico avanzados y políticas de balanceo de carga con filtros y cortafuegos específicos para ataques DDoS, señalando que el uso de técnicas proactivas y reactivas simultáneamente reduce la probabilidad de ataques exitosos mientras mejora el rendimiento general de la red y la experiencia del usuario incluso en entornos hostiles.

Renzo Manrique[5], se ha demostrado que estas medidas refuerzan la seguridad de las redes definidas por software (SDN) al proporcionar una mayor protección contra las superficies de ataque cibernético y amenazas de DoS, escaneo de puertos, botnet y dominios maliciosos. No solo estas medidas mejoran la seguridad de los sistemas, sino que también mejoran el rendimiento de la red utilizando funcionalidades como la evasión de cortafuegos y la reducción del tráfico espurio enviado al IDS, que aumenta la carga operativa del sistema.

Godfrey A, Daniel K y Robert A[6] diseñaron un sistema de detección de intrusiones híbrido que supuestamente intenta resolver los problemas actuales en la seguridad de redes debido a la naturaleza agresiva de los ataques. Con la integración de algoritmos de aprendizaje automático como redes neuronales artificiales, mapas autoorganizados y árboles de decisión, desarrollaron un modelo que integra aprendizaje supervisado y no supervisado para mejorar la precisión en la detección de amenazas mientras minimiza las falsas alarmas. Este sistema, desarrollado en Java para garantizar portabilidad, obtuvo resultados excepcionales en pruebas de evaluación contra los conjuntos de datos NSL-KDD y CIC-DDoS2019.

Uno de los trabajos más relevantes en el campo del escaneo y detección de intrusiones y evaluación de vulnerabilidades en las redes es el de David A. Franco et al.[7] quienes desarrollaron un enfoque novedoso utilizando una técnica basada en huellas de servicio para evaluar la seguridad de los dispositivos de red. Esta estrategia se concentra en descubrir los nombres y versiones de los servicios que se están ejecutando en un sistema determinado utilizando herramientas como NMAP para la recolección

de datos, que luego se comparan con información sobre vulnerabilidades almacenada en la Base de Datos Nacional de Vulnerabilidades (NVD).

Este antecedente destaca la importancia de utilizar enfoques sistemáticos para la detección de vulnerabilidades, subrayando que herramientas como UdeCEscaner no solo optimizan el proceso de análisis, sino que también minimizan el impacto sobre los sistemas evaluados al evitar interacciones excesivas con los servicios activos. La implementación de este tipo de soluciones puede ser un punto de partida significativo para nuevas investigaciones orientadas a mejorar la seguridad de las redes en entornos educativos y empresariales.

Luis R, José V y Luis G[8] realizaron un estudio único que se concentra en el diseño y aplicación de una estrategia integral para la identificación de vulnerabilidades en redes de datos, la cual ha sido y fue refinada a un contexto particular, como la red de datos de la Unidad de Negocios de Apoyo Logístico de la Empresa de Construcción y Montaje de Pinar del Río. Este estudio enfatiza la necesidad de estructurar etapas críticas (evaluación, ejecución e informes) hacia la identificación y remediación de vulnerabilidades, asistido por herramientas y software especializados que aseguren que se obtienen los resultados correctos. La aplicación práctica de este marco realmente funcionó, ya que pudo detectar varias vulnerabilidades en la red objetivo, demostrando claramente su valor como herramienta técnica y un instrumento para mejorar la seguridad de la información en diferentes entornos organizativos.

1.3 Fundamentación teórica

1.3.1 Tecnologías de la Información y Comunicación (TIC)

Las TIC, o Tecnologías de la Información y la Comunicación, comprenden una serie de herramientas y recursos tecnológicos utilizados para procesar, modificar y transmitir información. Esto incluye el uso de computadoras y software que facilitan la creación, almacenamiento, protección y recuperación de datos.

Estas tecnologías no solo se limitan a equipos modernos, sino que también abarcan medios tradicionales de comunicación, como la radio, la televisión y el teléfono. Desde

una perspectiva más amplia, las TIC combinan la digitalización y los sistemas tradicionales, lo que permite su aplicación en diversos entornos, como las zonas rurales, donde estos medios convencionales aún desempeñan un papel clave mientras se adopta gradualmente el internet[9]. Las Tecnologías de la Información incluyen las actividades de adquisición, creación, conservación, procesamiento y difusión de información, sin tener en cuenta el medio o formato empleado, y tienen una importancia clave en la sociedad contemporánea[10].

1.3.2 Sistema de Detección y Prevención de Intrusiones (IDPS)

Es un sistema que integra la detección y prevención de intrusiones, permitiendo registrar dentro de la red accesos no autorizados o actividades sospechosas en redes y sistemas reaccionando de manera proactiva bloqueando amenazas en tiempo real. Este tipo de herramientas trabaja como componente clave en la seguridad empresarial, monitoreando el tráfico, generando alertas ante anomalías y colaborando con otros controles para mitigar vulnerabilidades y prevenir ataques[11]. El sistema IDPS se utiliza para proteger redes y sistemas de posibles vulnerabilidades y ataques como el malware, ataques de denegación de servicios (Dos), entre otros.

1.3.3 Implementación de Software

La implementación de software se refiere a la ejecución de una solución de software donde el software es instalado, configurado y desplegado en un entorno de producción. Este proceso podría incorporar varias etapas como planificación, diseño, pruebas de aceptación del usuario y capacitación del usuario. Al ejecutar la implementación, el software en cuestión debe adecuarse con todos los otros programas dentro de la organización, cumplir con las expectativas del cliente u organización y asegurar que el sistema pueda ser operado y mantenido durante un largo período de tiempo[12].

La implementación puede realizarse por cuatro métodos:

a. Método directo

Se reemplaza el sistema anterior por uno nuevo de forma inmediata. Este cambio implica un alto nivel de riesgo, ya que, en caso de que surjan fallos, no hay posibilidad de revertir al sistema previo y será necesario realizar ajustes sobre la marcha.

b. Método paralelo

El sistema antiguo y el nuevo operan simultáneamente hasta que el nuevo demuestra ser confiable. Aunque es de bajo riesgo, implica costos elevados por el personal y equipo necesario, por lo que se aplica solo cuando una falla sería muy grave.

c. Método piloto

Se prueba el nuevo sistema en una sección de la organización y, tras confirmar su eficacia, se extiende al resto. Este método es más económico que el paralelo, pero conlleva mayor riesgo, aunque controlado al restringirse a áreas específicas sin impactar a toda la empresa.

d. Método de fases

El sistema se implementa de manera progresiva al dividir el proceso en etapas o fases que se desarrollan de forma consecutiva en un periodo de tiempo determinado. Cada fase debe ser completada con éxito antes de avanzar a la siguiente, siguiendo este procedimiento hasta llegar a la etapa final.

1.3.4 Seguridad Informática

Es la protección de la información almacenada en sistemas informáticos, asegurando que no sea robada, copiada, alterada ni destruida por personas no autorizadas. La seguridad informática abarca tanto aspectos lógicos, como la implementación de firewalls y protocolos de comunicación, como físicos, que incluyen la protección de los sistemas mediante salas de servidores y respaldos de datos. Además, es fundamental la educación de los usuarios para prevenir vulnerabilidades derivadas del desconocimiento o mal uso de las políticas de seguridad[13].

La protección en el ámbito informático requiere encontrar un equilibrio adecuado entre la inversión, la complejidad de las medidas adoptadas y los riesgos a los que se

enfrenta. Aunque no se puede lograr una seguridad absoluta, al aplicar estas ideas y establecer planes de contingencia, las empresas pueden reducir las amenazas y operar de forma más segura.

1.3.5 Normativas y Políticas de Ciberseguridad

Son directrices, regulaciones y estándares establecidos para proteger los activos digitales de una organización contra amenazas cibernéticas. Estas políticas definen las responsabilidades y procedimientos para el manejo seguro de la información y el uso de los sistemas tecnológicos. Abarcan áreas como el control de acceso, la protección de datos, la gestión de incidentes de seguridad, y el cumplimiento de las leyes y regulaciones de protección de datos (por ejemplo, GDPR). Estas normativas aseguran que las organizaciones sigan buenas prácticas de seguridad y cumplan con los requisitos legales y regulatorios para la protección de la información.

1.3.6 Gestión de Red

Consiste en coordinar y supervisar todos los elementos y servicios que forman parte de una infraestructura de red. Esto incluye actividades como analizar el rendimiento para prevenir o resolver inconvenientes, configurar y mantener dispositivos como routers, switches y firewalls, y aplicar protocolos de seguridad para proteger la integridad de la información y asegurar la continuidad del funcionamiento. También implica planificar mejoras, regular el flujo de tráfico en la red para maximizar la eficiencia y garantizar que todos los componentes operen de manera sincronizada. Su objetivo principal es garantizar que la red sea segura, eficaz y capaz de adaptarse a las demandas de los usuarios[14].

La gestión de red se divide en cinco áreas fundamentales.

a. Gestión de fallos

Este proceso implica detectar, separar y supervisar los errores de la red. Se lleva a cabo mediante la vigilancia del funcionamiento de la red. El análisis de notificación y reportes, y la aplicación de métodos predictivos.

b. Gestión de rendimiento

La función está orientada a medir el desempeño del hardware y software de la red. Para ello, se analizan indicadores como el procesamiento, los fallos, el nivel de uso y los tiempos de respuesta, mediante la recopilación y estudio de información sobre la red.

c. Gestión de configuración

Este proceso implica la detección y el despliegue de los dispositivos que supervisan y ajustan el comportamiento de la red.

d. Gestión de contabilidad

La función permite obtener datos detallados sobre el uso de la red, lo que facilita el análisis del consumo de recursos, el monitoreo de su utilización y el control del acceso.

e. Gestión de seguridad

Esta función se centra en salvaguardar la red, sus conexiones y los sistemas asociados, así como la información que maneja. Su propósito es prevenir accesos no autorizados, usos indebidos y otros riesgos.

1.3.7 Vulnerabilidades en el Acceso de la Red

La vulnerabilidad en redes es una debilidad o fallo en los sistemas informáticos que pueden comprometer la protección de los datos. Estas vulnerabilidades pueden ser aprovechadas por atacantes y afectar la integridad, disponibilidad o confidencialidad de la información. Se generan por errores en el diseño, configuración incorrectas o falta de procedimientos adecuados. Es esencial identificarlas y corregirlas para reducir los riesgos[15].

En el acceso de la red puede verse comprometido por diferentes tipos de vulnerabilidades, que pueden agruparse en categorías según su protocolo de comunicación y el tráfico de datos.

a. Vulnerabilidades en los protocolos de red

Son fallas o debilidades en los protocolos utilizados para la comunicación en la infraestructura de red que pueden ser explotadas por ciber delincuentes.

- **Protocolos de autenticación débiles**: Son mecanismos de verificación de identidad que presentan vulnerabilidades, como el uso de contraseñas predecibles, almacenamiento inseguro de credenciales, lo que facilita ataques como el robo de cuentas.

- **Suplantación de identidad en la red:** Es un tipo de fraude en el que un atacante se hace pasar por otra persona en plataformas digitales, redes sociales o sistemas en línea, con el objetivo de engañar, obtener información personal o cometer delitos.

- **Ataques de establecimiento de conexión:** Son ataques que explotan el proceso de conexión en protocolos como TCP, enviando múltiples solicitudes sin completar el proceso, lo que puede saturar los recursos del servidor y provocar una denegación de servicio.

Vulnerabilidades en el análisis y manipulación de trafico

Estas vulnerabilidades permiten a un atacante obtener acceso y controlar el flujo de información dentro de la red. A través de técnicas como la interceptación de paquetes.

- **Ataques Man-in-the-Middle (MITM):** Consiste en que el atacante se interpone entre el cliente y el servidor obteniendo credenciales en una conexión segura[16].

- **Ataques de denegación de servicio (DoS/DDoS):** Este tipo de ataque provoca la interrupción del servicio al sobrecargar sus recursos, lo que conlleva una disminución drástica en su rendimiento y un aumento exponencial de anomalías en su funcionamiento.

- **Sniffing de tráfico:** Es un software diseñado para capturar y analizar el tráfico de datos en una red. Este programa intercepta y almacena toda la información que pasa a través de la red, con el propósito de someterla a un análisis posterior.

1.4 Objetivos

1.4.1 Objetivo general

Implementar un Sistema de Detección y Prevención de Intrusiones (IDPS) para Mitigar Vulnerabilidades en el Acceso a la Red de la Unidad Educativa 'Pio López'.

1.4.2 Objetivos específicos

- Seleccionar el IDPS más adecuado para las necesidades de la institución.
- Identificar las vulnerabilidades existentes dentro de la Unidad Educativa "Pio López"
- Configurar el IDPS, asegurándola correcta identificación y prevención de ataques informáticos en la red de la institución.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para el presente proyecto de investigación dentro de la Unidad Educativa “Pio López” se emplearon herramientas que facilitaron una mejor comprensión del panorama dentro de la red institucional como primero se realizó una encuesta a los docentes y una entrevista al rector de la institución educativa.

2.1.1 Entrevista al rector de la ¨Unidad Educativa Pio López¨

Con el propósito de conocer la gestión de la seguridad informática en la institución, se llevó a cabo una entrevista al rector de la unidad educativa. Esta conversación se centró en aspectos clave como la protección de datos, las prioridades institucionales en materia de ciberseguridad, los recursos destinados a esta área, incidentes pasados, y la percepción sobre la implementación de un sistema de detección y prevención de intrusos (IDPS).

Asimismo, se abordaron temas relacionados con las medidas de seguridad existentes, la frecuencia de auditorías, el nivel de conciencia de la comunidad educativa sobre los riesgos en la red, y la viabilidad económica de fortalecer la infraestructura de seguridad informática. Las respuestas obtenidas, presentadas en la Tabla 6, permitieron identificar con claridad el estado actual de la seguridad informática en la institución, así como las posibles áreas de mejora.

2.1.2 Encuesta dirigida a los docentes de la “Unidad Educativa Pio López”

Con el propósito de conocer el nivel de conocimiento y las percepciones de los docentes de la Unidad Educativa Pío López en relación con la seguridad informática, se diseñó y aplicó una encuesta estructurada, como se detalla en el Anexo A. La información recopilada mediante este instrumento resulta fundamental para el diseño

de estrategias orientadas a fortalecer la protección de los datos institucionales y promover buenas prácticas de seguridad cibernética en el ámbito educativo.

2.1.3 Ficha de observación

Tabla 3. Ficha de observación.

N° Ficha: 01	**Hora:** 10:45 AM – 13:00 PM		
	Ubicación: Huachi Grande La Libertad		
Fecha de Observación: 10 de abril, 2025	**Responsable:** Brayan Alomaliza		
ASPECTOS POR OBSERVAR	**SI**	**NO**	**OBSERVACIÓN**
Observar si la institución tiene un sistema de monitoreo que muestra todos los dispositivos conectados, como servidores, estaciones de trabajo, impresoras, etc.		X	La institución no cuenta con un sistema de monitoreo debido a la falta de presupuesto, lo cual limita la capacidad para rastrear dispositivos conectados a la red.
Observar si la institución cuenta con herramientas automáticas de escaneo de puertos y si están programadas para hacer escaneos de red de manera periódica		X	No existen herramientas de escaneo de puertos definidas en la institución. La falta de esta herramienta impide la identificación temprana de vulnerabilidades o accesos no autorizados a la red.
Observar si se han implementado sistemas de protección de red (firewalls, IDS/IPS) y si están configurados correctamente para detectar y prevenir accesos no autorizados.		X	No se han observado sistemas de protección de red implementados dentro de la institucion.
Verificar si los datos sensibles de los estudiantes están respaldados de forma regular y segura, y si existen procedimientos establecidos para restaurarlos en caso de un incidente.		X	La mayoría de la información de los estudiantes se guarda en memorias USB y en laptops personales de los docentes, lo que representa un riesgo significativo para la seguridad y la integridad de los datos
Verificar si la institución tiene configuradas actualizaciones automáticas para sistemas operativos y aplicaciones clave, garantizando que los dispositivos estén protegidos con los últimos parches de seguridad.		X	La falta de personal capacitado ha resultado en la desconexión de las computadoras del laboratorio debido a la falta de actualizaciones.
Verificar si existen políticas institucionales que garanticen el uso de contraseñas seguras y autenticación de dos factores (2FA) para acceder a sistemas críticos.	X		Se ha constatado que existe un sistema de autenticación de dos factores (2FA) para acceder a los correos institucionales y a los sistemas educativos, lo cual refuerza la seguridad en el acceso
Conclusiones: La institución presenta deficiencias en seguridad informática, como la falta de un sistema de monitoreo, herramientas de escaneo de puertos y protección de red (firewalls, IDS/IPS). Los datos sensibles de los estudiantes se almacenan de manera insegura en memorias USB y laptops personales, y la falta de actualizaciones automáticas deja los dispositivos vulnerables.			

2.2 Métodos

2.2.1 Modalidad de la investigación

La presente investigación se centra en la modalidad de investigación de campo y bibliográfica-documental.

a. Investigación Bibliográfica-Documental

El trabajo de investigación abarco el enfoque bibliográfico-documental, ya que se recopilo y analizo la información proveniente de tesis, artículos científicos, revistas, libros, base de datos académicos y documentación técnica relacionada con el tema. El objetivo de este análisis se centró en las publicaciones más relevantes para el campo de la seguridad informática.

b. Investigación Experimental

El estudio tuvo un enfoque práctico, al realizar pruebas y análisis de diferentes herramientas y estrategias para detectar fallos en la red y crear un sistema contra intrusos. Se hicieron ensayos controlados para comprobar su funcionamiento, ajustando las configuraciones según los resultados obtenidos. Este método ayudó a verificar si el sistema funcionase correctamente en un ambiente real, asegurando soluciones que no solo fueran conceptualmente correctas, sino también útiles y eficientes para proteger la seguridad digital en la Unidad Educativa "Pio López".

c. Investigación de Campo

Se enfoco en la recopilación de información directa en el entorno institucional mediante la evaluación del estado actual de la red, incluyendo entrevista al rector de la unidad educativa “Pio López” como encuestas a los docentes. Esto permitió tomar decisiones fundamentadas para mejorar la red institucional.

2.2.2 Población y muestra

El proceso de recolección de datos se realizó considerando incluir a todo el personal dentro de la población de estudio. Esta determinación se debe a que la cantidad de individuos es reducida, con solo 19 miembros, lo que facilita su análisis. Al abarcar a la totalidad de empleados, se logra una visión más completa y fiel de la realidad de la unidad educativa "Pio López", fortaleciendo la validez y relevancia de los resultados. Asimismo, esta decisión minimiza posibles sesgos en la selección, garantizando una representación equitativa de la población. En la Tabla 4 se detalla la población seleccionada.

Tabla 4. Población de estudio.

Población	**Número**	**Porcentaje**
Director	1	5,26%
Docentes	18	94,74%
Total	19	100%

2.2.3 Recolección de información

Se realizo una entrevista al director encargado de la institución para conocer aspectos relevantes de la seguridad informática dentro de la red.

Tabla 5. Entrevista al rector de la institución.

Datos personales **Institución: Unidad Educativa "Pío López"** **Apellido y Nombre: López Aguilar Edisson Efraín** **Cargo: Director de la Institución**			
Nº	**Pregunta**	**Respuesta**	**Observación**
1	**¿Qué importancia le asigna la institución a la protección de datos y la seguridad cibernética?**	La institución asigna una importancia considerable a la protección de datos y la seguridad cibernética, dado que existen múltiples formas de acceder a los datos o de comprometer archivos valiosos. Estos archivos son cruciales para nuestra actividad diaria, ya que contienen información sensible, como calificaciones y registros académicos.	
2	**¿Qué aspectos de la seguridad informática son prioritarios dentro de la institución?**	Dentro de la institución, se considera prioritario asegurar todos los dispositivos informáticos que se utiliza a diario, como routers, computadoras y tabletas. Estos equipos son fundamentales para las actividades docentes y son utilizados constantemente por los miembros del personal académico.	
3	**Qué tan seguro considera que es el entorno informático de la institución**	Considero que el entorno informático de la institución no es completamente seguro. A pesar de que existe cierta seguridad, en general se percibe como medianamente protegido, ya que la red es accesible a diversos usuarios sin restricciones adecuadas.	
4	**¿Qué recursos se están destinando actualmente para mejorar la seguridad informática?**	Actualmente, no se han destinado recursos específicos para mejorar la seguridad informática. La institución depende exclusivamente del apoyo brindado por el Ministerio de Educación, que solo proporciona el servicio básico sin medidas adicionales de protección.	

Nº	Pregunta	Respuesta	Observación
5	**¿Ha habido incidentes de seguridad informática significativos en la institución en el pasado?**	No se han registrado incidentes de seguridad informática significativos, aunque se ha reportado el caso de cuentas de docentes que fueron clonadas.	
6	**¿Cuál es su opinión sobre la implementación de una herramienta que ayude a detectar y bloquear automáticamente posibles ataques informáticos?**	La información que se maneja, como los datos de los estudiantes y sus calificaciones, es sumamente valiosa. Aunque algunos docentes mantienen copias de seguridad, otros no lo hacen, lo que aumenta el riesgo de pérdida de datos importantes.	
7	**¿Qué impacto espera obtener la institución con la implementación de una herramienta que ayude a detectar y bloquear automáticamente posibles ataques informáticos?**	La implementación de dicha herramienta sería altamente beneficiosa, ya que permitiría confiar plenamente en la red, eliminando la preocupación por la pérdida de datos o el daño a la información.	
8	**¿Sabe si en la institución utilizan programas para proteger las computadoras y la red, como antivirus o sistemas para bloquear accesos no autorizados?**	No, la institución no emplea programas especializados para proteger las computadoras y la red. Se utilizan antivirus básicos en los equipos, pero estos no son lo suficientemente efectivos para garantizar una protección adecuada.	
9	**¿Con qué frecuencia se realizan pruebas para asegurarse de que el sistema está protegido contra posibles riesgos?**	No se realizan pruebas de seguridad periódicas, ya que no cuenta con los recursos o la posibilidad de implementarlas.	
10	**¿Alguna vez ha notado problemas de seguridad en la red de la institución, como dificultades para acceder, mensajes sospechosos o información expuesta?**	En varias ocasiones he escuchado sobre problemas de seguridad en la institución, como dificultades para acceder a ciertos sistemas o incidentes relacionados con ataques informáticos o fallos de seguridad.	
11	**¿Ha escuchado de algún caso en la institución donde alguien haya tenido problemas con su computadora o información debido a un ataque o error de seguridad?**	Sí, considero que la comunidad educativa está consciente de los peligros presentes en la red.	
12	**¿Considera que la comunidad educativa está adecuadamente consciente de los peligros que existen en la red?**	Sí, en algunas ocasiones se ha informado sobre problemas relacionados con ataques informáticos o errores de seguridad que han afectado a computadoras o la información de los usuarios.	
13	**¿Qué valor le asigna a la cooperación con expertos externos en ciberseguridad?**	Le asignó un alto valor, ya que la colaboración con expertos externos sería de gran ayuda para mejorar la protección de los datos de la institución.	

Nº	Pregunta	Respuesta	Observación
14	**¿Considera que los recursos económicos actuales permiten la incorporación de un sistema de detección de intrusos?**	No, la institución no dispone de los recursos económicos necesarios para implementar un sistema de detección de intrusos. Solo se cuentan con los fondos proporcionados por el Ministerio de Educación, que lamentablemente no están destinados a mejorar la seguridad informática.	
15	**¿Existen medidas de seguridad para responder a incidentes de seguridad informática?**	No, actualmente no existen medidas específicas para responder a incidentes de seguridad informática en la institución.	
Conclusiones:			

a. Encuesta a docentes.

Pregunta 1: ¿Con qué frecuencia cree que los datos sensibles de la institución (información de estudiantes, investigaciones, etc.) están en riesgo de ser comprometidos?

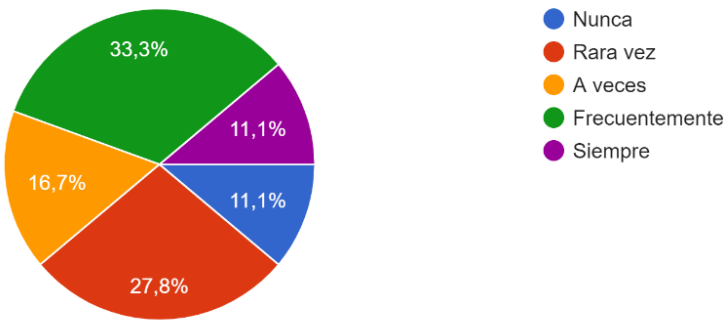


Figura 1. Datos de la pregunta 1.

Análisis e interpretación de resultados

De acuerdo con los resultados de la Figura 1, el 33,3% considera que los datos están frecuentemente en riesgo, lo que refleja una preocupación constante por la seguridad. Un 27,8% opina que los datos están rara vez en riesgo, lo que sugiere una precesión de vulnerabilidades ocasionales. Un 16,7% cree que los datos están a veces en riesgo, mientras que un 11,1% considera que los datos nunca están en riesgo, esto indica una fuerte preocupación por la seguridad de la información sensible.

Pregunta 2: ¿Qué tan preocupado/a esta por la posibilidad de que si cuenta de usuario sea hackeada o utilizada para ataque cibernéticos?

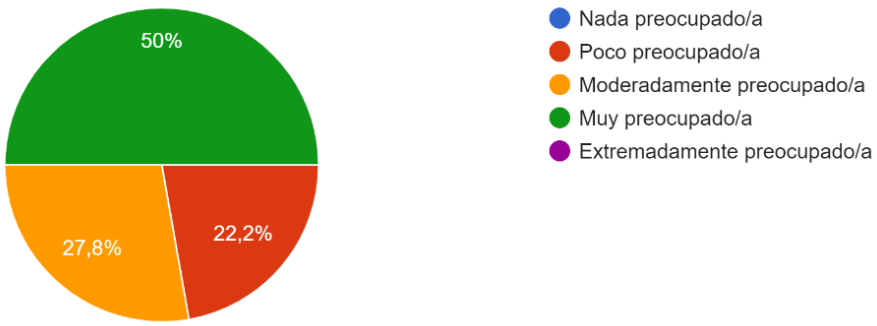


Figura 2. Datos de la pregunta 2.

Análisis e interpretación de resultados

Según los resultados que se muestran en la Figura 2, un 50% de los encuestados se considera muy preocupante por el tema, lo que indica una alta inquietud. Un 27,8% se siente moderadamente preocupado, lo que sugiere que hay una preocupación, pero no tan intensa. El 22,2% restantes se clasifica como poco preocupado, reflejando una menor preocupación al respecto.

Pregunta 3: ¿Considera que los dispositivos que utiliza para trabajar (computadoras, teléfonos, etc.) son vulnerables a ataques cibernéticos?

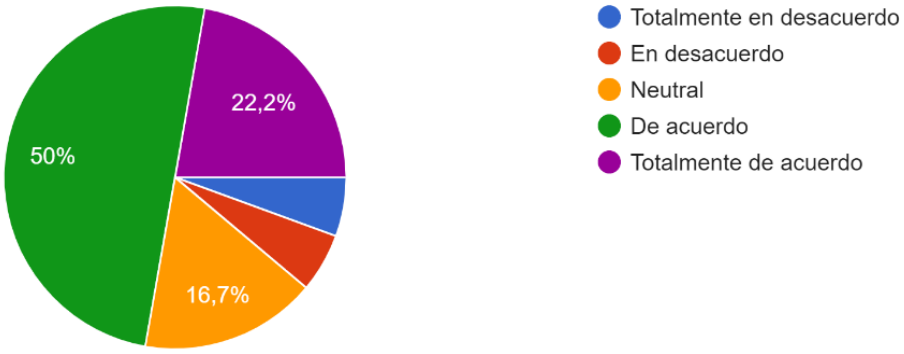


Figura 3. Datos de la pregunta 3.

Análisis e interpretación de resultados

Según los resultados que se muestran en la figura 3, 50% de los encuestados considera que sus dispositivos son vulnerables a ataques mientas que un 22,2% están totalmente de acuerdo con esta afirmación. Un16,7% se muestra neutral, sin tomar una postura clara, mientras que 5,6% no está de acuerdo y el otro 5,6% está totalmente en desacuerdo, indicando que hay una mayoría significativa percibe un riesgo cibernético.

Pregunta 4: ¿Alguna vez ha experimentado un incidente de seguridad informática (phishing, malware, etc.) en su entorno laboral?

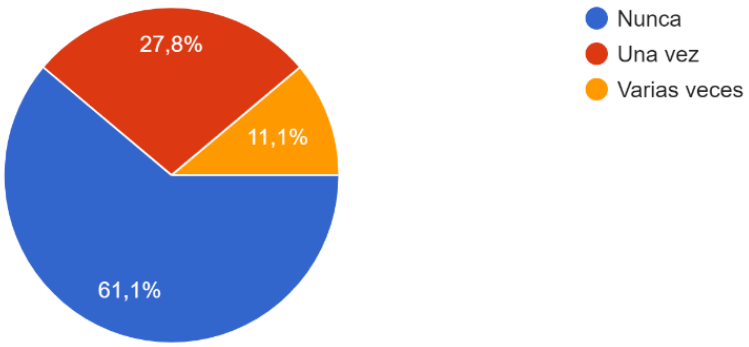


Figura 4. Datos de la pregunta 4.

Análisis e interpretación de resultados

Los resultados que se muestran en la Figura 4, revela que un 61,1% nunca ha tenido este tipo de incidente. Un 27,8% de los encuestados ha experimentado un incidente por lo menos una vez, mientras que un 11,1% ha enfrentado este tipo de problemas varias veces. Estos resultados sugieren que, aunque la mayoría no ha sido afectada por incidentes de seguridad, una parte significativa ha tenido alguna experiencia, ya sea ocasional o recurrente, con amenazas cibernéticas en su entorno laboral.

Pregunta 5: ¿Qué tan satisfecho/a estuvo con la respuesta de la institución ante el último incidente de seguridad que experimentó (si aplica)?

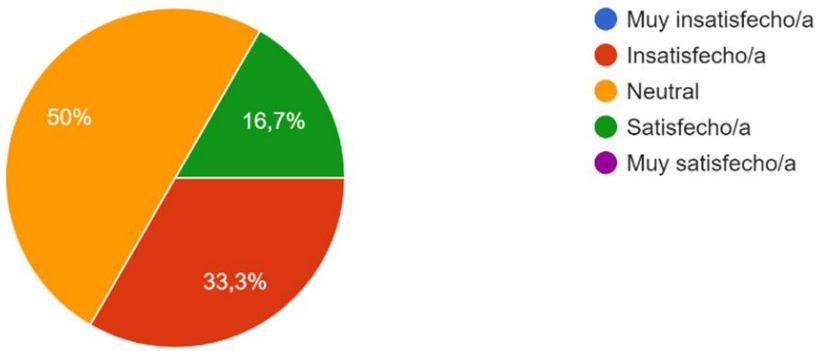


Figura 5. Datos de la pregunta 5.

Análisis e interpretación de resultados

Los resultados que se muestran en la Figura 5, indica que el 50% de los encuestados se muestra neutral respecto a las respuestas recibida. Un 33,3% se muestra insatisfecho, lo que indica una percepción negativa de la gestión del incidente. Por otro lado, un 16,7% se siente satisfecho, lo que sugiere que un pequeño porcentaje considera que la respuesta fue adecuada.

Pregunta 6: ¿Con qué frecuencia recibe correos electrónicos sospechosos (phishing) en su cuenta institucional?

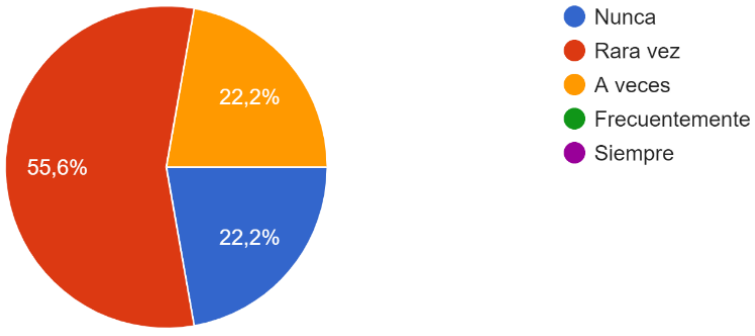


Figura 6. Datos de la pregunta 6.

Análisis e interpretación de resultados

Los resultados que se muestran en la Figura 6, el 55,6% de los encuestados recibe correos electrónicos sospechosos (phishing) raras veces, mientras que el 22,2% nunca los recibe. Un 22,2% adicional indicó que los recibe a veces. Estos datos sugieren que, aunque los intentos de phishing no son constantes, siguen ocurriendo con frecuencia suficiente como para requerir medidas de seguridad adicionales.

Pregunta 7: ¿Qué tan bien informado/a se siente sobre las políticas de seguridad informática de la institución?

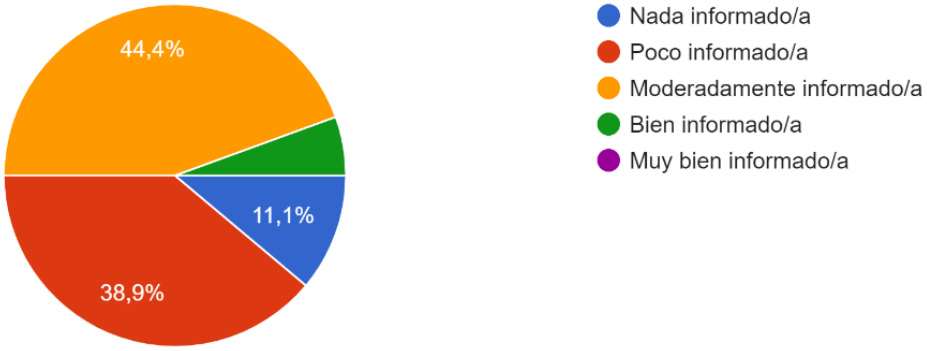


Figura 7. Datos de la pregunta 7.

Análisis e interpretación de resultados

Los resultados que se muestran en la Figura 7, un 44,4% de los encuestados se siente moderadamente informado, mientras que un 38,9% se considera poco informado. Solo el 5,6% de los participantes se siente bien informado, y un 11,1% manifestó estar nada informado. Estos resultados sugieren que existe una gran área de mejora en cuanto a la difusión y claridad de las políticas de seguridad.

Pregunta 8: ¿Considera que ha recibido suficiente capacitación sobre cómo proteger la información y prevenir ataques cibernéticos?

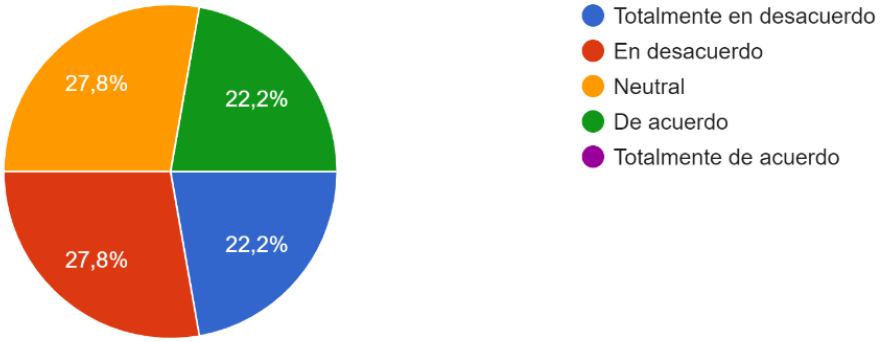


Figura 8. Datos de la pregunta 8.

Análisis e interpretación de resultados

En base al análisis que se muestran en la Figura 8, se puede apreciar que un 27,8% de los participantes se consideran neutrales, si bien no tienen una postura, reconocen cierto nivel de capacitación. Un 22,2% está de acuerdo con la capacitación recibida sobre las materias de la protección de la información y prevención de ataques cibernéticos. Sin embargo, un 27,8% expreso estar en desacuerdo con la capacitación recibida. Finalmente, el 22,2% restante se manifestó totalmente en desacuerdo, lo que señala una clara insatisfacción con los recursos o el contenido de la capacitación recibida.

Pregunta 9: ¿Cree que la implementación de un sistema de detección de intrusiones (IDPS) mejoraría la seguridad de la información en la institución?

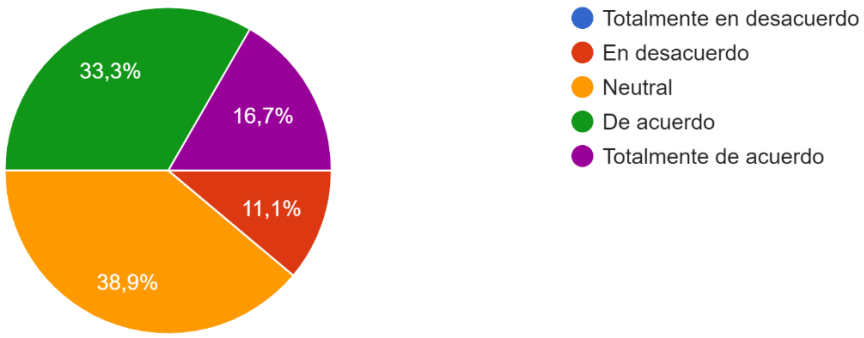


Figura 9. Datos de la pregunta 9.

Análisis e interpretación de resultados

En base al análisis que se muestran en la Figura 9, se puede apreciar que un 33,3% de los encuestados considera que la implementación de un IDPS mejoraría la seguridad, lo que indica una actitud positiva hacia la idea. Sin embargo, un 38,9% se muestra neutral, lo que sugiere que, aunque no se oponen completamente, no están convencidos de la efectividad del sistema. Un 11,1% se mostró en desacuerdo con la propuesta, mientras que el 16,7% restante está totalmente en desacuerdo, indicando que algunos perciben que la implementación de un IDPS no tendría un impacto en la seguridad de la institución.

Pregunta 10: ¿Con qué frecuencia cree que la red de la institución es vulnerable a ataques cibernéticos o accesos no autorizados?

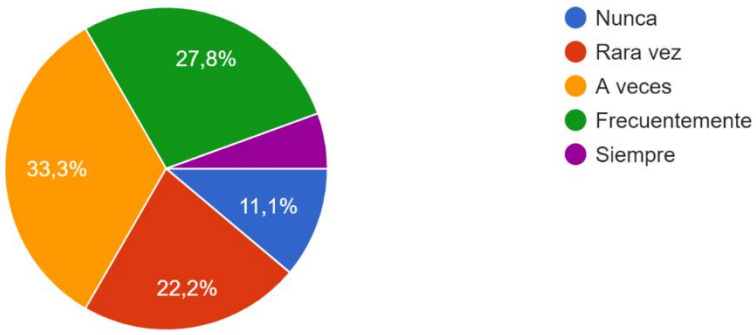


Figura 10. Datos de la pregunta 10.

Análisis e interpretación de resultados

Según los resultados que se muestran en la figura 10, el 33,3% de los encuestados cree que la red es vulnerable a veces, mientras que un 27,8% considera que es vulnerable frecuentemente. Un 22,2% opina que la red es vulnerable raras veces, y solo un 5,6% piensa que la red es vulnerable siempre. Finalmente, un 11,1% cree que nunca es vulnerable. Estos datos indican una percepción generalizada de riesgo, lo que sugiere la necesidad de reforzar la seguridad de la red.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

Antes de presentar los resultados, es importante señalar que el desarrollo de este proyecto se guio bajo los principios de la norma internacional ISO/IEC 27001, la cual establece los lineamientos para la gestión de la seguridad de la información mediante un Sistema de Gestión de Seguridad de la Información (SGSI). Esta metodología no solo proporcionó un marco normativo reconocido internacionalmente, sino que también permitió estructurar de forma ordenada y coherente las actividades desarrolladas a lo largo del proyecto. Dichas actividades se organizaron en torno a cuatro componentes fundamentales del ciclo de mejora continua: planificación, implementación, verificación y actuación. En la etapa de planificación se realizó el análisis de la red, la identificación de activos críticos y la evaluación de riesgos. La fase de implementación abarcó el despliegue técnico del sistema IDPS, la selección de herramientas adecuadas y la adaptación de la infraestructura tecnológica existente. En la fase de verificación se validó el desempeño del sistema, mediante pruebas de funcionamiento y simulación de incidentes, evaluando la capacidad de detección y respuesta del IDPS. Finalmente, en la etapa de actuación, se plantearon propuestas de mejora continúa orientadas a garantizar la sostenibilidad del sistema y se formularon recomendaciones para su mantenimiento y actualización futura. A lo largo del presente capítulo, se discuten los resultados obtenidos en cada una de estas fases, siguiendo la estructura lógica de la norma ISO/IEC 27001 aplicada a un entorno educativo.

3.1.1 Análisis de la infraestructura de red

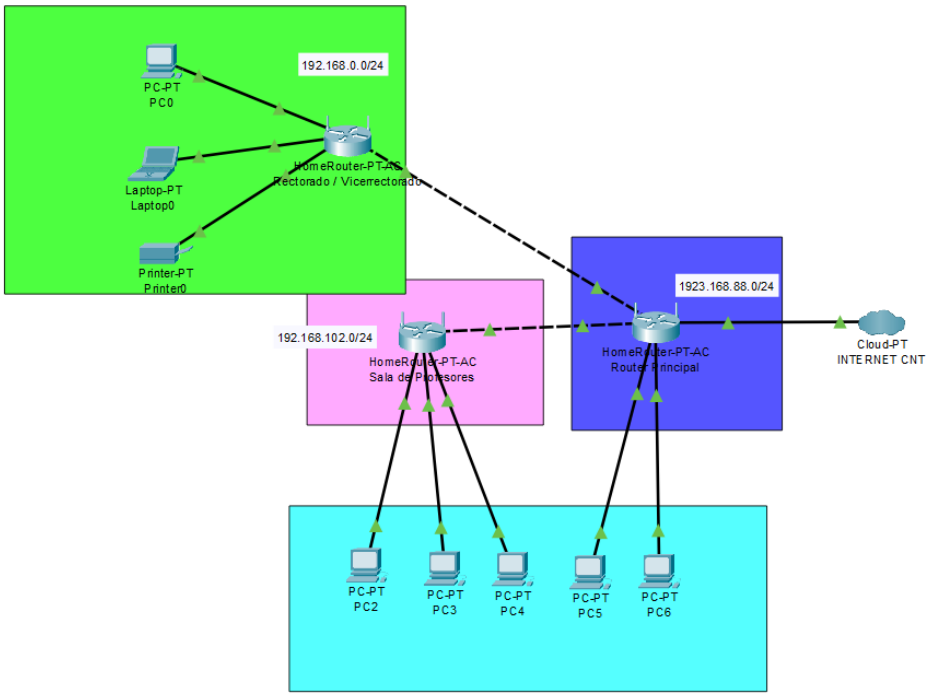


Figura 11. Topología de red de la institucion.

En la Figura 11, se representa la infraestructura de la red institucional de la Unidad Educativa “Pio López”, la institucion trabaja con dos bloques el primer bloque se encuentran los estudiantes de educación básica y en el segundo los estudiantes de bachillerato para esta investigación el escaneo se presentó con mayores resultados en el segundo bloque debido que los estudiantes utilizan con mayor frecuencia los dispositivos tecnológicos.

3.1.2 Identificación de activos críticos

Se identifico cuatro áreas principales que conforman la infraestructura, las cuales se detallan a continuación en la Tabla 6.

Tabla 6. Activos en la Institución.

Área	Cantidad de Dispositivos	Observación
Router Principal	1	El router está ubicado en el laboratorio de computación.
Rectorado / Vicerrectorado	5	En la habitación del rectorado existen dispositivos móviles y un biométrico.
Sala Profesores	10	Dentro de la sala de profesores con dispositivos móviles y laptops portátiles
Laboratorio	7	Dentro del laboratorio se cuentan con siete pc físicas y cuentan con Xtenda X300 que funcionan como un escritorio remoto.

Gestión de Activos y Vulnerabilidades en Sistemas de Información

a. Router Principal

Durante la evaluación de la infraestructura de red de la unidad educativa "Pio López", se identificó que el router principal se encuentra instalado dentro del laboratorio de computación. Se evidenció una falta de seguridad física, ya que el acceso al equipo era directo y sin restricciones. Además, se constató que dos computadoras del laboratorio estaban conectadas directamente al router, lo cual representa un riesgo potencial. La institución no contaba con protocolos de seguridad adecuados, y tras acceder al dispositivo, se detectó que las configuraciones predeterminadas, como el nombre de usuario y la contraseña, habían sido modificadas sin control ni documentación.

b. Sala de Profesores/ Laboratorio

En la unidad educativa, el área destinada a la sala de profesores no cuenta con un espacio exclusivo, por lo que actualmente ocupa el laboratorio de computación. Esto ha generado un acceso generalizado a la red Wi-Fi por parte de todos los docentes, lo que evidencia una falta de control sobre los dispositivos que pueden conectarse. Mediante un escaneo de puertos previo, se identificaron múltiples hosts activos en la red, lo cual refleja una carencia de segmentación y políticas de acceso.

El router asignado a esta área mantiene su configuración por defecto (marca TP-Link), lo que permitió el acceso no autorizado al dispositivo, representando una vulnerabilidad crítica. Se constató la existencia de siete computadoras físicas, las

cuales están conectadas a través de terminales X300 de NComputing para habilitar un entorno de 20 estaciones de trabajo compartidas. Además, se observó que dichos equipos utilizan sistemas operativos obsoletos, como Windows XP, lo cual incrementa significativamente el riesgo de explotación por vulnerabilidades conocidas.

c. Rectorado/ Vicerrectorado

Al igual que en el laboratorio, se identificó que los usuarios se conectaban a la red mediante conexión inalámbrica. Entre los dispositivos destacados se encontraban dos computadoras, una impresora Epson y un equipo biométrico de la marca ZKTime. Este último no contaba con una dirección IP estática, lo que generaba inconvenientes al momento de reinicios por cortes de energía, dificultando la obtención oportuna de los reportes de asistencia del personal docente.

3.1.3 Evaluación de riesgos y amenazas

a. Escaneo con Nmap

Es una herramienta de código abierto utilizado para el descubrimiento de host y servicios en una red. El escaneo se realizó en distintos segmentos de la red en la institucion permitiendo obtener información clave como son.

Direcciones Ip Activas: Se enfocó en las tres áreas principales de la infraestructura de red de la institución, realizando escaneos específicos según los rangos asignados por cada router. El router principal, ubicado en el laboratorio general, opera bajo la red 192.168.88.0/24; el router del laboratorio utilizado por docentes y estudiantes maneja la red 192.168.1.0/24; mientras que el router correspondiente al área de rectorado utiliza la red 192.168.0.0/24.

Puertos abiertos TCP/UDP: Durante el escaneo de la red institucional se identificaron múltiples puertos TCP y UDP abiertos en distintos dispositivos. Esta exposición incluye servicios comunes como HTTP (puerto 80), HTTPS (443), SSH (22), RDP (3389) y otros relacionados con impresoras y terminales remotas.

Sistemas Operativos: Los equipos del laboratorio presentaron sistemas operativos obsoletos, como Windows XP, lo que represento un riesgo significativo para la seguridad de la red institucional debido a la falta de soporte y actualización.

b. Escaneo con OpenVAS

Es una plataforma completa de escaneo de vulnerabilidades que realiza evaluaciones automáticas basadas en una base de datos. A diferencia de Nmap, OpenVas evalúa las posibles vulnerabilidades y las vincula con CVEs conocidos, dentro de la institución educativa se detectaron vulnerabilidades como servicios sin parchar, contraseñas por defectos y protocolos obsoletos (SMBv1)

Los resultados de los escaneos realizados fueron analizados para determinar la gravedad y el alcance de cada vulnerabilidad. Cada hallazgo fue relacionado con su respectivo CVE (Common Vulnerabilities and Exposures) y se documentó el impacto potencial en la integridad, disponibilidad y confidencialidad de la red institucional.

La evaluación de riegos es una etapa clave dentro de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), ya que permite identificar las amenazas que afectan los activos críticos de la organización, valorar sus vulnerabilidades y establecer el nivel de riesgo resultante. Esta valoración se realiza con base en la combinación del impacto que tendría un incidente sobre la confidencialidad, integridad o disponibilidad de la información, y la probabilidad de que dicho incidente ocurra.

En el presente proyecto, se utilizó como referencia la metodología de análisis cualitativo, asignando valores Bajo, Medio y Alto tanto al impacto como a la probabilidad.

El nivel de riego se calculó como el producto de ambas variables y se clasifico en:

Bajo (1-2) aceptable sin medidas adicionales.

Medio (3-4) requiere monitoreo y control.

Alto (6-9) requiere tratamiento inmediato.

A continuación, se presenta la Tabla 7 de evaluación de riesgos más relevantes identificados en la topología de la institución educativa.

Tabla 7. Evaluación de riesgo.

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de riesgo	Clasificación
Red Wi-fi	Suplantacion (spoofing)	Claves débiles	3	2	6	**Alto**
Switch administrable	Intercepción de tráfico	Falta de VLANs o aislamiento	2	3	6	**Alto**
Estaciones de laboratorio	Malware por USB	Sin políticas de control de dispositivos	3	2	6	**Alto**
Router institucional	Escaneo de puertos externo	Firmware desactualizado	2	2	4	**Medio**

La Tabla 7 de evaluación de riesgo se basa en un modelo cualitativo simple, utilizado para la implementación practica de la ISO/IEC 27001. El cálculo del nivel de riesgo se hace multiplicando dos factores impacto por probabilidad.

3.1.4 Clasificación de vulnerabilidades

La clasificación de vulnerabilidades se realizó tomando como referencia el estándar CVSS (Common Vulnerability Scoring System), que valora los riesgos. El resultado del escaneo de OpenVAS ofrece ya una calificación por criticidad como se muestra en la Tabla 8.

Tabla 8. Resumen de Vulnerabilidades.

Vulnerabilidad	Descripción	CVE	Severidad
TCP Timestamps Information Disclosure	Vulnerabilidad de TCP, lo que permite calcular el tiempo de actividad del sistema.	Sin CVE específico	Bajo
ICMP Timestamp Reply Information Disclosure	Vulnerabilidad que responde a solicitudes ICMP, exponiendo datos de tiempo del sistema.	CVE-1999-XXXX	Bajo

Vulnerabilidad	Descripción	CVE	Severidad
SMB/NETBIOS Authentication Bypass	Vulnerabilidad critica de omisión de autenticación a través de SMB/NETBIOS, permitiendo iniciar sesión en el recurso compartido.	CVE-1999-XXX, CVE-1999-XXX, CVE-2002-XXX	Alto
DCE/RPC and MSRPC Enumeration	Vulnerabilidad de consultas al puerto, permitiendo identificar servicios disponibles.	CVE-2021-XXX	Medio
jQuery XSS Vulnerability	jQuery en versiones anteriores a la 1.9.0 es vulnerable a ataques de cross-site scripting (XSS).	CVE-2012-XXX	Medio
Clear Text Authentication Over HTTP	Vulnerabilidad de transmisión de información sensible en texto claro a través de HTTP, exponiendo los datos a posibles ataques.	Sin CVE específico	Medio

Esta clasificación sirvió como base para la creación de reglas personalizadas en Suricata, abordando primero las vulnerabilidades de mayor riesgo dentro de la institución educativa.

3.1.5 Controles de seguridad seleccionados ISO/IEC 27001

Como parte de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001, se realizó una selección de controles de seguridad del Anexo A, versión 2022, que fueran pertinentes al contexto técnico de la organización y a los riesgos identificados previamente. Esta selección fue guiada por el principio de aplicabilidad justificada, tal como establece la norma: no todos los controles deben aplicarse, pero cada exclusión debe estar debidamente sustentada.

Los controles seleccionados pertenecen a los cuatro dominios definidos en la versión actualizada: Controles Organizacionales (A.5), Controles Orientados a las Personas (A.6), Controles Físicos (A.7) y Controles Tecnológicos (A.8). A continuación, se

detallan los más relevantes para la solución técnica basada en un sistema de detección y prevención de intrusos (IDPS) como se muestra en la Tabla 9[17].

Tabla 9. Controles de la norma ISO/IEC 27001.

Código	Control resumido	Aplicación
5.9	Inventario de información y otros activos asociados	Se elaboró un inventario detallado de activos de red dentro de la unidad educativa "Pío López".
5.15	Control de acceso	Se configuraron accesos restringidos en routers, switches y el servidor.
5.24	Gestión de incidentes de seguridad de la información	Se estableció un flujo de respuesta a alertas generadas por Suricata.
5.26	Respuesta a incidentes	El IDPS detecta, alerta y el bloqueo de amenazas dentro de la institución.
5.28	Recolección de evidencia	Los logs generados por Suricata y enviados a ELK son almacenados como evidencia.
8.7	Protección contra malware	Las reglas de Suricata ayudan a detectar patrones de comportamiento malicioso.
8.8	Gestión de vulnerabilidades técnicas	Se usó OpenVAS para detectar vulnerabilidades técnicas.
8.15	Registro	Se registraron eventos de seguridad en tiempo real.
8.16	Actividades de seguimiento	Se utilizó Kibana para monitorear y analizar el tráfico detectado.
8.20	Seguridad de redes	Se reforzó la segmentación, filtrado de tráfico y monitoreo constante.

La implementación de estos controles responde directamente a los resultados del análisis de riesgos, y su objetivo es mitigar o reducir las amenazas detectadas, fortaleciendo la capacidad de detección, monitoreo y respuesta del entorno tecnológico.

3.2 Implementación del sistema IDPS (Fase de Ejecución)

3.2.1 Metodología para el proyecto

La presente investigación se guía bajo los principios de la gestión de la seguridad de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este enfoque se fundamenta en la aplicación de la metodología ISO/IEC 27001, una norma internacional ampliamente reconocida que establece los requisitos para desarrollar, implementar, mantener y mejorar de forma continua un SGSI eficaz dentro del contexto organizacional[17].

La norma ISO/IEC 27001 permite estructurar el tratamiento de la seguridad de la información a través de un enfoque sistemático basado en el ciclo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar). Esta metodología facilita la identificación, análisis y gestión de riesgos asociados a los activos de información, garantizando la confidencialidad, integridad y disponibilidad de los mismos. Durante el desarrollo del proyecto, la aplicación de esta norma permitió realizar un diagnóstico detallado del entorno tecnológico, establecer un inventario de activos críticos, evaluar riesgos potenciales, e implementar controles técnicos[18].

La implementación del sistema de detección y prevención de intrusos (IDPS), como medida técnica dentro del SGSI, responde a la necesidad de fortalecer la capacidad de detección temprana de amenazas, mitigar vulnerabilidades activas y generar alertas que permitan tomar decisiones informadas en tiempo real.

La adopción de la norma ISO/IEC 27001 en esta investigación permitirá establecer una base sólida para la gestión de la seguridad de la información, y además favorecerá la mejora continua mediante la retroalimentación obtenida en las fases de evaluación y prueba del sistema, contribuyendo significativamente a la sostenibilidad del entorno informático institucional.

3.2.2 Diseño de la arquitectura de red

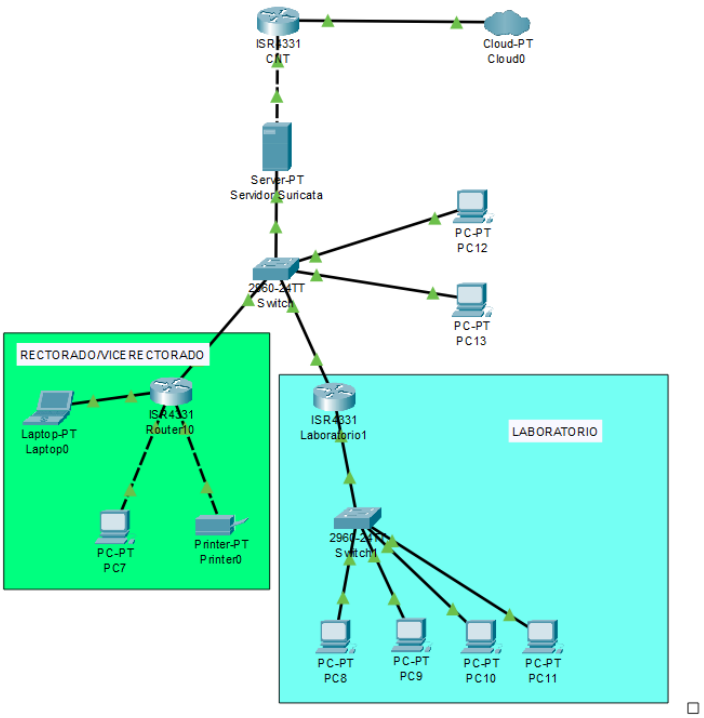


Figura 12. Topología de red.

Durante el proceso de implementación de la infraestructura de red institucional, se realizó el rediseño y optimización de la topología existente con el fin de integrar un sistema de detección y prevención de intrusos (IDPS) de manera eficiente y segura. Como parte central de esta infraestructura, se procedió con la instalación y configuración de un switch administrable Ubiquiti UniFi USW-Flex Mini, cuya función es centralizar la conectividad y facilitar la segmentación lógica del tráfico dentro de la institución educativa.

La ubicación física del equipo fue determinada estratégicamente, considerando factores clave como la seguridad del entorno, la ventilación adecuada y la proximidad a nodos críticos de la red, incluyendo los routers principales de acceso a Internet. El switch fue alimentado mediante una fuente de energía externa dedicada, lo que garantiza estabilidad operativa y minimiza el riesgo de interrupciones.

3.2.3 Selección e instalación de Suricata

Las tecnologías de detección y prevención de intrusiones (IDPS) se clasifican, principalmente, en tres tipos: basadas en host, en red y sistemas híbridos. En el marco del presente proyecto, se ha optado por utilizar un sistema IDPS basado en host, debido a que se adapta mejor a los requerimientos técnicos y operativos de la infraestructura existente[19].

Un IDPS (Intrusion Detection and Prevention System) es una herramienta avanzada de seguridad informática que combina la capacidad de detección de un IDS con mecanismos activos de respuesta ante amenazas. Mientras que un IDS se limita a observar y reportar comportamientos sospechosos, un IDPS actúa de forma inmediata para prevenir ataques, neutralizando vulnerabilidades antes de que afecten la seguridad del sistema[20].

Para llevar a cabo esta implementación, se consideraron diversas soluciones disponibles en el mercado. Dado el presupuesto limitado con el que cuenta la institución educativa “Pío López”, se decidió recurrir a plataformas de código abierto. Estas alternativas permiten acceder a funcionalidades robustas y confiables sin incurrir en los costos que implican las licencias comerciales. Entre las opciones evaluadas, destacan las siguientes:

Suricata: Sistema de detección y prevención de intrusiones (IDPS) de alto rendimiento y de código abierto. Capaz de analizar el tráfico de red, incluyendo inspección profunda de paquetes, detección basada en firmas y análisis de protocolos[21].

Snort: Herramienta de detección de intrusos en red, libre y gratuito. Se basado en red, implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía en tiempo real[22].

Zeek: Framework de análisis de red gratuito y de código abierto, diseñado para fortalecer la seguridad de los sistemas mediante la identificación y prevención de actividades maliciosas. encargado de analizar en tiempo real los eventos de red y alertar sobre accesos no autorizados o comportamientos sospechosos [23].

Tabla 10. Comparativa de software IDS/IPS[24].

Fundamento	Suricata	Snort	Zeek
Enfoque principal	Detección análisis de intrusos, de tráfico en tiempo real, y captura de datos	Detección de intrusos basado en firmas	Análisis profundo del tráfico de red y monitoreo comportamiento
Detección	Basado en firmas y análisis del comportamiento (detección múltiple)	Basados principalmente en firmas (patrones conocidos de ataques)	Análisis basado en comportamiento y eventos
Rendimiento	Soporta alta velocidad, ideal para grandes redes de trafico	Adecuado para redes medianas y grandes, pero puede sufrir bajo alta carga.	Adecuado para análisis profundo, pero con mayor uso de recursos.
Capacidad de inspección	Inspección de trafico de red a nivel de capa de aplicación, soporte para DPI (Deep Packet Inspection)	Inspección a nivel de paquetes, limitado en cuanto a DPI en capas superiores.	Inspección profunda de sesión y conexiones, con enfoque en análisis a nivel de aplicación.
Velocidad	Muy eficiente en el análisis de tráfico a alta velocidad (10 Gbps o más)	Menor rendimiento que Suricata en entornos de alta trafico	No esta optimizado para alta velocidad, enfoca en análisis detallado.
Actualización de firmas	Soporte para firmas de Snort, más actualizaciones propias.	Aplica base de firmas, actualizaciones frecuentes.	No depende de firmas, sino de políticas de comportamiento.
Facilidad de uso	Amplias capacidades, pero con curva de aprendizaje moderado debido a sus múltiples funciones.	Relativamente fácil de configurar y usar, especialmente para detección basada en firmas.	Requiere mayor conocimiento técnico y personalización
Documentación y comunidad	Excelente documentación, activa comunidad de soporte y contribuciones.	Documentación sólida, muy popular y bien respaldado por la comunidad	Documentación técnica extensa, comunidad académica y profesional activa.

Una vez analizado las características de los diferentes softwares de detección y prevención de intrusiones, se decidió utilizar Suricata debido a su capacidad en el análisis de tráfico lo que resulta esencial para mitigar las vulnerabilidades presentes en la unidad educativa “Pío López”. Su arquitectura multihilo nativa permite aprovechar al máximo los recursos del sistema, ofreciendo un rendimiento superior en entornos con alto volumen de tráfico.

La elección de Suricata como solución de seguridad dentro del presente proyecto responde a su capacidad para abordar no solo amenazas conocidas mediante firmas, sino también comportamientos anómalos a través del análisis de tráfico. Este enfoque

combinado fortalece la capacidad de detección, ofreciendo una protección más efectiva contra ataques desconocidos. Esto es especialmente importante en entornos académicos, donde los métodos de ataque pueden variar constantemente.

A diferencia de Snort, que se basa principalmente en reglas ya definidas, y Zeek, que orienta el análisis a investigación forense, Suricata es una herramienta practica para entornos productivos, capaz de analizar en tiempo real y adaptarse dinámicamente a nuevas amenazas. Esta adaptabilidad se ve reforzada por su compatibilidad con firmas de Snort lo que nos permite mantener una política de reglas de seguridad actualizadas sin depender de una sola fuente.

Su arquitectura multihilo garantiza un rendimiento óptimo en redes de alta velocidad, lo que lo convierte en una herramienta adecuada para instituciones que proyectan un espacio de equipos informáticos. Suricata tiene una flexibilidad para la visualización de tráfico que facilita la correlación de eventos en tiempo real. Suricata ofrece una capacidad de abierta de implementación de nuevas reglas personalizadas que permiten mitigar riesgos específicos detectados en la infraestructura de red, fortaleciendo así la seguridad del entorno institucional[25].

En este sentido, Suricata representa una inversión tecnológica estratégica combinando eficacia operativa, escalabilidad y potencial de integración con tecnologías avanzadas, garantizando así una solución alineada tanto con los requerimientos técnicos del presente como con las proyecciones de crecimiento institucional a mediano plazo.

a. Implementación y Configuración de Suricata como IDPS

Para la implementación y configuración de Suricata como sistema de detección y prevención de intrusiones. Se detalla la instalación de Ubuntu Server en un equipo físico. Adicional se integraron herramientas para la visualización avanzada de datos como son los ELK Stack con Elasticsearch, Kibana, Filebeat la actualización del sistema operativo, la configuración básica de red y los paquetes necesarios posteriores a la instalación de Suricata todo esto se detalla en los Anexos C**.**

b. Configuración del entorno de trabajo

Para la configuración inicial del sistema operativo Ubuntu Server en el equipo, Se preparo un dispositivo USB booteable con la imagen ISO utilizando una herramienta de creación de medios de instalación. Una vez listo, se procedió a acceder a la BIOS del equipo destinado para el servidor, donde se configuro la prioridad de arranque, estableciendo la unidad USB como primer dispositivo. Esto permitió iniciar el proceso de instalación del sistema directamente desde el medio extraíble. Dentro de la instalación se escogió el idioma en la cual se va a trabajar luego se configuro la distribución del teclado en inglés y fuero configuradas según las opciones se eligieron según la compatibilidad de hardware disponibles y las necesidades del entorno del proyecto.

Se configuró la red, eligiendo entre DHCP o IP estática según los requerimientos de conectividad. No fue necesario configurar un proxy, por lo que se mantuvieron las opciones predeterminadas para asegurar la conexión directa con los servidores oficiales de Ubuntu[26].

Se revisó el resumen de las particiones y se continuó con la instalación. Para usuarios que requieran un esquema de almacenamiento personalizado, se sugiere consultar la documentación oficial de Canonical, como se detalla en el Anexo B. En el apartado de la Figura 13, se creó un usuario principal, se asignó una contraseña segura y se definió el nombre del host del servidor. Se habilitó el servicio OpenSSH para permitir la administración remota del sistema. Se omitió la suscripción a Ubuntu Pro y, tras completar la instalación, se reinició el equipo[26].

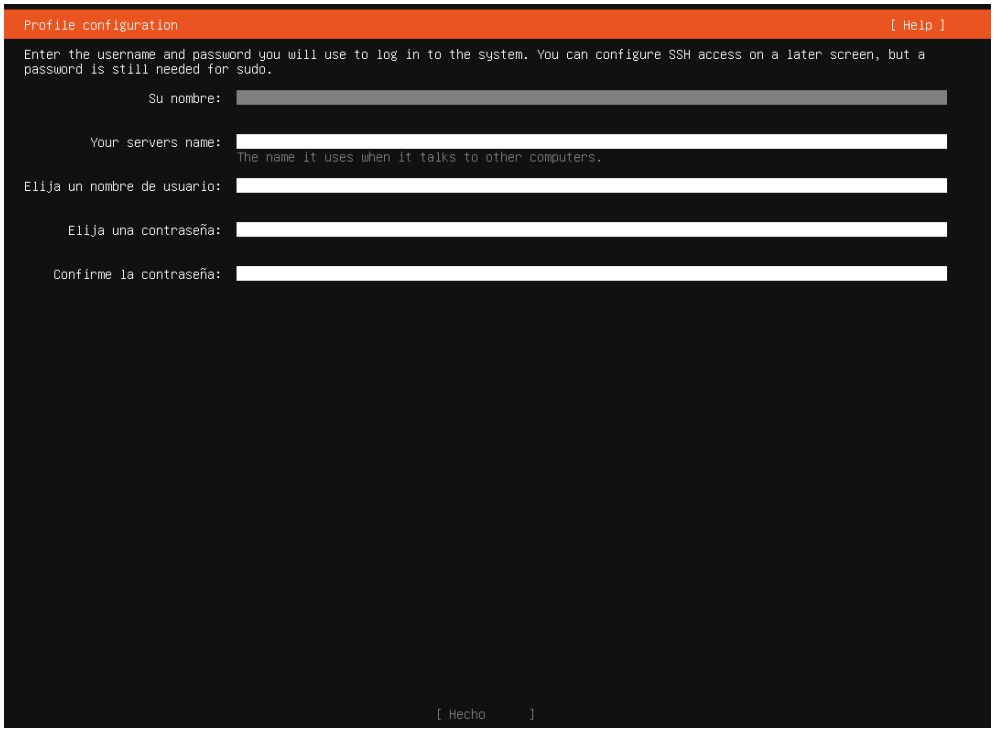


Figura 13. Configuración del perfil.

c. Configuración de herramienta para detección de comportamientos anómalos en la red

Una vez completada la instalación del sistema operativo, se procedió con la instalación y configuración de las herramientas necesarias para llevar a cabo el monitoreo de la red institucional, comenzando con Suricata. Como paso inicial, se consideró fundamental actualizar el sistema para garantizar la instalación de paquetes recientes y evitar posibles conflictos. Para ello, se accedió al modo superusuario utilizando el comando *'sudo su'*. A continuación, se actualizó la lista de paquetes disponibles mediante *'apt update'*, y luego se realizó la actualización de los paquetes ya instalados con el comando *'apt upgrade -y'*. Con el sistema debidamente actualizado, se procedió a instalar Suricata utilizando el comando *'apt-get install suricata'*, como se muestra en la Figura 14. Este paso marcó el inicio de la preparación del entorno de monitoreo, sobre el cual se configuraron posteriormente los parámetros necesarios para su correcto funcionamiento dentro del Anexo C [27].

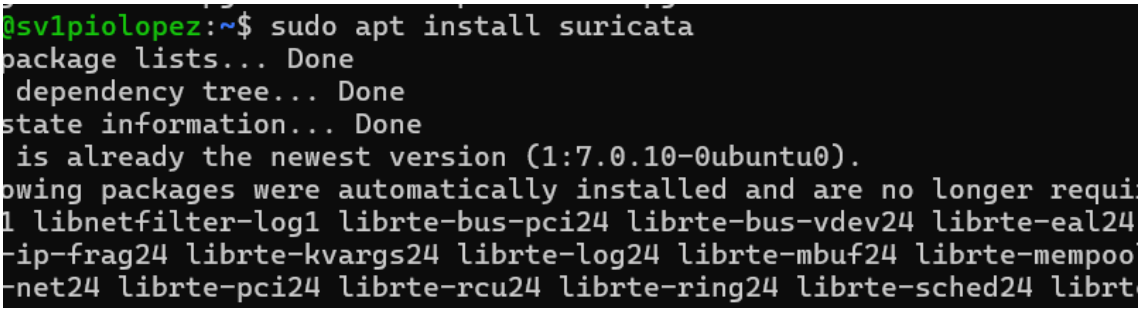


Figura 14. Instalación de Suricata.

3.2.4 Configuración de reglas personalizadas

Dentro del proceso de configuración de Suricata, fue necesario crear un archivo de reglas personalizado en la ruta correspondiente al repositorio de reglas del sistema, ubicada en *'/var/lib/suricata/rules'*. En este directorio, se generó un archivo con extensión .rules, el cual se utilizó para registrar las reglas específicas basadas en las vulnerabilidades detectadas previamente mediante el escaneo realizado con OpenVAS. Estas reglas fueron redactadas de forma manual, tomando como referencia los resultados obtenidos, con el fin de permitir que Suricata identifique y reaccione ante patrones de tráfico relacionados con dichas vulnerabilidades. La creación y edición de este archivo se realizó cuidadosamente, como se ilustra en la Figura 15, asegurando su correcta integración con el motor de detección de Suricata para su funcionamiento efectivo dentro de la red institucional. Para una mejor comprensión y referencia, el contenido detallado de las reglas utilizadas puede consultarse en el Anexo E de este documento.

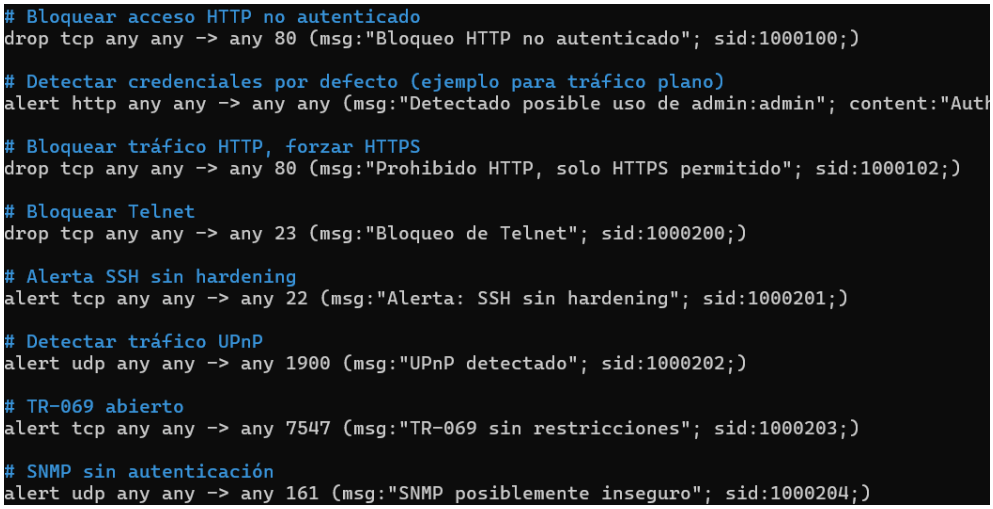


Figura 15. Reglas de suricata.

Finalmente, se modificó el modo de operación, habilitando el funcionamiento como IPS en lugar de IDS como se muestra en la Figura 16, lo cual permitió no solo la detección de tráfico malicioso, sino también su bloqueo en tiempo real. Estos cambios fueron esenciales para asegurar que Suricata operara de forma efectiva, brindando una capa adicional de protección activa dentro del sistema de seguridad implementado, esto se detalla más en el Anexo C [27].

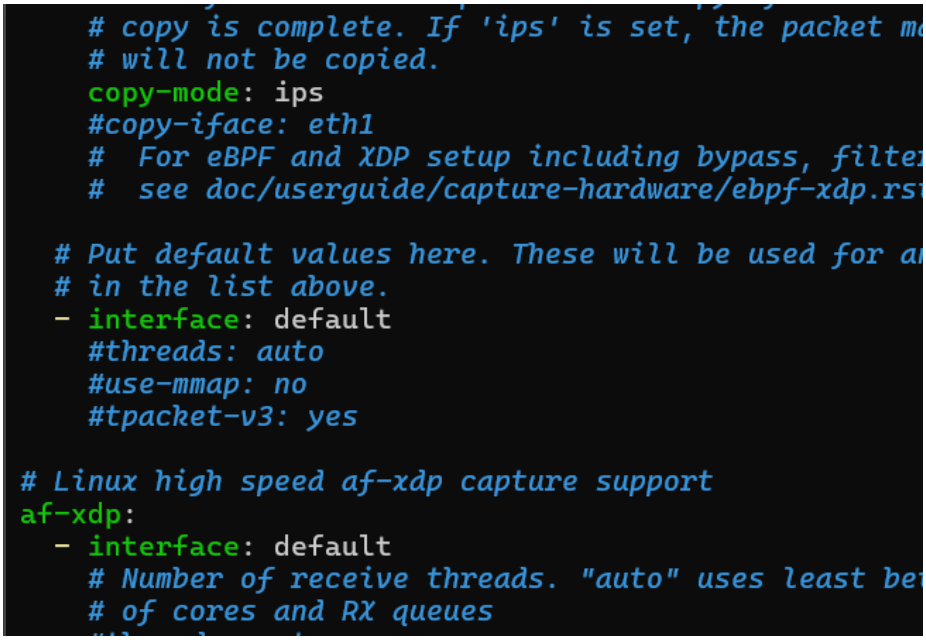


Figura 16. Editor de archivos de suricata.

3.2.5 Integración con ELK Stack para monitoreo

La integración de Suricata con el ELK Stack se realizó para facilitar el monitoreo y análisis en tiempo real del tráfico de red. Este proceso implicó la instalación y configuración coordinada de varias herramientas que permiten la captura, procesamiento y visualización de datos generados por el sistema de detección de intrusiones[28].

Se procedió con la instalación de Filebeat para la recolección eficiente de logs generados por Suricata, y de Logstash para el procesamiento y transformación de dichos datos antes de ser almacenados en Elasticsearch. La configuración de estos componentes fue esencial para garantizar el flujo continuo y seguro de la información hacia la plataforma de análisis. Para detalles específicos de comandos, archivos de configuración y despliegue, se remite al Anexo D [29].

La integración de Suricata con el ELK Stack se realizó para facilitar el monitoreo y análisis en tiempo real del tráfico de red. Este proceso implicó la instalación y configuración coordinada de varias herramientas que permiten la captura, procesamiento y visualización de datos generados por el sistema de detección de intrusiones.

Se procedió con la instalación de Filebeat para la recolección eficiente de logs generados por Suricata, y de Logstash para el procesamiento y transformación de dichos datos antes de ser almacenados en Elasticsearch. La configuración de estos componentes fue esencial para garantizar el flujo continuo y seguro de la información hacia la plataforma de análisis. Para detalles específicos de comandos, archivos de configuración y despliegue, se remite al Anexo D.

a. Configuración de Elasticsearch y Kibana

Elasticsearch fue configurado para almacenar y facilitar la búsqueda rápida de los eventos capturados, mientras que Kibana se ajustó para ofrecer una interfaz gráfica amigable, permitiendo la visualización y exploración de los datos a través de dashboards personalizados. Los archivos de configuración principales y las pruebas de

conexión se describen con detalle en el Anexo D, incluyendo la gestión de puertos, autenticación y aseguramiento del servicio[29].

b. Recolección, visualización y análisis de eventos en tiempo real

Con la correcta integración y configuración de Suricata con ELK Stack, se logró la recolección continua y la visualización en tiempo real de eventos de seguridad como se muestra en la Figura 17. Esta capacidad facilita la detección oportuna de amenazas y el análisis detallado de patrones de tráfico, apoyando la toma de decisiones para la gestión de la seguridad en la red institucional. La implementación completa, junto con la documentación visual, está disponible en el Anexo D.

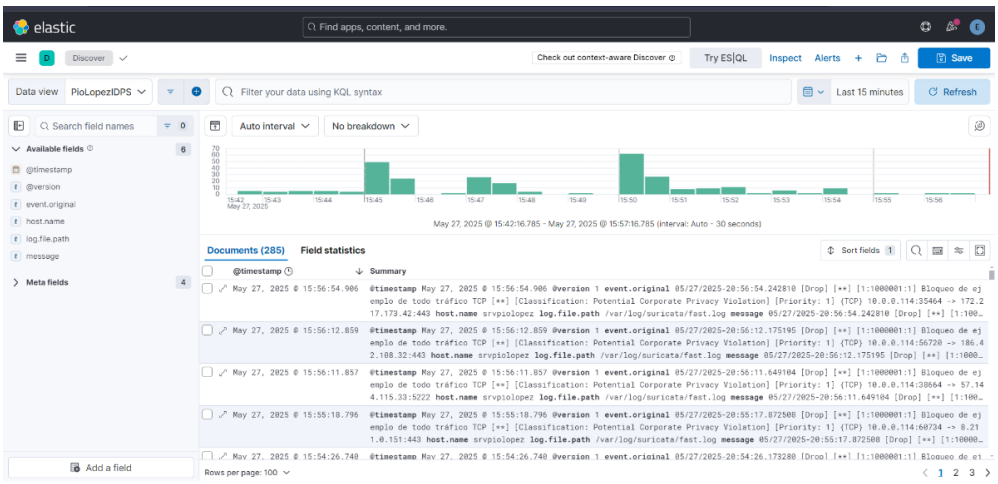


Figura 17. Visualizacion de Logs.

3.2.6 Adaptaciones en la infraestructura física

Para garantizar el correcto funcionamiento del sistema de detección y prevención de intrusiones basado en Suricata, fue necesario realizar ajustes de infraestructura, como solución se realizó una adaptación en la topología física de la red mediante la incorporación de un Ubiquiti UniFi Switch USW Flex Mini administrable, el cual fue instalado como punto central de interconexión. A este switch se conectaron el router principal, los routers secundarios como son el router de rectorado y vicerrectorado al igual que el router del laboratorio, y el servidor Suricata. De esta manera, se centralizó el flujo de datos de la red institucional, permitiendo que Suricata pueda monitorear y analizar el tráfico de todos los segmentos.

Estos cambios no implicaron una reestructuración compleja de la infraestructura, pero sí requirieron:

- La adquisición e instalación de un switch administrable.
- La reorganización física del cableado entre los routers y el nuevo switch central.

Con estas adaptaciones, se logró una integración completa del sistema IDPS, mejorando la visibilidad de la red y asegurando una cobertura integral para la detección de amenazas.

En la Figura 18. presenta el esquema de red del laboratorio, donde fue implementado el servidor IDPS. Para su correcta instalación y funcionamiento, se gestionó el uso de un área específica dentro del laboratorio destinada a la ubicación del switch TP-Link, el cual cumple la función de centralizar el tráfico de red y permitir una supervisión eficiente desde el servidor de seguridad.

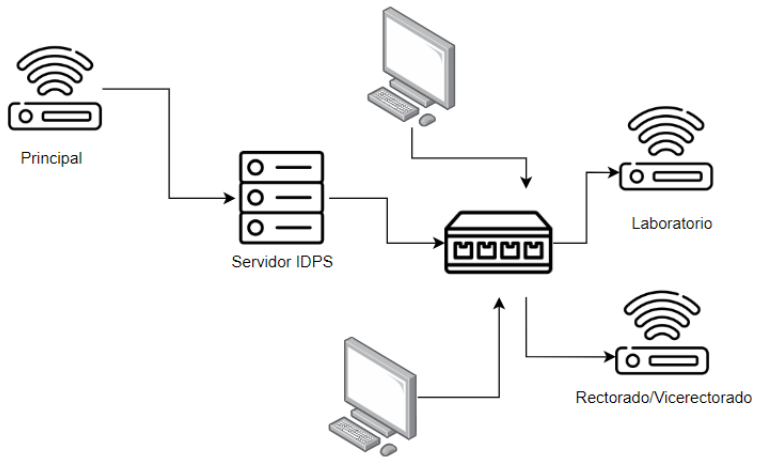


Figura 18. Esquema de red con el switch.

3.3 Evaluación de la eficacia del sistema (Fase de Verificación)

Con el propósito de evaluar la eficiencia del sistema de Detección y Prevención de Intrusos (IDPS), se llevaron a cabo pruebas funcionales en un entorno controlado. Estas pruebas consistieron en la ejecución de diversos tipos de ataques con el fin de simular intentos reales de intrusión y validar la capacidad del sistema para detectarlos y prevenirlos de manera efectiva.

Los ataques seleccionados incluyeron Slowloris, EternalBlue, Denegación de Servicio (DoS) y Man in the Middle (MitM). Dichos ataques fueron lanzados desde un equipo atacante utilizando Kali Linux, el cual se encontraba dentro de la red institucional. Esta configuración permitió simular un escenario realista en el que se buscaba comprometer los recursos tecnológicos de una institución educativa.

Durante las pruebas, se monitoreó detenidamente el comportamiento del IDPS ante cada tipo de amenaza, verificando su capacidad de respuesta, detección oportuna y los mecanismos de mitigación implementados.

3.3.1 Pruebas funcionales del IDPS

Una vez finalizada la implementación del sistema de Detección y Prevención de Intrusos (IDPS), fue necesario comprobar si realmente cumplió protegiendo la red institucional de posibles amenazas. Para ello, se diseñó una fase de verificación que incluyó pruebas funcionales de simulación de ataques, con el fin de analizar las respuestas y compararlas con el estado previo de la red institucional. Este proceso no solo permitió medir la eficiencia del sistema implementado, sino que también genero aprendizaje clave para la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

3.3.2 Simulación de incidentes y análisis de respuesta

Las pruebas de funcionalidad representaron el primer paso para comprender, de manera práctica, como responde el sistema ante posibles ataques. Se realizo en un entorno controlado y seguro, simulando tres tipos de vulnerabilidades desde un equipo con Kali Linux conectado directamente a la red institucional.

Slowloris (Dos HTTP): Este ataque intenta dejar inservible un servidor manteniendo muchas conexiones abiertas durante largos periodos. El sistema generó una alerta, pero no logró bloquear el ataque de inmediato, lo que evidenció la necesidad de ajustar los

parámetros de detección para este tipo de amenazas lentas y sigilosas. La Figura 19 muestra los registros (logs) generados por Suricata.



Figura 19. Registro de log de Suricata.

Asimismo, los eventos recolectados fueron registrados en Elasticsearch (ELK), permitiendo su visualización a través de un panel de control (dashboard), tal como se muestra en la Figura 20.

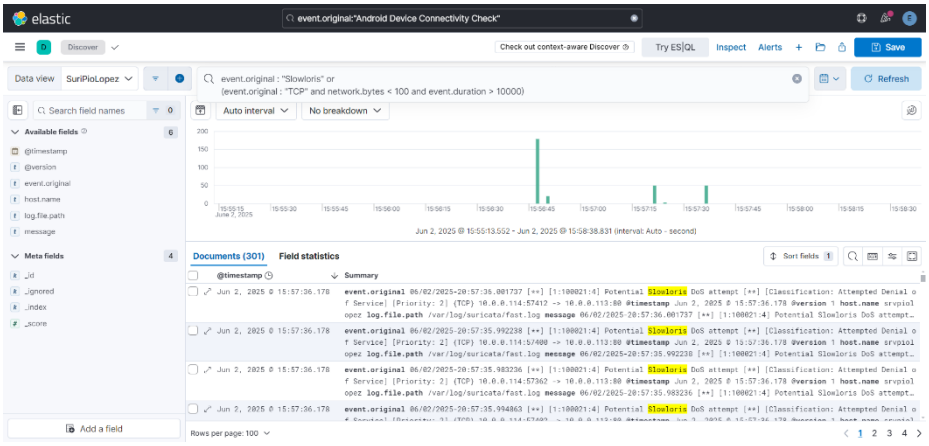


Figura 20. Registro de eventos en elastic.

SYN Flood: Se realizó un ataque de tipo SYN Flood utilizando la herramienta hping3. Inicialmente, al tener las reglas configuradas únicamente con la acción “alert”, los eventos generados por los ataques DDoS fueron registrados, pero no mitigados. Posteriormente, se modificaron las reglas del archivo piolopez2.rules, cambiando la acción de alert a drop, lo que permitió al sistema de prevención de intrusos (IPS) bloquear activamente los paquetes maliciosos. Esta medida contribuye a mitigar la

vulnerabilidad detectada, fortaleciendo la confidencialidad, disponibilidad e integridad de la red de la institución educativa. El ataque simulado se visualiza en la Figura 21.

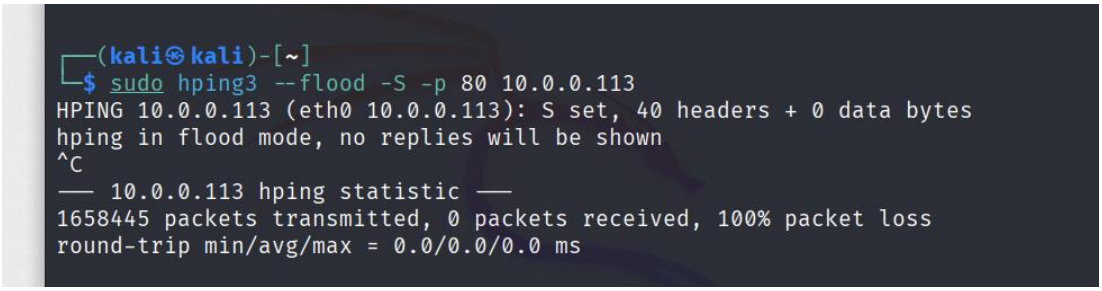


Figura 21. Ataque de utilizando hping3.

Man in the Middle (MitM – ARP Spoofing): Al intentar interceptar el tráfico entre dos dispositivos de la red, el sistema detectó rápidamente la manipulación de tablas ARP y generó alertas precisas en el panel de control (dashboard), como se evidencia en la Figura 22.



Figura 22. Registro del ataque en Elastic.

Estas pruebas permitieron observar el correcto funcionamiento del sistema al detectar los ataques y visualizar los eventos generados por el sistema.

3.3.3 Métricas de desempeño (detección, precisión, tiempo de respuesta)

A partir de las pruebas realizadas, se obtuvieron indicadores clave que permiten medir el desempeño real del sistema

a. Tasa de detección

$$Tasa\ de\ detección = \frac{Ataques\ detectados\ correctamente\ (TP)}{Total\ de\ ataques\ realizados} X100$$

En la evaluación del sistema IDPS se realizaron tres ataques: Slowloris, SYN Flood y MitM. De estos, dos fueron detectados correctamente (SYN Flood y MitM), mientras que el ataque Slowloris solo generó una alerta leve, sin ser bloqueado lo que impidió considerarlo una detección efectiva. Este resultado refleja la capacidad del sistema para identificar ciertas amenazas, pero también señala la necesidad de mejorar su configuración y afinar las reglas de detección para abordar ataques más complejos como Slowlori.

$$Tasa\ de\ detección\ = \frac{2}{3}\ X\ 100 = 66.7\%$$

b. Precisión

La precisión nos permitió evaluar la calidad de las alertas generadas por el sistema IDPS. De esta manera nos indica que alertas emitidas corresponden a amenazas reales y no a falsos positivos.

$$Precisión\ = \frac{Verdaderos\ Positivos\ (TP)}{Verdaderos\ Positivos\ (TP) + Falsos\ Positivos\ (FP)}\ X\ 100$$

- **Verdaderos Positivos (TP):** Son alertas generadas correctamente cuando el sistema detecta ataques reales, como SYN Flood y MitM (Man-in-the-Middle). En ambos casos, la actividad maliciosa fue identificada y el sistema respondió de acuerdo con su configuración de seguridad.
- **Falsos Positivos (FP):** Son alertas incorrectas que se activaron por tráfico legítimo, como sesiones de navegación web prolongadas o solicitudes DNS normales, que fueron interpretadas erróneamente como amenazas.

$$Precisión\ = \frac{2}{2+2}\ X\ 100 = 50\%$$

El sistema logró una precisión del 50%, lo que significa que la mitad de las alertas generadas por el sistema fueron correctas y la otra mitad no correspondían a amenazas

reales. Aunque exista margen de mejora, este resultado se considera aceptable para una primera fase de implementación.

Este porcentaje resalta la necesidad de optimizar las reglas de detección y adaptarlas mejor al entorno de la red institucional, reduciendo la generación de falsos positivos y mejorando la respuesta ante ataques.

c. Tiempo de respuesta

El tiempo de respuesta del sistema IDPS mide cuánto tarda en reaccionar tras detectar una anomalía, ejecutando una acción como bloqueo, alerta o registro.

Para calcularlo, se analizaron los logs de eventos, tomando el tiempo transcurrido entre el primer paquete malicioso detectado y la acción tomada por el sistema.

Los valores de tiempo de respuesta obtenidos fueron:

SYN Flood: Respuesta en 1.1 segundos.

MitM: Respuesta en 2.0 segundos.

$$Promedio = \frac{1.1 + 2.0}{2} = 1.55\ segundos$$

En los casos detectados correctamente, el tiempo transcurrido entre la detección y la acción del sistema fue de aproximadamente 1.55 segundos, lo que demuestra una adecuada capacidad de reacción en tiempo real. Estas métricas, en su conjunto, reflejan un funcionamiento efectivo del IDPS.

3.3.4 Comparación con estado inicial

Previamente a la implementación del sistema IDPS, la red institucional operaba sin herramientas especializadas para la detección o prevención de intrusiones en tiempo real. La seguridad dependía de mecanismos tradicionales, como firewalls convencionales y revisiones manuales de registros, limitando significativamente la capacidad de respuesta ante amenazas. Con la incorporación del IDPS, se logró una protección más activa y automatizada, permitiendo identificar comportamientos sospechosos en el tráfico de red, aplicar reglas de mitigación en el momento de la

detección de una amenaza, y registrar incidentes para facilitar el análisis forense y la mejora continua.

3.4 Mejora continua del SGSI (Fase de Actuación)

Esta fase, correspondiente al último paso del ciclo PHVA (Planificar-Hacer-Verificar-Actuar), se enfoca en la aplicación de acciones correctivas, preventivas y de mejora continua sobre el Sistema de Gestión de Seguridad de la Información (SGSI), fundamentadas en los resultados obtenidos durante la verificación del sistema IDPS [30].

3.4.1 Ajustes realizados tras la implementación

Tras la evaluación de la eficacia del IDPS en un entorno controlado, se identificaron diversos puntos de mejora que fueron corregidos para optimizar su desempeño.

a. ***Optimización de reglas***

Se modificaron umbrales de duración de conexiones y volúmenes de datos para mejorar la detección de ataques lentos como Slowloris, sin afectar el tráfico legítimo.

b. ***Reducción de falsos positivos***

Se configuraron listas blancas (whitelists) para direcciones IP internas confiables y se refinaron reglas para minimizar alertas erróneas asociadas a servicios habituales como DNS y HTTP.

3.4.2 Recomendaciones para la actualización de reglas y políticas

Para garantizar la eficacia a largo plazo del IDPS, se formulan las siguientes recomendaciones:

a. Actualización periódica de firmas y reglas

Configurar el sistema para recibir actualizaciones automáticas de fuentes como Emerging Threats o Snort VRT, y realizar revisiones manuales al menos una vez por mes[31].

b. Alineación con políticas institucionales

Adaptar las reglas del IDPS a las políticas internas de acceso, uso de la red y control de dispositivos externos.

c. Monitoreo de nuevos vectores de ataque

Mantener vigilancia sobre vulnerabilidades emergentes y técnicas de evasión para adaptar las reglas preventivamente.

d. Capacitación continua del personal

Formar a los responsables del SGSI en análisis de tráfico de red, detección de anomalías y gestión de incidentes.

3.4.3 Proyecciones de escalabilidad y mantenimiento

El sistema implementado garantiza escalabilidad y sostenibilidad a mediano y largo plazo.

a. Escalabilidad del sistema

El diseño del IDPS permite la adición de nuevas unidades en diferentes áreas de la red sin comprometer su funcionamiento. Cada unidad opera de forma local, comunicándose con un centro principal de monitoreo.

b. Mantenimiento preventivo

Se recomienda establecer un calendario de mantenimiento estructurado, que contemple la revisión periódica de logs, actualización de software, verificación de sensores y análisis del rendimiento del sistema, con el objetivo de optimizar su funcionamiento y anticipar posibles fallos.

c. Integración con otros sistemas

A futuro, se puede considerar la integración del IDPS con un SIEM (Security Information and Event Management), lo que permitiría una correlación avanzada de

eventos y una mayor inteligencia de amenazas, reforzando la seguridad y eficiencia del sistema[32].

3.4.4 Lecciones aprendidas y sostenibilidad del sistema

Durante el proceso de implementación, pruebas y evaluación del Sistema de Detección y Prevención de Intrusos (IDPS), se identificaron una serie de lecciones clave fundamentales para el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y el aseguramiento de su continuidad en el tiempo.

Se comprobó que la mera instalación de una herramienta tecnológica no garantiza la seguridad. La eficacia del IDPS depende en gran medida de una planificación adecuada, una configuración específica para el entorno y un proceso continuo de ajuste, basado en la observación de eventos reales y simulaciones. Es indispensable dedicar tiempo y recursos de personal capacitado para supervisar, afinar y actualizar regularmente el sistema.

Se evidenció que los entornos educativos presentan una alta diversidad en el tráfico de red, debido a la variedad de dispositivos conectados (PCs, laptops, teléfonos, impresoras, servidores académicos) y la amplitud de servicios utilizados (plataformas educativas, servicios web, videoconferencias, entre otros). Esta heterogeneidad implica que las reglas del IDPS deben ser cuidadosamente calibradas para evitar falsos positivos que interfieran con el funcionamiento normal de los servicios institucionales.

Otro hallazgo importante fue la dificultad que presentan ciertos ataques de tipo lento, como Slowloris, los cuales emplean técnicas de evasión que dificultan su detección mediante reglas genéricas. Este tipo de amenazas requiere configuraciones específicas en el sistema, como umbrales más sensibles y temporizadores adecuados, lo que refuerza la necesidad de realizar pruebas frecuentes para adaptar el sistema a nuevas variantes de ataque.

Asimismo, quedó demostrado que el compromiso institucional es un factor crítico para la sostenibilidad del SGSI. Contar con el respaldo de los niveles administrativos permite la asignación de recursos suficientes, el establecimiento de políticas claras y la promoción de una cultura de seguridad informática entre los usuarios.

La tecnología por sí sola no es suficiente si no se acompaña de concientización, formación continua y apoyo organizacional.

Finalmente, para asegurar la sostenibilidad a largo plazo del sistema, resulta fundamental integrar el monitoreo de seguridad como una función permanente dentro del área de Tecnologías de la Información. Esto requiere definir responsabilidades, contar con personal capacitado, garantizar la actualización constante del sistema y aplicar una estrategia de mejora continua que incluya auditorías, revisión de eventos y adaptación a nuevas amenazas.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- El proyecto logró la implementación exitosa de un Sistema de Detección y Prevención de Intrusiones (IDPS) en la red de la Unidad Educativa "Pio López", demostrando su capacidad para identificar y, en algunos casos, mitigar ataques informáticos comunes. Las pruebas funcionales validaron la operatividad del sistema al detectar con éxito ataques de tipo SYN Flood y Man-in-the-Middle, confirmando su rol esencial en el fortalecimiento de la postura de seguridad de la institución.

- A pesar de la capacidad de detección demostrada, la precisión del 50% y la respuesta incompleta al ataque Slowloris evidencian la necesidad crítica de una optimización continua de las reglas y configuraciones del IDPS. Esto subraya que la eficacia del sistema no reside únicamente en su instalación, sino en la adaptación constante a los nuevos vectores de ataque y a las particularidades del tráfico de red institucional, lo que es fundamental para reducir falsos positivos y mejorar la capacidad de mitigación.

- La incorporación del IDPS transformó la gestión de la seguridad de la red de la Unidad Educativa "Pio López" de un enfoque reactivo y basado en herramientas tradicionales a uno proactivo y automatizado. Esta transición permitió la identificación temprana de comportamientos sospechosos, la aplicación de medidas de mitigación en tiempo real y la generación de registros para análisis forense, lo que representa una mejora sustancial en la confidencialidad, disponibilidad e integridad de la red institucional.

- La experiencia del proyecto resalta que la seguridad informática efectiva va más allá de la mera implementación tecnológica. La sostenibilidad a largo plazo del IDPS y del SGSI en su conjunto depende crucialmente de un enfoque integral que incluya la capacitación del personal, el compromiso de los niveles administrativos para la asignación de recursos, y la integración de un monitoreo

de seguridad permanente. Esto garantiza la adaptación del sistema a un entorno dinámico y la promoción de una cultura de seguridad sólida en la institución.

4.2 Recomendaciones

- Para mejorar la tasa de detección y reducir los falsos positivos, se recomienda establecer un calendario de revisión y actualización periódica de las reglas de Suricata. Esto debe incluir la configuración de fuentes de firmas automáticas (como Emerging Threats o Snort VRT) y revisiones manuales al menos una vez al mes para ajustar umbrales, crear listas blancas y afinar las reglas de detección, especialmente para ataques lentos o evasivos como Slowloris.

- Es fundamental capacitar al personal responsable del SGSI (y potencialmente a otros usuarios clave) en análisis de tráfico de red, interpretación de alertas del IDPS, gestión de incidentes y las últimas tendencias en ciberseguridad. Esto asegurará que el equipo pueda operar, mantener y optimizar el sistema de manera efectiva, además de reaccionar proactivamente ante nuevas amenazas.

- Para una gestión de seguridad más robusta y una mejor inteligencia de amenazas, se recomienda la integración del IDPS con un sistema SIEM. Esto permitirá la correlación avanzada de eventos de seguridad de diversas fuentes, la centralización de logs, la automatización de respuestas a incidentes y una visibilidad unificada de la postura de seguridad de la red.

- Es crucial que la Unidad Educativa "Pio López" formalice y socialice políticas de seguridad de la información que complementen la implementación del IDPS. Estas políticas deben abordar aspectos como el uso aceptable de la red, la gestión de contraseñas, el control de acceso, la respuesta a incidentes y la concientización sobre ciberseguridad. Esto creará un marco de seguridad integral que combine la tecnología con la conducta de los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

[1] B. Castillejos López, C. A. Torres Gastelú, and A. Lagunes Domínguez, "La seguridad en las competencias digitales de los millennials," *Apertura*, vol. 8, no. 2, pp. 54–69, Oct. 2016, doi: 10.32870/ap.v8n2.914.

[2] P. I. Morales-Paredes and P. Medina-Chicaiza, "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.

[3] CASTILLO TUMBACO DALEMBERG ANDRÉS, "Implementación de hacking ético para la evaluación de vulnerabilidades en la red de datos de una institución educativa de nivel primario.," La Libertad, Aug. 2021.

[4] L. Molina, Y. Cevallos, G. Machado, and A. Furfaro, "El enemigo moderno: Ataques DDoS en la capa de red y de aplicación."

[5] Renzo Edú Manrique Huamaní, "ESTUDIO DEL RENDIMIENTO DE SISTEMAS DE DETECCIÓN DE," pp. 46–47, Dec. 2020.

[6] G. A. Mills, D. K. Acquah, and R. A. Sowah, "Network Intrusion Detection and Prevention System Using Hybrid Machine Learning with Supervised Ensemble Stacking Model," *Journal of Computer Networks and Communications*, vol. 2024, Sep. 2024, doi: 10.1155/2024/5775671.

[7] D. A. Franco, J. L. Perea, and L. C. Tovar, "Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios," *Informacion Tecnologica*, vol. 24, no. 5, pp. 13–22, 2013, doi: 10.4067/S0718-07642013000500003.

[8] K.- Linux *et al.*, "334 Editada por el Centro de Información y Gestión Tecnológica," Dec. 2016.

[9] E. Sánchez Duarte, "LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC) DESDE UNA PERSPECTIVA SOCIAL," 2008.

[10] M. Grande De Prado and I. Mayo, "ICT: CONCEPT EVOLUTION AND ATTRIBUTES / TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN," 2016. [Online]. Available: https://es.wikipedia.org/wiki/Tecnolog%C3%ADa

[11] F. DE Sistemas Mercantiles, P. Fernando Espinoza Romero, and I. Freddy Baño, "UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES INFORME FINAL DE TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE 'DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA LA PROTECCIÓN DE LOS SISTEMAS INFORMÁTICOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO CAMPESINA COOPAC' AUTOR," 2013.

[12] M. DE Desarrollo De Software and E. Gabriel Pacienzia, "FACULTAD DE QUÍMICA E INGENIERIA 'FRAY ROGELIO BACON' PONTIFICIA UNIVERSIDAD CATÓLICA ARGENTINA SANTA MARIA DE LOS BUENOS AIRES Cátedra Seminario de Sistemas," Dec. 2015.

[13] JUAN IGNACIO MAURICIO ISLA CORTES, “SEGURIDAD EN REDES INFORMATICAS,” 2005.

[14] Elena María Delgado Senía, “Estudio de una plataforma integrada para la monitorización de alarmas en la gestión de un ISP,” May 2001.

[15] J. R. Serrano, “Trabajo Fin de Grado Análisis de Redes y Vulnerabilidades,” Madrid, Jan. 2024.

[16] A. Jesús, “‘MAN IN THE MIDDLE ATTACKS ON SSL/TLS,’” Jan. 2013.

[17] “Controles ISO 27001: Descripción general de todas las medidas del Anexo A.” Accessed: Jun. 03, 2025. [Online]. Available: https://www.dataguard.com/knowledge/iso-27001-controls-annex-a/

[18] “Controles ISO 27001: cuáles son y qué debes saber para implementarlos.” Accessed: Jun. 03, 2025. [Online]. Available: https://innevo.com/blog/controles-iso27001

[19] “Sistema de detección y prevención de intrusiones (IDPS) - Rapid7.” Accessed: Jun. 03, 2025. [Online]. Available: https://www.rapid7.com/fundamentals/intrusion-detection-and-prevention-systems-idps/

[20] “¿Qué son los sistemas de detección y prevención de intrusos (IDPS)?” Accessed: Jun. 03, 2025. [Online]. Available: https://www.redhat.com/es/topics/security/que-son-los-sistemas-de-deteccion-y-prevencion-de-intrusos-idps

[21] “Inicio - Suricata.” Accessed: Jun. 03, 2025. [Online]. Available: https://suricata.io/

[22] “Snort - Sistema de detección y prevención de intrusiones en la red.” Accessed: Jun. 03, 2025. [Online]. Available: https://www.snort.org/

[23] “El monitor de seguridad de red Zeek.” Accessed: Jun. 03, 2025. [Online]. Available: https://zeek.org/

[24] Jairo Guillermo Lascano Banshuy, “SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) BASADO EN MACHINE LEARNING PARA EL CONTROL DE LA RED EN LA UNIDAD EDUCATIVA ‘19 DE SEPTIEMBRE’ EN LA CIUDAD DE SALCEDO,” Feb. 2025.

[25] Josué Guillermo Balseca Castro, “SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) PARA FORTALECER LA SEGURIDAD INFORMÁTICA EN LA EMPRESA AMBACAR,” Feb. 2025.

[26] “3. Instalación — Documentación de Suricata 8.0.0-rc1-dev.” Accessed: Jun. 03, 2025. [Online]. Available: https://docs.suricata.io/en/latest/install.html#source

[27] “How to Setup a Suricata IPS: Part 1.” Accessed: Jun. 03, 2025. [Online]. Available: https://www.criticaldesign.net/post/how-to-setup-a-suricata-ips

[28] “ELK Stack y Suricata IDS - Hardsoft Security.” Accessed: Jun. 03, 2025. [Online]. Available: https://hardsoftsecurity.es/index.php/2021/11/17/elk-stack-y-suricata-ids/

[29] “How to Setup a Suricata IPS: Integrating Suricata with ELK Stack.” Accessed: Jun. 03, 2025. [Online]. Available: https://www.criticaldesign.net/post/how-to-setup-a-suricata-ips-elk-stack

[30] “¿Cómo llevar a cabo la mejora continua del SGSI?” Accessed: Jun. 05, 2025. [Online]. Available: https://www.isotools.us/2019/01/24/como-llevar-a-cabo-la-mejora-continua-del-sgsi/

[31] “Reglas SNORT , detección de intrusos y uso no autorizado.” Accessed: Jun. 05, 2025. [Online]. Available: https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/

[32] “What is SIEM? | IBM.” Accessed: Jun. 05, 2025. [Online]. Available: https://www.ibm.com/think/topics/siem

ANEXOS

ANEXO A. ENCUESTA A DOCENTES DE LA INSTITUCIÓN

ENCUESTA A DOCENTES DE LA INSTITUCIÓN

ELABORADO POR:
BRAYAN STIVEN ALOMALIZA CHUCA

FORMULARIO DE ENCUESTA

Dirigida a: Docentes de la Unidad Educativa.

Instrucciones: Marcar con una **"X"** la opción que mejor represente su respuesta

1. ¿Con qué frecuencia cree que los datos sensibles de la institución (información de estudiantes, investigaciones, etc.) están en riesgo de ser comprometidos?

(1) Nunca
(2) Rara vez
(3) A veces
(4) Frecuentemente
(5) Siempre

2. ¿Qué tan preocupado/a está por la posibilidad de que su cuenta de usuario sea hackeada o utilizada para ataques cibernéticos?

(1) Nada preocupado/a
(2) Poco preocupado/a
(3) Moderadamente preocupado/a
(4) Muy preocupado/a
(5) Extremadamente preocupado/a

3. ¿Considera que los dispositivos que utiliza para trabajar (computadoras, teléfonos, etc.) son vulnerables a ataques cibernéticos?

(1) Totalmente en desacuerdo
(2) En desacuerdo
(3) Neutral
(4) De acuerdo
(5) Totalmente de acuerdo

4. ¿Alguna vez ha experimentado un incidente de seguridad informática (phishing, malware, etc.) en su entorno laboral?

(1) Nunca
(2) Una vez
(3) Varias veces

5. ¿Qué tan satisfecho/a estuvo con la respuesta de la institución ante el último incidente de seguridad que experimentó (si aplica)?

(1) Muy insatisfecho/a
(2) Insatisfecho/a
(3) Neutral
(4) Satisfecho/a
(5) Muy satisfecho/a

6. ¿Con qué frecuencia recibe correos electrónicos sospechosos (phishing) en su cuenta institucional?

(1) Nunca
(2) Rara vez
(3) A veces
(4) Frecuentemente
(5) Siempre

7. ¿Qué tan bien informado/a se siente sobre las políticas de seguridad informática de la institución?

(1) Nada informado/a
(2) Poco informado/a
(3) Moderadamente informado/a
(4) Bien informado/a
(5) Muy bien informado/a

8. ¿Considera que ha recibido suficiente capacitación sobre cómo proteger la información y prevenir ataques cibernéticos?

(1) Totalmente en desacuerdo
(2) En desacuerdo
(3) Neutral
(4) De acuerdo
(5) Totalmente de acuerdo

9. ¿Qué tan útil le resultan las capacitaciones sobre seguridad informática que ha recibido?

(1) Nada útil
(2) Poco útil
(3) Moderadamente útil
(4) Útil
(5) Muy útil

10. ¿Cree que la implementación de un sistema de detección de intrusiones (IDPS) mejoraría la seguridad de la información en la institución?

(1) Totalmente en desacuerdo
(2) En desacuerdo
(3) Neutral
(4) De acuerdo
(5) Totalmente de acuerdo

ANEXO B. GUIA DE INSTALACION UBUNTU SERVER

GUIA DE INSTALACION UBUNTU SERVER 24.04.2

ELABORADO POR:
BRAYAN STIVEN ALOMALIZA CHUCA

INTRODUCION

Ubuntu Server es una distribución robusta y ampliamente utilizada en entornos de servidores por su estabilidad, seguridad y facilidad de administración.
Es una solución de código abierto mantenida por Canonical, ideal para implementaciones en centros de datos, servicios en la nube, entornos virtualizados y servidores físicos. Esta guía está dirigida tanto a administradores de sistemas como a usuarios con conocimientos básicos de sistemas operativos Linux que deseen realizar una instalación limpia y eficiente del sistema.

REQUISITOS MINIMOS DEL SISTEMA

Los requerimientos mínimos del sistema Ubuntu 24.04.2 son:

- Procesador Doble núcleo de 2 GHz o superior (64 bits recomendado)
- 4 GB de RAM
- 25 GB de espacio libre en disco duro
- Medio de instalación: Unidad USB o DVD (no necesaria si se utiliza virtualización)
- Conexión a internet: Recomendada para actualizaciones y descarga de paquetes adicionales
- Imagen ISO de Ubuntu 24.04.2

INSTALACION Y CONFIGURACION DE UBUNTU SERVER

Para iniciar con la instalación, se preparó una unidad USB booteable con la imagen ISO de Ubuntu Server, empleando una herramienta especializada para la creación de medios de instalación. Posteriormente, se accedió al firmware UEFI/BIOS del equipo físico asignado al servidor, donde se modificó la secuencia de arranque, estableciendo la unidad USB como dispositivo prioritario. Esta configuración permitió que el sistema iniciara desde el medio extraíble, dando paso al proceso de instalación del sistema operativo.

Configuración Inicial

Selecciona un idioma español y daremos “Enter”.

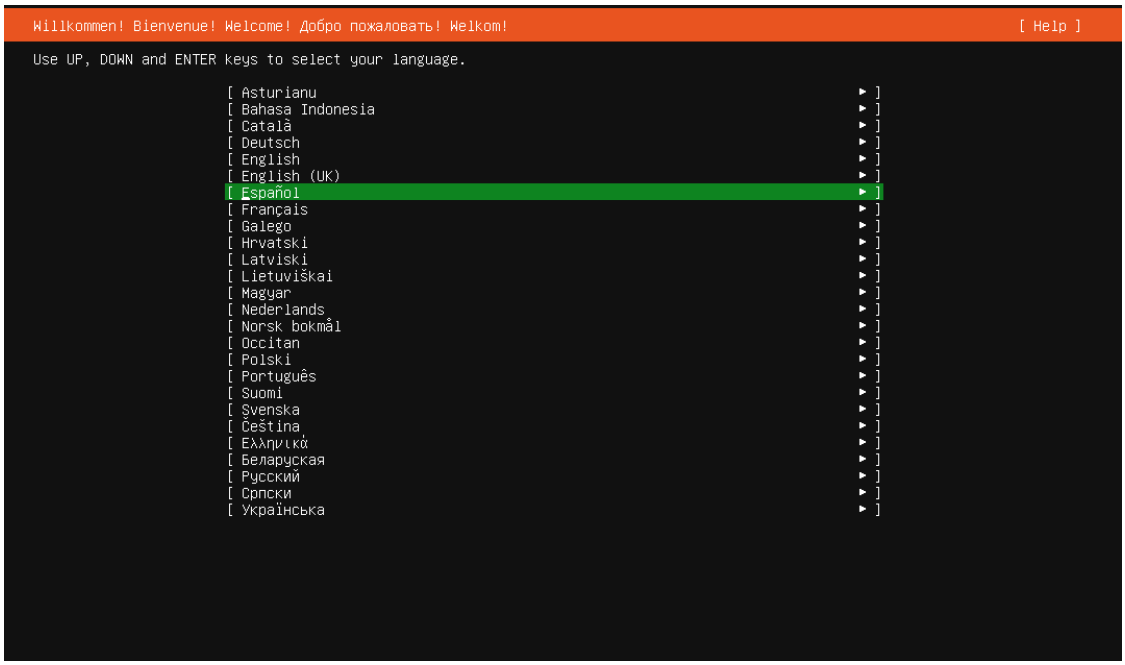


Figura B1. Idiomas del sistema operativo

Durante el proceso de instalación del sistema operativo, se seleccionó el idioma correspondiente al diseño del teclado. En este caso, se eligió la opción 'English' como disposición del teclado. La navegación a través del menú de selección se realizó utilizando las teclas direccionales, y se confirmó la selección presionando la tecla Enter sobre la opción 'Hecho'.

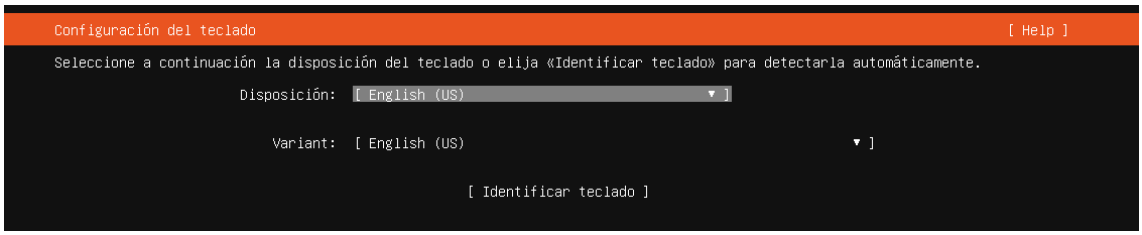


Figura B2. Selección idioma del teclado.

A continuación, se procedió a seleccionar el tipo de instalación. Para este proyecto, se optó por la distribución *Ubuntu Server*, la cual aparece preseleccionada por defecto. Una vez verificada esta opción, se confirmó la selección presionando la tecla Enter sobre la opción 'Hecho'.

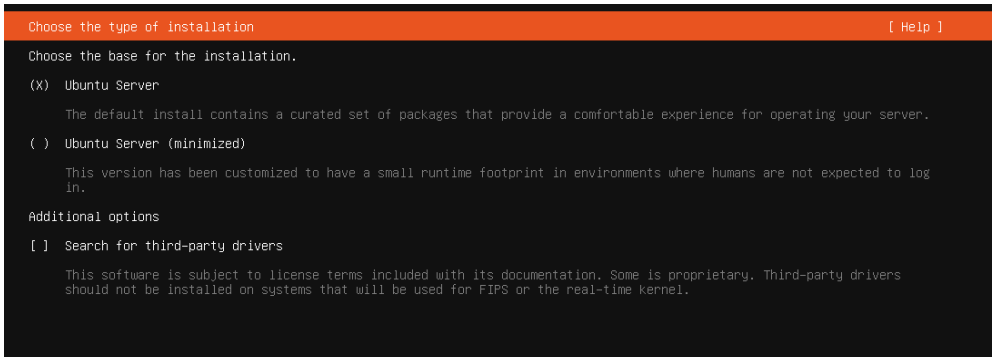


Figura B3. Selección de Ubuntu Server.

TIPO DE CONEXIÓN

En esta etapa, se seleccionó el tipo de configuración de red a utilizar. Se presentó la opción de asignación automática mediante DHCP o configuración manual mediante una dirección IP estática. Según los requerimientos del entorno, se eligió la opción más adecuada y se continuó con la instalación tras confirmar la configuración seleccionada.

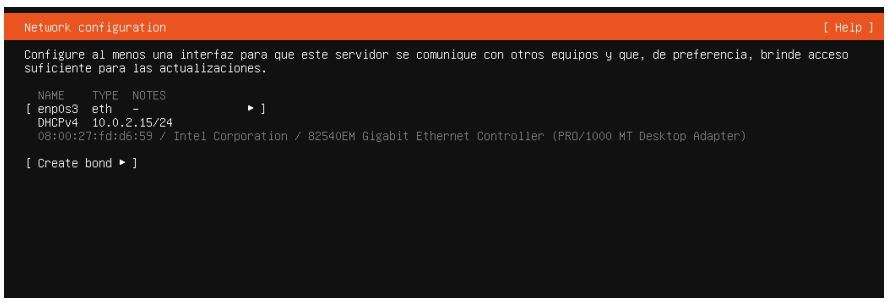


Figura B4. Configuración de red.

No se configuró un servidor proxy ni se utilizó un espejo (mirror) personalizado, ya que la red no requería estas opciones para acceder a los repositorios oficiales. Se mantuvo la configuración predeterminada y se procedió con la instalación seleccionando la opción 'Hecho'.

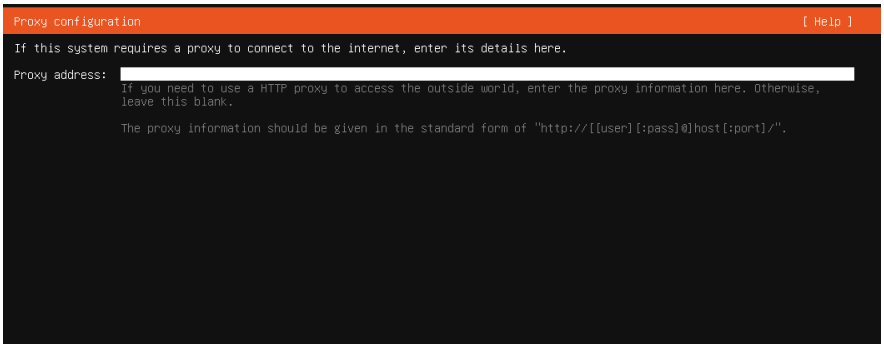


Figura B5. Configuración de Proxy.

En caso de que la red requiriera configuración de proxy para el acceso a Internet, este es el momento oportuno para introducir los parámetros correspondientes. No obstante, al no ser necesario en la infraestructura utilizada, se dejó el campo en blanco y se seleccionó la opción 'Hecho' para continuar con el proceso de instalación.

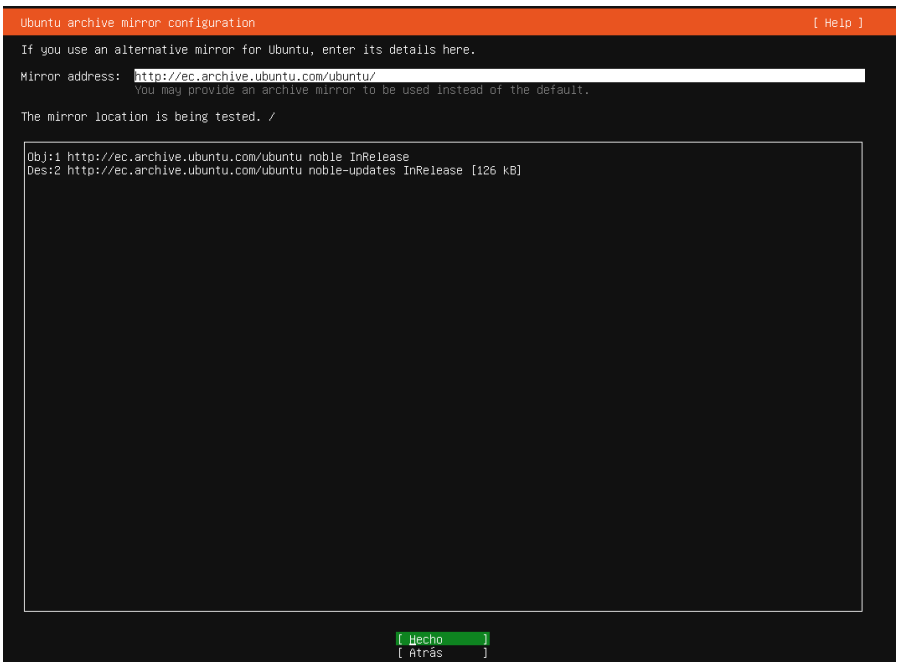


Figura B6. Configuración del espejo de archivo de Ubuntu

En la sección de configuración del almacenamiento, se mantuvieron los valores predeterminados proporcionados por el sistema, ya que estos cumplían con los requisitos del entorno. Una vez verificada esta configuración, se procedió a seleccionar la opción 'Hecho' para continuar con la instalación.

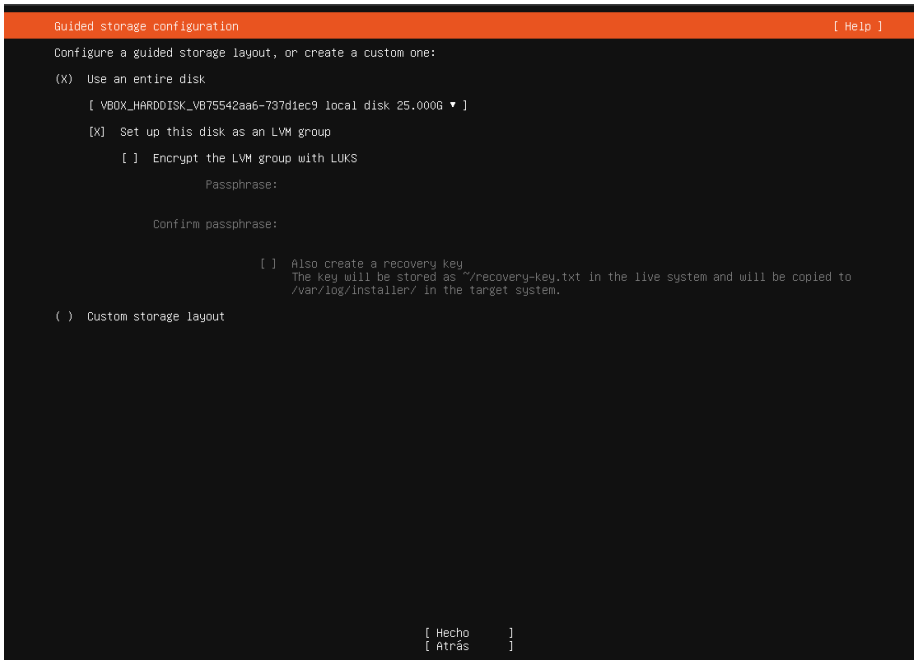


Figura B7. Configuración de almacenamiento

A continuación, se presentó un resumen preliminar de la configuración del sistema de almacenamiento. Estos valores fueron generados por defecto por el instalador. En caso de requerir una partición personalizada, se recomienda consultar la documentación oficial de Canonical en el siguiente enlace y seguir las instrucciones detalladas para la configuración manual del almacenamiento: https://canonical-subiquity.readthedocs-hosted.com/en/latest/howto/configure-storage.html#configure-storage.

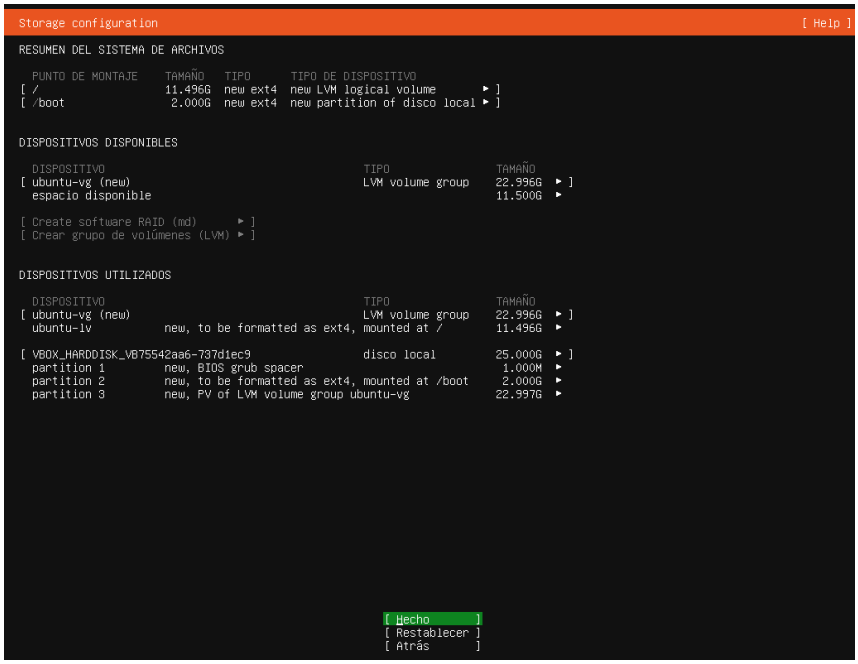


Figura B8. Configuración del almacenamiento.

En esta etapa, se recomienda revisar cuidadosamente la configuración realizada. Si se detecta algún error, se puede utilizar la opción 'Restablecer' o 'Atrás' para corregir los parámetros ingresados. En caso de que toda la configuración sea correcta, se debe seleccionar 'Hecho' para continuar con el proceso de instalación.

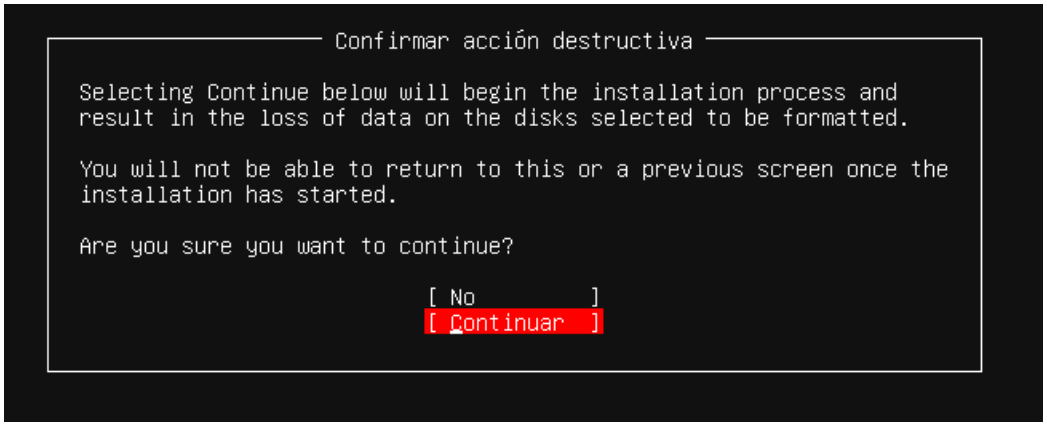


Figura B9. Confirmación de almacenamiento

Se procedió a la creación del usuario principal del sistema, asignando un nombre de usuario y una contraseña segura. Asimismo, se definió el nombre del equipo (hostname), el cual identificará al servidor dentro de la red. Esta información es esencial para la administración remota y la identificación del servidor dentro de la infraestructura implementada.

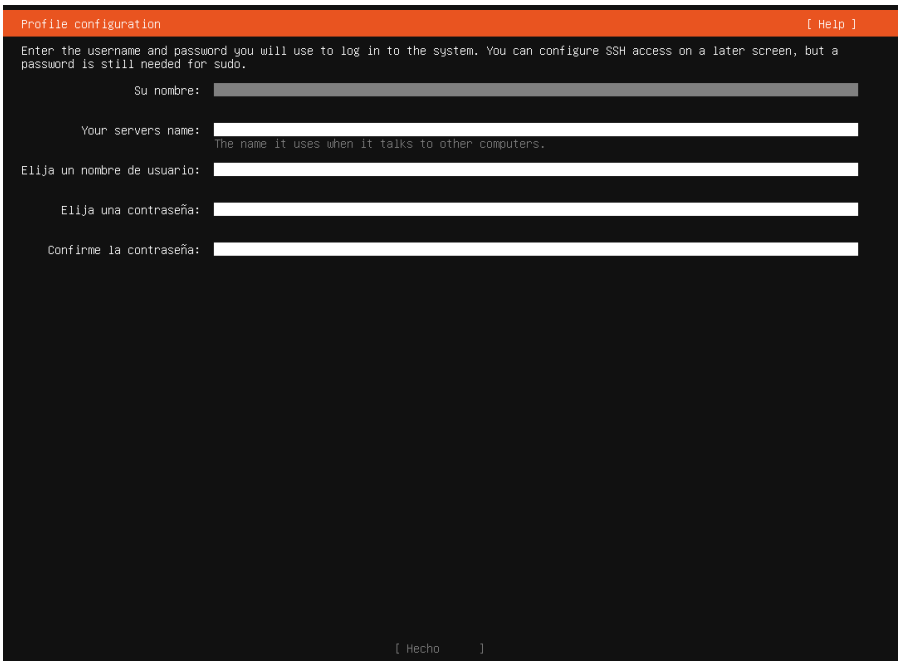


Figura B10. Configuración de Perfil

Se omitió la suscripción a Ubuntu Pro, ya que no era necesaria para los fines del proyecto. Para continuar con la instalación, se seleccionó la opción 'Hecho'.

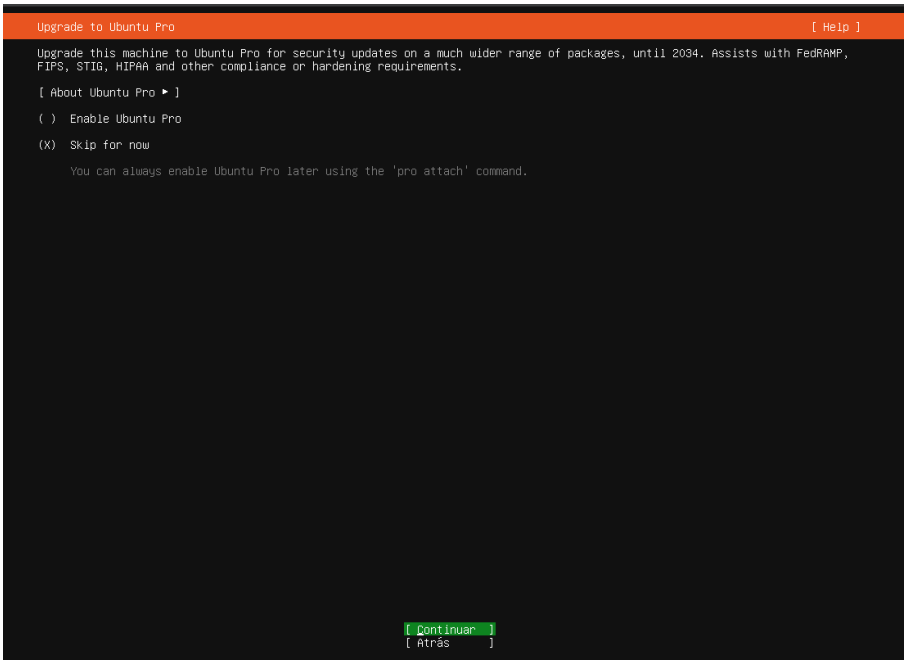


Figura B11. Actualización Ubuntu Pro

Se procedió a habilitar el servicio OpenSSH, el cual permite el acceso remoto seguro al servidor a través del protocolo SSH. Una vez seleccionada esta opción, se continuó con la instalación presionando 'Hecho'.

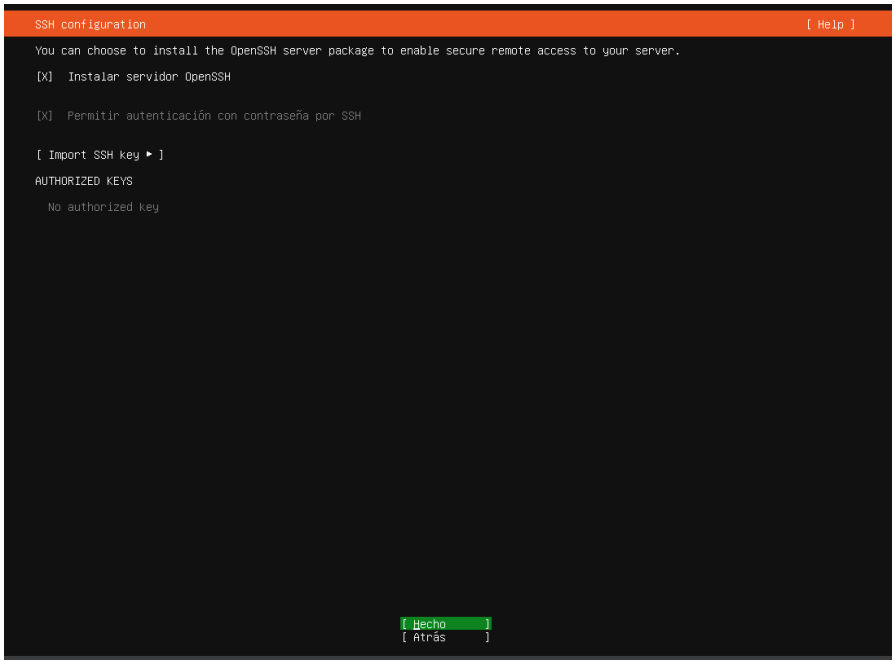


Figura B12. Idiomas del sistema operativo

En la siguiente sección del instalador, no fue necesario realizar configuraciones adicionales, por lo que se continuó con el proceso presionando la opción 'Hecho' para avanzar.

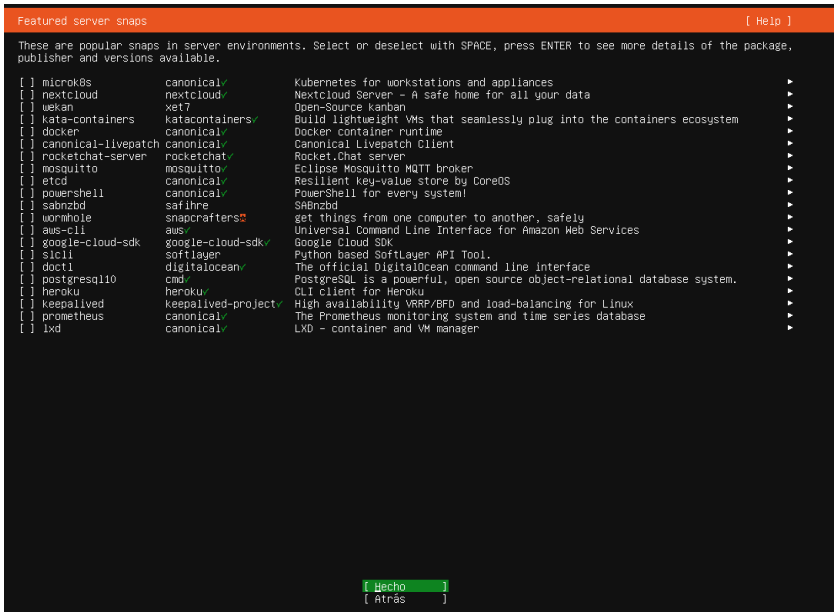


Figura B13. Selección de snaps.

La instalación se ejecutará y registrará un registro mínimo de lo realizado. Una vez que aparezca la opción "Reiniciar ahora", selecciónela y la máquina virtual se reiniciará y arrancará en Ubuntu.

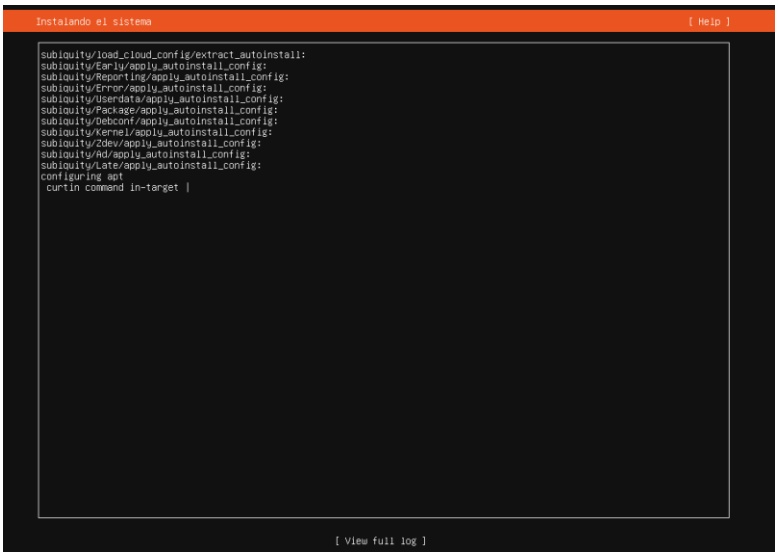


Figura B14. Idiomas del sistema operativo

Una vez finalizado el proceso de instalación, se seleccionó la opción 'Reiniciar'. Al reiniciar el sistema, se procedió a iniciar sesión utilizando las credenciales previamente configuradas (nombre de usuario y contraseña).

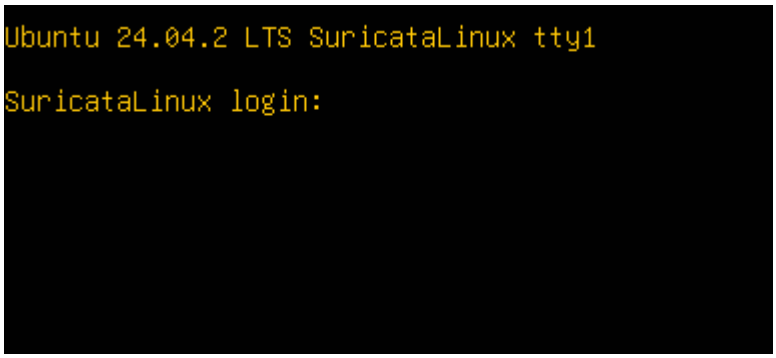


Figura B15. Terminal de Ubuntu

DOCUMENTACION

Enlace para descargar imagen ISO Ubuntu 24.04.2:
https://ubuntu.com/download/server/thank-you?version=24.04.2&architecture=amd64&lts=true

Link de requisitos mínimos del Sistema:
https://documentation.ubuntu.com/server/reference/installation/system-requirements/#system-requirements

Link de guía de escritorio:

https://documentation.ubuntu.com/_/downloads/server/en/latest/pdf/

ANEXO C. GUÍA DE INSTALACIÓN SURICATA

GUÍA DE INSTALACIÓN DE SURICATA VERSION 7.0

ELABORADO POR: BRAYAN STIVEN ALOMALIZA CHUCA

INTRODUCCION

Suricata es una de las herramientas más implementadas en entornos empresariales es el Sistema de Detección y Prevención de Intrusos (IDPS). Este sistema opera mediante reglas predefinidas que permiten detectar o incluso bloquear actividades maliciosas en la red. A diferencia de un IDS, que solo genera alertas ante eventos sospechosos, Un IDPS puede tomar acciones activas como bloquear o descartar paquetes maliciosos.

Dado el gran volumen de registros generados por estos sistemas, se vuelve necesario integrar herramientas de análisis y visualización de eventos. Este papel lo cumple un SIEM (Security Information and Event Management), que permite correlacionar eventos, realizar análisis forense de red y visualizar la información recopilada.

REQUISITOS PREVIOS

Es necesario contar con un servidor Linux y cuente con acceso administrativo. Suricata no menciona requisitos mínimos de hardware, pero se recomienda 2 núcleos de CPU con 4GB de RAM esto dependerá de la cantidad de tráfico a monitorear de esta manera se garantizará un rendimiento optimo.

INSTALACION DE SURICATA

Para garantizar el acceso a versiones estables y actualizadas del sistema de detección de intrusos Suricata, se añadió el repositorio oficial mantenido por la Open Information Security Foundation (OISF) mediante un PPA (Personal Package Archive). Esta acción permite la instalación del software desde fuentes confiables y certificadas.

```
sv1piolopez:~$ sudo add-apt-repository ppa:oisf/suricata-stable
y: 'Types: deb
ps://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
oble
s: main

on:
IDS/IPS/NSM stable packages
uricata.io/
isf.net/
```

Figura C1. Repositorio de Suricata

El comando sudo ‘apt update’ se utiliza para actualizar la base de datos de paquetes del sistema, permitiendo que este reconozca los paquetes más recientes disponibles en los repositorios configurados, incluyendo aquellos provenientes del repositorio oficial de Suricata.

```
sv1piolopez:~$ sudo apt update
p://security.ubuntu.com/ubuntu noble-security InRelease
p://ec.archive.ubuntu.com/ubuntu noble InRelease
p://ec.archive.ubuntu.com/ubuntu noble-updates InRelease [
ps://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu
p://ec.archive.ubuntu.com/ubuntu noble-backports InRelease
26 kB in 2s (71.1 kB/s)
ackage lists... Done
```

Figura C2. Actualización de paquetes.

Una vez actualizados, se procede a instalar Suricata utilizando el comando ‘apt install suricata’, lo que asegura que se descargue e instale la versión más reciente disponible desde los repositorios configurados.

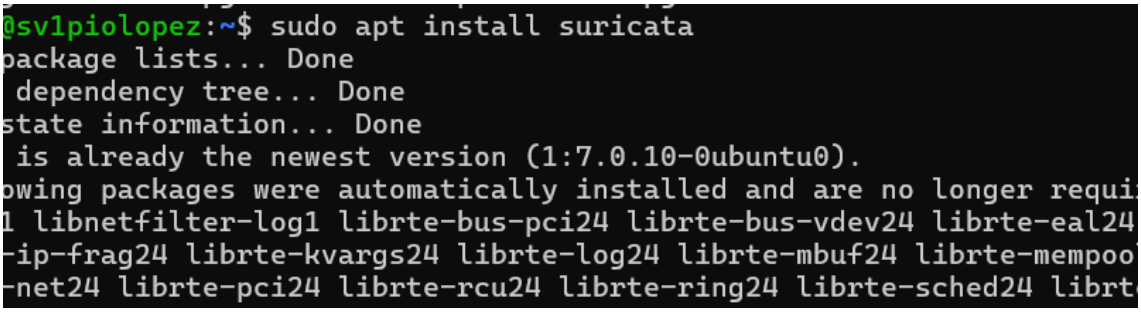


Figura C3. Instalación de Suricata.

El servicio de Suricata se habilitará para que inicie automáticamente junto con el sistema operativo. Esto asegura que el motor de detección de intrusos se ejecute tras cada reinicio. Posteriormente, se puede verificar el estado del servicio utilizando el comando sudo 'systemctl status suricata'.



Figura C4. Estado de Suricata.

Se procederá con la instalación del paquete net-tools, el cual proporciona utilidades esenciales para la administración de red, como ifconfig, netstat y otras herramientas que permiten verificar configuraciones de interfaces, monitorear conexiones y realizar diagnósticos básicos de red.

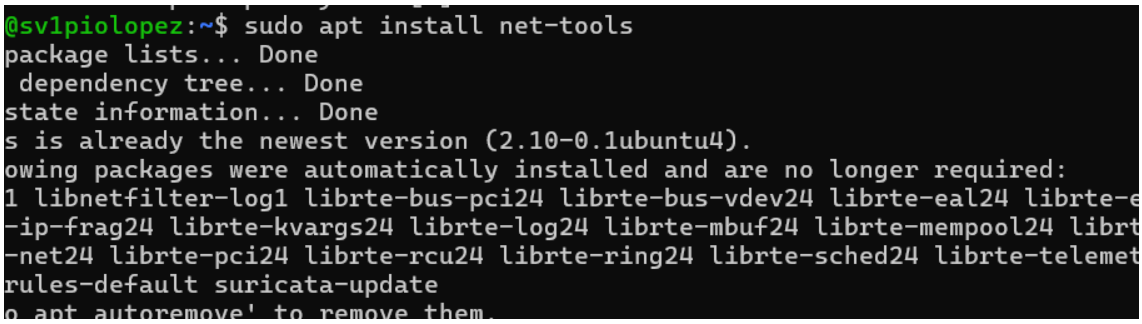


Figura C5. Instalación de net-tools

Dentro del archivo de configuración de red ubicado en /etc/netplan/50-cloud-init.yaml, se establecerá IP mediante DHCP a la interfaz que ira al conectado al router ISP y mi otra interfaz tendrá una ip estática que será conectado al router que estará conectado a

la red interna de la institución. Para ello, se accede mediante el comando ‘sudo nano /etc/netplan/50-cloud-init.yaml’. Una vez realizadas las modificaciones necesarias, se aplican los cambios ejecutando el comando ‘sudo netplan apply’. Esto asegura que la nueva configuración de red entre en efecto de inmediato.

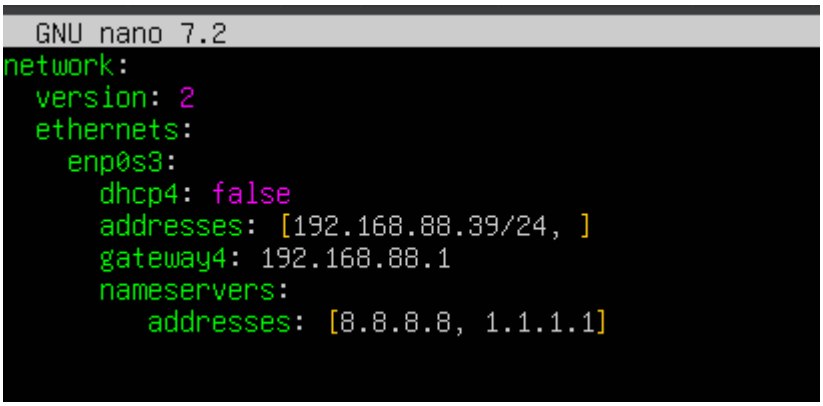


Figura C6. Editor de archivos.

En el editor de texto de suricata nos dirigimos a la línea de community-id: false. En el archivo de configuración de Suricata, se debe acceder mediante un editor de texto ‘nano /etc/suricata/suricata.yaml’ y ubicar la línea correspondiente a community-id. Esta opción debe establecerse en true para habilitar la generación de identificadores comunitarios (Community ID), lo cual facilita la correlación de eventos entre diferentes herramientas de monitoreo y análisis de tráfico en red.

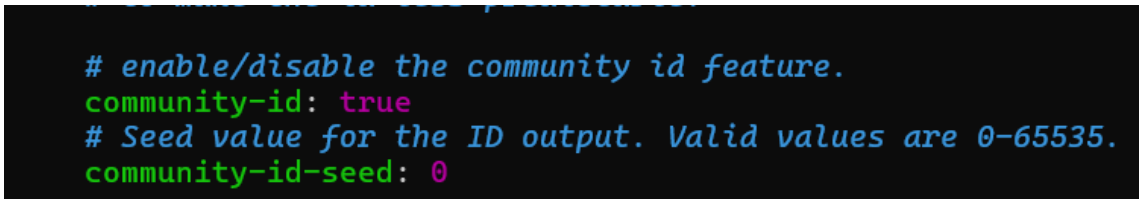


Figura C7. Archivo de Suricata

Dentro del archivo de configuración de Suricata, se debe buscar la sección correspondiente a af-packet y verificar que la interfaz de red especificada coincida con la interfaz predeterminada del sistema. En caso de que no coincidan, es necesario

modificar el valor para que se corresponda con la interfaz de red activa, asegurando así una correcta captura del tráfico.

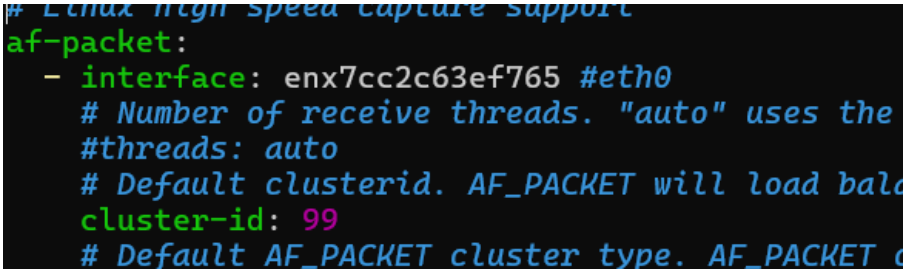


Figura C8. Editor de la interfaz.

Se procederá a reiniciar el servicio de Suricata utilizando el comando 'sudo service suricata restart' para aplicar los cambios realizados en la configuración.

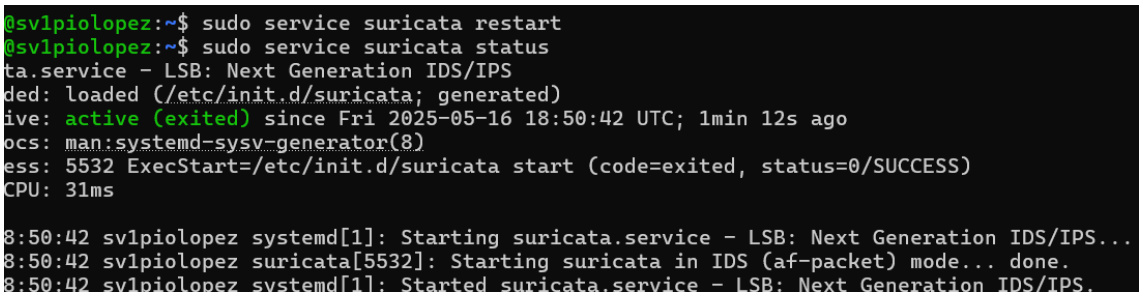


Figura C9. Servicio Suricata

Suricata-update es una herramienta destinada a recuperar conjuntos de reglas provenientes de proveedores externos y a actualizar las reglas existentes de Suricata de manera automática y eficiente.

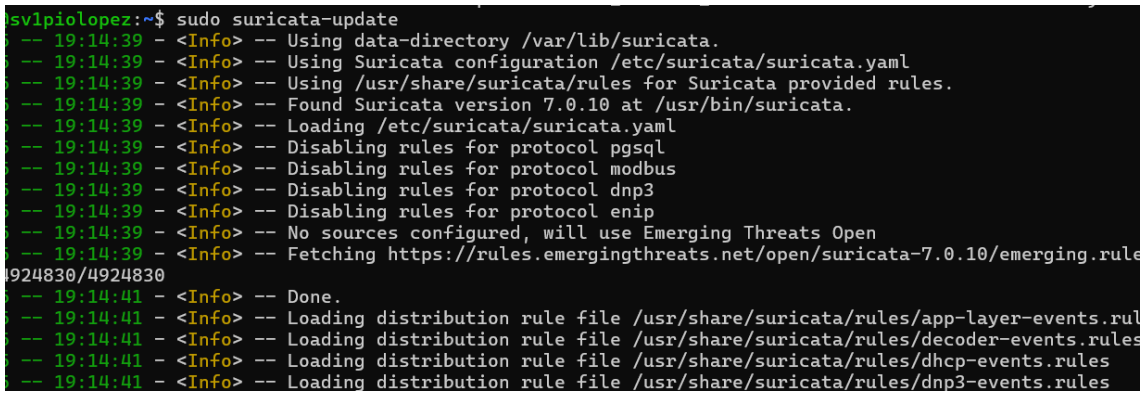


Figura C10. Actualizaciones de reglas.

A continuación, se ejecutará el comando destinado a actualizar todos los conjuntos de reglas provenientes de los proveedores de Suricata. La opción de certificado sin comprobación permite omitir la validación de la autoridad certificadora durante el proceso.



Figura C11. Actualización de Reglas.

En este punto, es posible verificar si Suricata está funcionando correctamente en modo IDS. La salida generada está diseñada para activar una alerta simulando una actividad del usuario raíz.

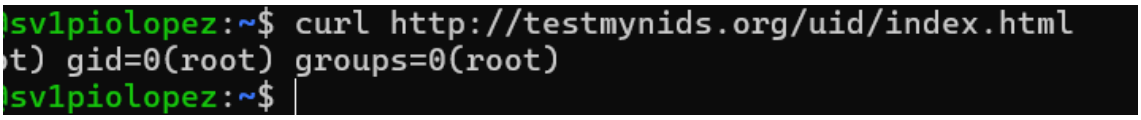


Figura C12. Funcionamiento de Suricata

CONFIGURACIÓN DE SURICATA A (IDS/IPS)

Dentro del archivo de configuración ubicado en /etc/suricata/suricata.yaml, es necesario realizar modificaciones específicas en determinadas líneas con el objetivo de habilitar el modo IPS en el servidor Suricata, permitiendo que todo el tráfico sea procesado de manera adecuada.

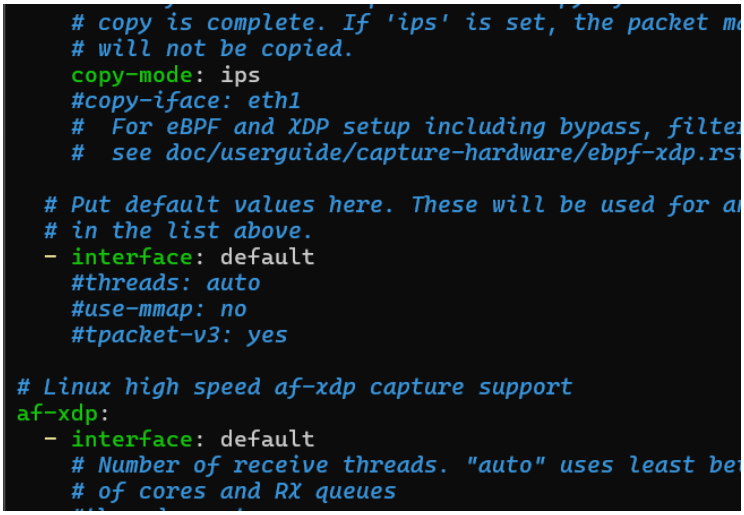


Figura C13. Archivo de edición.

Se guarda la configuración y se debe reiniciar Suricata mediante el siguiente comando 'sudo service suricata restart'. Una vez realizada la modificación en el archivo de configuración, se debe guardar el cambio y reiniciar el servicio de Suricata. Esto se puede hacer ejecutando el siguiente comando 'sudo service suricata restart' Este

reinicio asegura que Suricata aplique la nueva configuración establecida en el archivo editado.

```
sv1piolopez:~$ sudo service suricata restart
sv1piolopez:~$ sudo service suricata status
a.service - LSB: Next Generation IDS/IPS
ed: loaded (/etc/init.d/suricata; generated)
ve: active (running) since Fri 2025-05-16 20:48:11 UTC; 7s ago
cs: man:systemd-sysv-generator(8)
ss: 8162 ExecStart=/etc/init.d/suricata start (code=exited, status=0/S
ks: 1 (limit: 2272)
ry: 112.7M (peak: 335.3M)
PU: 7.438s
up: /system.slice/suricata.service
    └─8169 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile

:48:11 sv1piolopez systemd[1]: Starting suricata.service - LSB: Next G
:48:11 sv1piolopez suricata[8162]: Starting suricata in IPS (nfqueue)
:48:11 sv1piolopez systemd[1]: Started suricata.service - LSB: Next Ge
```

Figura C14 Estatus del sistema Suricata.

Para gestionar las vulnerabilidades identificadas en análisis previos, se procede a la creación de un nuevo archivo destinado a almacenar las reglas correspondientes. Este archivo se genera mediante el siguiente comando *"sudo nano /var/lib/suricata/rules/piolopez2.rules"* Las reglas definidas en este archivo se establecen con base en los resultados obtenidos a través de los escaneos de vulnerabilidades realizados previamente.

```
# Bloquear acceso HTTP no autenticado
drop tcp any any -> any 80 (msg:"Bloqueo HTTP no autenticado"; sid:1000100;)

# Detectar credenciales por defecto (ejemplo para tráfico plano)
alert http any any -> any any (msg:"Detectado posible uso de admin:admin"; content:"Auth

# Bloquear tráfico HTTP, forzar HTTPS
drop tcp any any -> any 80 (msg:"Prohibido HTTP, solo HTTPS permitido"; sid:1000102;)

# Bloquear Telnet
drop tcp any any -> any 23 (msg:"Bloqueo de Telnet"; sid:1000200;)

# Alerta SSH sin hardening
alert tcp any any -> any 22 (msg:"Alerta: SSH sin hardening"; sid:1000201;)

# Detectar tráfico UPnP
alert udp any any -> any 1900 (msg:"UPnP detectado"; sid:1000202;)

# TR-069 abierto
alert tcp any any -> any 7547 (msg:"TR-069 sin restricciones"; sid:1000203;)

# SNMP sin autenticación
alert udp any any -> any 161 (msg:"SNMP posiblemente inseguro"; sid:1000204;)
```

Figura C15. Reglas personalizadas

Agregaremos las reglas creadas al archivo de configuración de Suricata.

```
    #
    hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - piolopez2.rules
```

Figura C16. Archivo editable.

Vuelva a probar la configuración para comprobar que no hubo problemas al crear la regla con el comando 'sudo suricata -T -c /etc/suricata/suricata.yaml -v'. De esta manera ya tendremos nuestro host configurado en modo IDS e IPS.

DOCUMENTACION

Link para la instalación de Suricata: https://docs.suricata.io/en/latest/install.html

INSTALACIÓN Y CONFIGURACIÓN DE ELK STACK

ELABORADO POR: BRAYAN STIVEN ALOMALIZA CHUCA

INTRODUCCIÓN

La plataforma de análisis y visualización de datos está diseñada para gestionar grandes volúmenes de información en tiempo real, proporcionando herramientas avanzadas para el procesamiento y la interpretación de datos. Su arquitectura está compuesta por cuatro componentes fundamentales: Elasticsearch, Logstash, Beats y Kibana, cada uno con una función específica dentro del flujo de trabajo. Beats se encarga de la recolección de datos desde diversas fuentes, Logstash procesa y transforma la información recopilada, Elasticsearch la almacena y permite su búsqueda avanzada, mientras que Kibana ofrece una interfaz gráfica intuitiva para explorar, analizar y visualizar los datos. La instalación de esta plataforma puede llevarse a cabo tanto en entornos locales como en la nube, lo que brinda una gran flexibilidad para adaptarse a distintos escenarios tecnológicos. Una configuración adecuada y una integración eficiente entre estos componentes garantizan un funcionamiento óptimo, facilitando la administración de datos y la generación de dashboards e informes personalizados según las necesidades específicas de cada usuario o sistema.

REQUISITOS MÍNIMOS DEL SISTEMA

- Se recomienda para el correcto funcionamiento los siguientes requisitos mínimos.
- Procesador de 4 núcleos.
- 8GB de memoria RAM.
- 50GB de espacio libre en disco esta cantidad varía dependiendo el volumen de datos.

INSTALACION Y CONFIGURACION DE ELK STACK

Para la instalación vamos a importar claves públicas con el siguiente comando '*wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -*'. Se

agregará el repositorio de Elastic con el siguiente comendo '*sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" > /etc/apt/sources.list.d/elastic-8.x.list''* como se muestra en la Figura1.



Figura D1. Clave publica y repositorio

Se llevó a cabo la actualización del sistema operativo como paso previo a la instalación de Elasticsearch, el motor de búsqueda y análisis del ELK Stack. Se añadieron los repositorios oficiales y se importó la clave GPG para garantizar la seguridad e integridad de los paquetes. A continuación, se instaló Elasticsearch utilizando el gestor de paquetes APT. Una vez completada la instalación, se verificó el estado del servicio para asegurar su correcto funcionamiento. Este procedimiento permitió dejar operativo el componente que se encargará de indexar y almacenar los datos recopilados. El proceso se muestra detalladamente en la Figura D2.

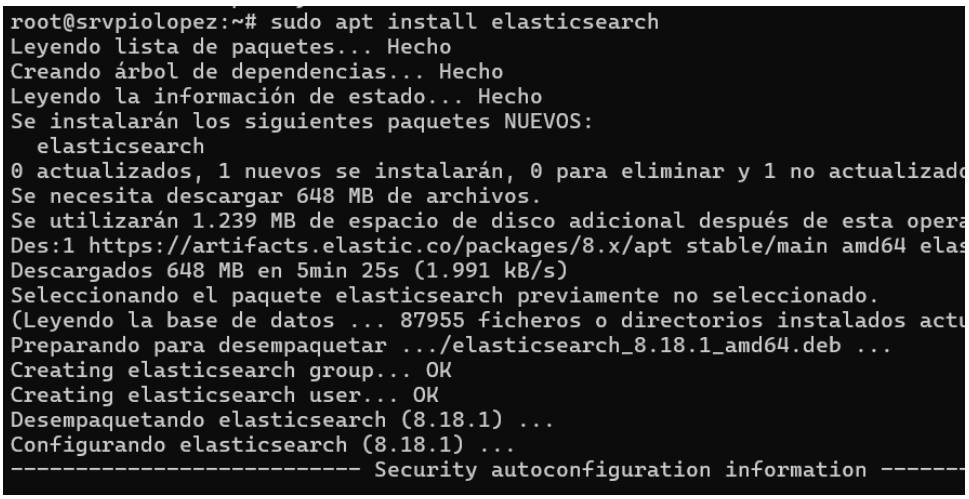


Figura D2. Instalación de Elasticsearch.

Posteriormente, se procedió con la instalación de Logstash, herramienta responsable del procesamiento y transformación de datos dentro del ELK Stack. Para ello, se utilizó el comando sudo apt install logstash. Una vez instalado, se habilitó su ejecución automática al inicio del sistema mediante sudo systemctl enable logstash y se inició el servicio con sudo systemctl start logstash. Estos pasos garantizaron que Logstash estuviera operativo y se ejecutara de forma automática al reiniciar el servidor. El procedimiento seguido se muestra en la Figura D3.

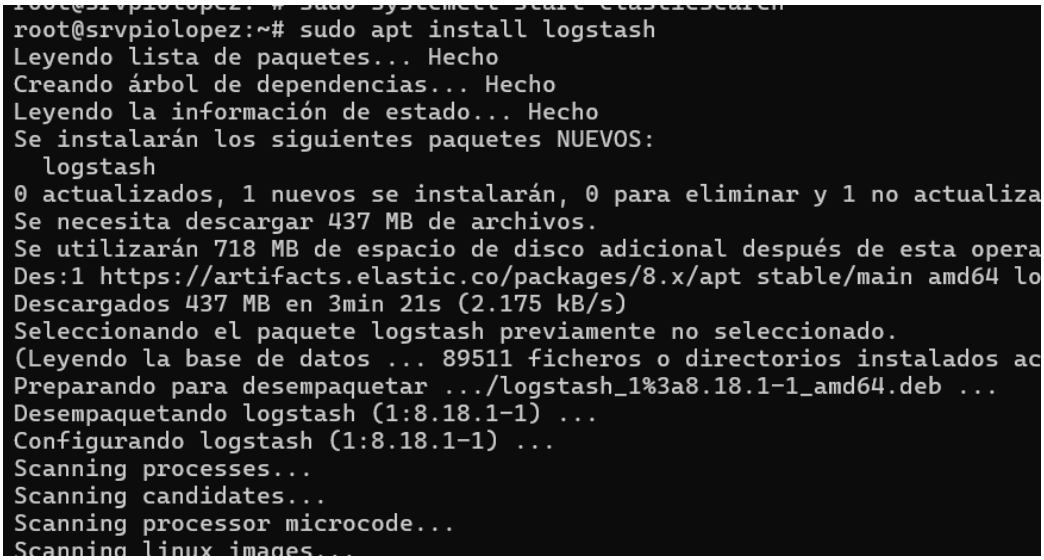


Figura D3. Instalación de logstash.

Una vez instalado Logstash, se procedió a iniciar su servicio utilizando el comando sudo systemctl start logstash, asegurando así su funcionamiento en segundo plano. A continuación, se instaló Kibana, herramienta encargada de la visualización de los datos procesados a través de dashboards interactivos. Para ello, se empleó el comando sudo apt install kibana. Esta etapa fue fundamental para habilitar la interfaz gráfica del ELK Stack, como se observa en la Figura D4.

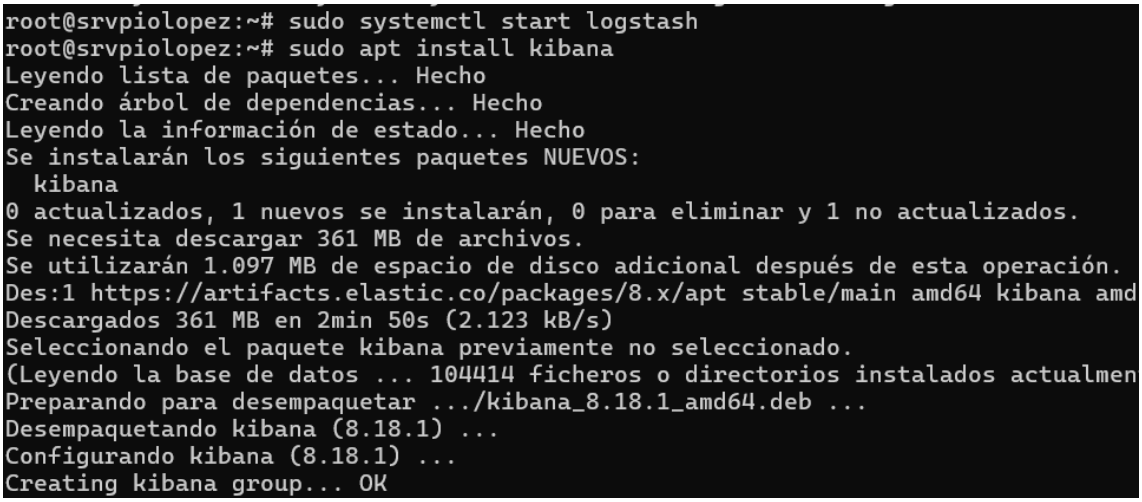


Figura D4. Instalación Kibana.

CONFIGURACIÓN

Con el fin de configurar correctamente el servicio de Elasticsearch, se procedió a editar el archivo de configuración principal ubicado en la ruta /etc/elasticsearch/elasticsearch.yml. En este archivo, se especificó el puerto por el cual el servicio escucharía las solicitudes, permitiendo así su correcta comunicación con los demás componentes del ELK Stack. Esta configuración fue un paso clave para garantizar la accesibilidad y el funcionamiento del servicio dentro de la red. El proceso realizado se muestra en la Figura D5.

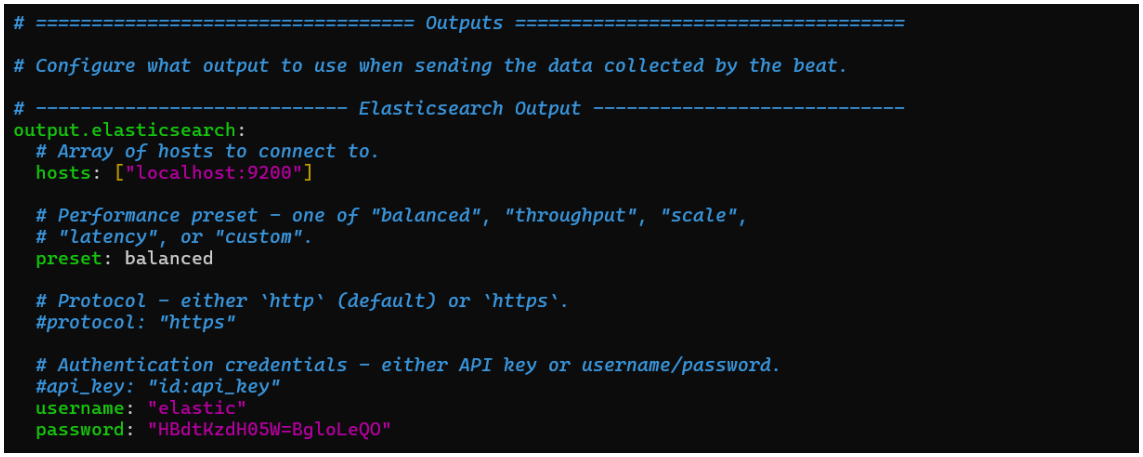


Figura D5. Configuración de elasticsearch.

Una vez finalizada la configuración del archivo elasticsearch.yml, se reinició el servicio de Elasticsearch utilizando el comando sudo systemctl restart elasticsearch para aplicar los cambios realizados. Posteriormente, se verificó que el servicio estuviera escuchando correctamente en el puerto 9200 mediante el comando curl -X

GET "localhost:9200/", el cual fue ejecutado con las credenciales correspondientes de usuario y contraseña. Esta comprobación permitió asegurar que Elasticsearch estaba activo y accesible, como se muestra en la Figura D6.

```
root@srvpiolopez:~# curl -k -u elastic:HBdtKzdH05W=BgloLeQO https://localhost:9200/
{
  "name" : "srvpiolopez",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "O7RTlePyTBmHqIvTdpgweQ",
  "version" : {
    "number" : "8.18.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "df116ec6455476a07daafc3ded80e2bb1a3385ed",
    "build_date" : "2025-04-30T10:07:44.026929518Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.1",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Figura D6. Resultados del elasticsearch.

CONFIGURACIÓN DE KIBANA

Posteriormente, se procedió a editar el archivo de configuración de Kibana, ubicado en la ruta /etc/kibana/kibana.yml, con el propósito de establecer la conexión con el servicio de Elasticsearch previamente configurado. En este archivo se definieron parámetros clave, como la URL del host de Elasticsearch y los datos de autenticación necesarios, permitiendo que Kibana pudiera acceder y visualizar los datos indexados. Esta configuración fue esencial para el correcto funcionamiento de la interfaz gráfica de monitoreo, como se ilustra en la Figura D7.

```
# ================== System: Elasticsearch ==================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["https://localhost:9200"]

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "elastic"  #"kibana_system"
elasticsearch.password: "HBdtKzdH05W=BgloLeQO"  #"pass"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# Service account tokens are Bearer style tokens that replace the traditional username/password based configuration.
# Use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults to the value of
```

Figura D7. Archivo editado de Kibana.

Una vez realizada la configuración correspondiente, se procedió a iniciar el servicio de Kibana utilizando el comando sudo systemctl restart kibana, con el objetivo de

aplicar los cambios realizados en el archivo de configuración. Posteriormente, se verificó el estado del servicio mediante el comando sudo systemctl status kibana, asegurando que se estuviera ejecutando correctamente y sin errores. Esta comprobación permitió confirmar la disponibilidad de la interfaz de Kibana, como se muestra en la Figura D8.

```
root@srvpiolopez:~# nano /etc/kibana/kibana.yml
root@srvpiolopez:~# sudo systemctl restart kibana
root@srvpiolopez:~# sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-05-27 20:15:10 UTC; 11s ago
       Docs: https://www.elastic.co
   Main PID: 26093 (node)
      Tasks: 11 (limit: 4482)
     Memory: 170.5M (peak: 170.8M)
        CPU: 5.617s
     CGroup: /system.slice/kibana.service
             └─26093 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/
```

Figura D8. Iniciar servicio de kibana.

Una vez finalizada la configuración e iniciado el servicio de Kibana, se procedió a revisar los registros del sistema para verificar su funcionamiento. Para ello, se utilizó el comando sudo tail -n 50 /var/log/kibana/kibana.log, el cual permitió visualizar las últimas 50 líneas del archivo de log de Kibana. Esta revisión fue fundamental para detectar posibles errores o advertencias durante el arranque del servicio. La salida del registro se muestra en la Figura D9.

```
root@srvpiolopez:~# sudo tail -n 50 /var/log/kibana/kibana.log
{"ecs":{"version":"8.11.0"},"@timestamp":"2025-05-27T19:38:37.047+00:00","message":"Kibana
id":21512,"uptime":9.714098066}}
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
nfigured with roles: [background_tasks, ui]","log":{"level":"INFO","logger":"node"},"proce
7f671eb2c0663d79cb48"},"transaction":{"id":"1b3929eda9397066"}}
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
gins are disabled: \"cloudChat,cloudExperiments,cloudFullStory,dataUsage,investigateApp,in
es,securitySolutionServerless,serverless,serverlessObservability,serverlessSearch\".","log
12,"uptime":38.180891087},"trace":{"id":"713e24c9cf7a7f671eb2c0663d79cb48"},"transaction":
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
ng at http://localhost:5601","log":{"level":"INFO","logger":"http.server.Preboot"},"proces
7f671eb2c0663d79cb48"},"transaction":{"id":"1b3929eda9397066"}}
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
ugins: [interactiveSetup]","log":{"level":"INFO","logger":"plugins-system.preboot"},"proce
a7f671eb2c0663d79cb48"},"transaction":{"id":"1b3929eda9397066"}}
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
p\" plugin is holding setup: Validating Elasticsearch connection configuration…","log":{"l
8.776563315},"trace":{"id":"713e24c9cf7a7f671eb2c0663d79cb48"},"transaction":{"id":"1b3929
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
il preboot stage is completed.","log":{"level":"INFO","logger":"root"},"process":{"pid":21
3d79cb48"},"transaction":{"id":"1b3929eda9397066"}}
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
- initiating shutdown","log":{"level":"INFO","logger":"root"},"process":{"pid":21512,"upti
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
g down","log":{"level":"INFO","logger":"root"},"process":{"pid":21512,"uptime":2200.236743
{"service":{"node":{"roles":["background_tasks","ui"]}},"ecs":{"version":"8.11.0"},"@times
```

Figura D9. Salida de log de Kivana.

DOCUMENTACION

Link de instalación: https://www.elastic.co/docs/deploy-manage/deploy/self-managed/install-elasticsearch-from-archive-on-linux-macos

ANEXO E. GUIA DE CREACION DE REGLAS

PERSONALIZADAS PARA SURICATA

GUIA DE CREACION DE REGLAS PERSONALIZADAS PARA SURICATA

ELABORADO POR: BRAYAN STIVEN ALOMALIZA CHUCA

INTRODUCCION

En cualquier entorno de red, es fundamental identificar y mitigar vulnerabilidades específicas que puedan poner en riesgo la integridad, disponibilidad o confidencialidad de los sistemas. Suricata permite diseñar reglas adaptadas a estas necesidades concretas, de modo que se pueda actuar de forma inmediata ante actividades sospechosas o configuraciones inseguras previamente detectadas.

Estas reglas no solo buscan bloquear tráfico malicioso, sino también generar alertas tempranas ante comportamientos anómalos, servicios expuestos o protocolos desactualizados. Al desarrollar reglas personalizadas en función de las debilidades halladas en la infraestructura de la institución, se establece un control más preciso sobre el flujo de datos y se fortalece la seguridad del entorno de forma proactiva.

FORMATO DE REGLAS Y ESTRUCTURA

Cada regla en Suricata se compone de dos partes esenciales que trabajan en conjunto para definir cómo debe analizarse el tráfico de red. La primera es la cabecera, que establece los parámetros generales del flujo a inspeccionar, como el protocolo, direcciones IP y puertos de origen y destino. La segunda parte son las opciones, que detallan los criterios específicos que deben cumplirse y qué acciones tomar en caso de coincidencia.

<acción> <protocolo> <IP_origen> <puerto_origen> <dirección> <IP_destino> <puerto_destino> (opciones)

La forma oficial de instalar conjuntos de reglas definidas por Suricata es a través del comando ‘suricata-update’. Una regla o firma consiste en

Acción: Determina que ocurre cuando se cumple una condición.

Encabezado: Definen protocolos, IP’s, puertos y direcciones.

Opciones de regla: Definen los detalles de las reglas.

EJEMPLO DE REGLA

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1;)

Esta regla de Suricata genera una alerta cuando se detecta una solicitud HTTP tipo GET desde la red interna hacia el exterior que contenga la palabra "rule" en el URI. Está orientada a identificar posibles actividades sospechosas o automatizadas que intenten acceder a recursos específicos del servidor. Se aplica únicamente a conexiones establecidas hacia el servidor y clasifica el evento como comportamiento desconocido.

ESTRUCTURA DE CABECERA DE UNA REGLA EN SURICATA

Dentro de Suricata, las acciones válidas que pueden ejecutarse ante una coincidencia incluyen la generación de alertas, el bloqueo o rechazo del tráfico, así como la posibilidad de permitir el paso del paquete registrado para su análisis posterior. Estas acciones son configuradas según la política de seguridad establecida en el sistema.

Tabla 1: Estructura de Reglas de Suricata

Elemento	Función	Ejemplo
Acción	Define cómo Suricata debe reaccionar al detectar coincidencias.	alert, pass, reject, drop, rejectdst
Protocolo Básicos	Protocolo que se evaluará en el análisis del tráfico.	tcp, icmp, udp, ip

Elemento	Función	Ejemplo
IP de Origen	Dirección IP desde donde se genera el tráfico a inspeccionar.	10.1.1.10, any, 172.16.0.0/12
Puerto de Origen	Puerto desde el cual se inicia la conexión.	443, 20:1023, any
Sentido del Tráfico	Define si el análisis es unidireccional o bidireccional.	->, =>, <>
Operadores	Definir condiciones específicas que el motor de detección debe evaluar en el tráfico de red.	:, !, [..,..]
IP de Destino	Dirección IP que recibe el tráfico examinado.	192.168.100.100, any
Puerto de Destino	Puerto hacia el cual se dirige el tráfico.	8080, any, 1000:2000

OPCIONES DE CONFIGURACIÓN EN LAS REGLAS DE SURICATA

Tabla 2. Configuración de reglas

Parámetro	Propósito	Ejemplo
sid	Identificador numérico que diferencia una regla de otra.	sid:3050001;
msg	Texto descriptivo que aparece cuando la regla genera una alerta.	msg:"Intento de escaneo detectado";
rev	Número de revisión que indica cambios o actualizaciones de la regla.	rev:5;
content	Patrón de texto que se busca en el cuerpo del paquete.	content:"/cgi-bin";
http.method	Indica el método HTTP que se analizará.	http.method; content:"GET";
flow	Condición del flujo de tráfico (establecido, dirección).	flow:to_client, established;
threshold	Permite definir una frecuencia límite para generar alertas.	threshold: type limit, count 3, seconds 60;
classtype	Clasifica el tipo de amenaza o evento para priorizar respuestas.	classtype:policy-violation;
priority	Nivel de criticidad asignado a la alerta.	priority:3;
metadata	Información extra como nombre del creador, fecha o referencias.	metadata: author "admin", created 2025-05-16;

CREACIÓN DE REGLAS

Una vez comprendida la estructura de las reglas en Suricata, se procedió a la creación de reglas personalizadas adaptadas a las necesidades del proyecto de integración. Estas

reglas fueron definidas en función de los resultados obtenidos tras el escaneo de la red institucional, considerando las vulnerabilidades detectadas en la infraestructura existente.

REGLA 1. Permite el tráfico SSH en el puerto 22.

pass tcp any any -> any 22 (msg:"Permitir SSH"; sid:1000003;)

Descripción:

Acción: pass - detiene la inspección adicional del paquete.

Protocolo: tcp – Análisis de tráfico TCP

Dirección y Puerto: any -> any:22

Mensaje: “Permitir SSH”

Opciones: sid:10000003 – Identificador único de la regla.

Permite explícitamente conexiones SSH sin generar alertas.

REGLA 2 - ICMP Timestamp Reply Detection CVE: CVE-1999-XXXX

alert icmp any any -> any any (itype:14; msg:"ICMP Timestamp Reply Disclosure - CVE-1999-XXXX"; reference:cve,1999-0524; classtype:misc-activity; sid:1000102; rev:2;)

Descripción:

Acción: Alertar

Protocolo: ICMP

Dirección y Puerto: any -> any

Mensaje: "ICMP Timestamp Reply Disclosure - CVE-1999-XXXX"

Opciones: sid:1000102 – Identificador único de la regla.

Alerta si un host responde con ICMP timestamp reply, indicador de habilitación de timestamps para fingerprinting.

REGLA 3 - jQuery vulnerable (XSS - CVE-2012-XXXX)

alert http any any -> any any (msg:"Potential vulnerable jQuery version used (XSS - CVE-2012-XXXX)"; flow:to_client,established; content:"jquery.js"; http.uri; content:"1.7.1"; file_data; reference:cve,2012-6708; classtype:web-application-attack; sid:100001; rev:2;)

Descripción:

Acción: Alertar.

Protocolo: HTTP

Dirección y Puerto: any -> any

Mensaje: "Potential vulnerable jQuery version used (XSS - CVE-2012-XXXX)"

Opciones: sid:100001 – Identificador único de la regla.

Alerta cuando se detecta uso de jQuery versión vulnerable 1.7.1 para prevenir ataques XSS.

REGLA 4 - Transmisión de credenciales por HTTP (sin cifrado)

alert http any -> any any (msg:"HTTP Basic Authentication over cleartext (Sensitive data exposure)"; flow:to_server, established; content:"Authorization: Basic "; http.header; classtype:policy-violation; sid:100002; rev:1;)

Descripción:

Acción: Alertar

Protocolo: HTTP

Dirección y Puerto: any -> any

Mensaje: "HTTP Basic Authentication over cleartext (Sensitive data exposure)"

Opciones: sid:100002 – Identificador único de la regla.

Alerta si se transmiten credenciales en texto claro en HTTP.

REGLA 5 - SMB Null Session Authentication Bypass

Descripción:

Acción: Alertar

Protocolo: TCP

Dirección y Puerto: any -> any puerto 445

Mensaje: "SMB Null Session Authentication Bypass attempt"

Opciones: sid:200001 – Identificador único de la regla.

Detecta intentos de acceso sin autenticación a recurso compartido SMB IPC$.

REGLA 6 - DCE/RPC y MSRPC Service Enumeration

alert tcp any any -> any any 135 (msg:"DCE/RPC or MSRPC service enumeration attempt"; flow:to_server, established; classtype: attempted-recon; sid:200002; rev:1;)

agregar detección por patrones más específicos si tienes firmas DCE/RPC.

Descripción:

Acción: Alertar

Protocolo: TCP

Dirección y Puerto: any -> any puerto 135

Mensaje: "DCE/RPC or MSRPC service enumeration attempt"

Opciones: sid:200002 – Identificador único de la regla.

Alerta intentos de reconocimiento/escaneo de servicios RPC en puerto 135.

REGLA 7 - ICMP Timestamp Reply Information Disclosure

alert icmp any any -> any any (msg:"ICMP Timestamp Reply detected"; itype:14; classtype:info; sid:200004; rev:2;)

Descripción:

Acción: Alertar

Protocolo: ICMP

Dirección y Puerto: any -> any

Mensaje: "ICMP Timestamp Reply detected"

Opciones: sid:200004 – Identificador único de la regla.

Alerta recepción de paquete ICMP timestamp reply, usado para fingerprinting.

IMPLEMENTACION Y VERIFICACION DE REGLAS EN SUIRCATA

Se debe crear un nuevo archivo de reglas en la ruta /etc/suricata/rules/ con el nombre piolopez.rules, donde se colocarán todas las reglas personalizadas. Una vez agregadas, se guarda el archivo, como se muestra en la Figura 1.

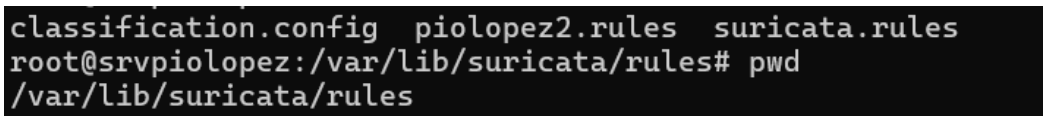


Figura 1. Creación de la regla piolopez2.rules.

Luego, se edita el archivo suricata.yaml, ubicado en /etc/suricata/, y en la sección rule-files se añade el nombre del nuevo archivo: - piolopez2.rules como se muestra en la Figura 2. Finalmente, se guardan los cambios y se reinicia el servicio de Suricata con el comando sudo systemctl restart suricata para aplicar las nuevas reglas.

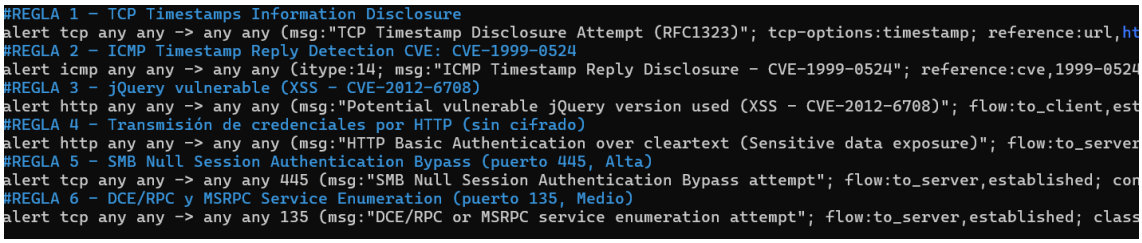


Figura 2. Archivo editable.

Documentación

Link: https://docs.suricata.io/en/latest/rules/intro.html